KAUR, JOTI. Ph.D. Assessing Thriving at Work and Employee Competence for Information Security Job Performance. (2022)
Directed by Dr. Kane Smith. 153 pp.

Majority of the organizations are continuously under threat because of employees' mishandling of sensitive information. While information security is an integral part of employee responsibility, failure to follow security procedures and non-compliance with organizational information security policies result in sub-par job performance. There are numerous instances where regular employees have inadvertently and without malicious intent caused a data breach (for instance, the Federal Deposit Insurance Corp. data breach in 2016, Home Depot data breach in 2014, Colonial Pipeline cyberattack in 2021). Given the fact that close to 51 percent of information threats are posed by organizations' employees, it is crucial to understand how information security job performance can be enhanced to mitigate such threats. While studies over the past several decades have acknowledged the importance of security education training and awareness (SETA) programs (Puhakainen and Siponen, 2010; Hu et al., 2021; Dhillon et al., 2020) and other motivational strategies to ensure compliance, there has been limited emphasis on improving information security job performance by developing competent individuals.

This research facilitates a deeper understanding of the multifaceted and complex construct of information security job performance as an outcome of an individual self-adaptive process which includes thriving in the work environment and competence to fulfil one's job responsibility. Thriving is an important domain of inquiry as it is a subjective experience that allows employees to develop in a positive manner. To further understand the knowledge, ability, and skills from information security related behavior of employees, we explored the impact of psychological capital which is a higher-order construct comprising the work-related tenets of positive psychology: hope, self-efficacy, resilience, and optimism. Furthermore, we also

investigated the impact of employee competence on information security job performance. Drawing from the extant literature, competence is an idiosyncratic combination of what Weick and Roberts (1993) term as *know-how* and *know-that*. We conducted this research using a sequential qualitative and quantitative approach situated in a large public sector bank in India. The findings of this research have both theoretical and practical implications. Our results show that employee competence leveraged through thriving and agentic work behaviors can impact information security job performance. Overall, this research extends the information security literature by exploring the dimensionality of information security job performance and also offers insights on improving employee competence towards information security roles and activities.

ASSESSING THRIVING AT WORK AND EMPLOYEE COMPETENCE FOR INFORMATION SECURITY JOB PERFORMANCE

by

Joti Kaur

A Dissertation
Submitted to
the Faculty of The Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Greensboro

2022

Approved by

Dr. Kane Smith
Committee Chair

DEDICATION

To my family and friends.

APPROVAL PAGE

This dissertation written by Joti Kaur has been approved by the following committee of the Faculty of The Graduate School at The University of North Carolina at Greensboro.

Committee Chair

Dr. Kane Smith

Committee Members

Dr. Gurpreet Dhillon

Dr. Franck Loic Soh Noume

Dr. Kwasi Amoako-Gyampah

Dr. Zhiyong Yang

July 8, 2022

Date of Acceptance by Committee

July 8, 2022

Date of Final Oral Examination

ACKNOWLEDGEMENTS

I would like to acknowledge the incredible support and encouragement of my advisors and teachers whose guidance and contributions have made this research a possible endeavor. Thank you, first and foremost, to the members of my Dissertation Committee: Dr. Kane J. Smith, Dr. Gurpreet Dhillon, Dr. Franck Loic Soh Noume, Dr. Kwasi Amoako-Gympah, and Dr. Zhiyong Yang. I would like to express my profound gratitude to my current Dissertation Chair, Dr. Kane Smith and my previous Committee Chair, Dr. Gurpreet Dhillon for their immense support and encouragement on the path that made this research possible. I am indebted to them in countless ways and for being great educators. I am truly grateful to Dr. Franck Loic Soh Noume, Dr. Kwasi Amoako-Gympah, and Dr. Zhiyong Yang for their tremendous assistance and advice in navigating this huge endeavor. It was indeed the most enriching experience of learning for me, and I am grateful to have advisors who generously shared their expertise and wealth of knowledge to make this research a success.

Finally, I would also like to extend my gratitude to the ISSCM Department Head, Dr. Gargeya, Ph.D. Program Director, Dr. Al Salam, Ph.D. program teachers, my fellow doctoral friends, and my loving family for their support and understanding.

Thank you All!

TABLE OF CONTENTS

LIST OF TABLES x

LIST OF FIGURES xi

CHAPTER I: INTRODUCTION 1

1.1 Problem domain 2
1.2 Definitions 5
1.3 Significance of this Study 8
1.4 Scope of this Research 9
1.5 Structure of this Thesis 10

CHAPTER II: A LITERATURE REVIEW OF INFORMATION SECURITY RESEARCH IN INFORMATION SYSTEMS 13

2.1 Introduction 13
2.2 The State of Information Security Research and Performance Outcomes 14
2.3 Thriving at Work and Information Security Research 19
Agentic Work Behavior 24
2.4 Employee Competence and Information Security Research 25
2.5 Conclusion 30

CHAPTER III: THEORY AND RESEARCH METHODOLOGY 32

3.1 Introduction 32
3.2 Informing Theories 33
3.2.1 Thriving at Work 33
Agentic Enablers of Thriving 35
3.2.2 Psychological Capital 37
3.2.3 Competence 44
3.3 Study methodology 46
3.4 Mixed methods research design 47
3.4.1 Qualitative Case Study 49
General Banking Sector in India 50
The Case of a Public Sector Bank in India 52

3.4.2 Quantitative Study 53
3.5 Conclusion 53
CHAPTER IV: THRIVING AT WORK AND INFORMATION SECURITY JOB PERFORMANCE 55
4.1 Introduction 55
4.2 Background 56
4.3 Qualitative Case Study 59
4.4 Hypotheses development 65
4.4.1 Psychological capital and agentic work behaviors 66
4.4.2 Thriving at work 67
4.4.3 Information security job performance 68
4.5 Empirical analysis 69
4.5.1 Data collection 69
4.5.2 Data analysis 70
4.5.3 Measurement model 71
4.5.4 Structural model 72
4.6 Contribution 75
4.7 Conclusion 76
CHAPTER V: EMPLOYEE COMPETENCE AND INFORMATION SECURITY JOB PERFORMANCE 78
5.1 Introduction 78
5.2 The concept of information security compliance 79
5.3 Qualitative Case Study 81
5.3.1 Context – General Banking Sector in India 81
5.3.2 Design and Procedure – Case of a Public Sector Bank in India 82
5.3.3 Analysis and Findings – Security job performance in Alpha Bank 83
Determinants of Employee Competence 84
5.4 Emergent Conceptual Model and Hypotheses 88
5.4.1 Purposeful heedful interactions 88
5.4.2 Tacit knowledge 88
5.4.3 Explicit knowledge 89
5.4.4 Information security job performance 89

5.5 Empirical Analysis 91
5.5.1 Design and procedure 91
5.5.2 Analysis 92
Measurement Model 93
Structural Model 94
5.6 Contributions 96
5.6.1 Theoretical Contribution 96
5.6.2 Practical Contribution 98
5.7 Conclusion 98

CHAPTER VI: INTERPRETING IMPACT OF THRIVING AT WORK AND EMPLOYEE COMPETENCE ON INFORMATION SECURITY 100

6.1 Introduction 100
6.2 Evaluation of Thriving at Work and Agentic Work Behaviors 100
6.2.1 Thriving and information security outcomes 101
6.2.2 Agentic work behaviors 103
6.2.3 Individual enablers contribute to thriving 105
6.3 Evaluation of Employee Competence 106
6.3.1 A step beyond Security Education Training and Awareness (SETA) 106
6.3.2 Impact of employee competence on performance outcome 107
6.3.3 Competent employees and management 109
6.4 Conclusion 110

CHAPTER VII: CONCLUSION 111

7.1 Introduction 111
7.2 Overview 112
7.2.1 Thriving at work and agentic work behaviors 113
7.2.2 Employee competence 113
7.2.3 Summary of contributions of this research 114
7.3 Limitations of this research 116
7.4 Opportunities for future research 117
7.5 Summary 118

REFERENCES 119

APPENDIX A: MEASUREMENT ITEMS FOR THRIVING AT WORK STUDY 146

APPENDIX B: MEASUREMENT ITEMS FOR EMPLOYEE COMPETENCE STUDY 149

APPENDIX C: ITEM LOADINGS AND CROSS-LOADINGS FOR THRIVING AT WORK STUDY 151

APPENDIX D: ITEM LOADINGS AND CROSS-LOADINGS FOR EMPLOYEE COMPETENCE STUDY..... 153

LIST OF TABLES

Table 1. Summary of Information Security research 22

Table 2. Summary of Behavioral IS security research on human factors 29

Table 3. Sample interview quotes for emergent concepts: Thriving at work 64

Table 4. Summary of hypotheses: Thriving at work 68

Table 5. Descriptive statistics, correlation, composite reliability (CR), and average variance extracted (AVE) 71

Table 6. Heterotrait-Monotrait (HTMT): Thriving at work 72

Table 7. Bootstrapping result for structural model: Thriving at Work 74

Table 8. Sample interview quotes for emergent concepts: Employee competence 83

Table 9. Summary of hypotheses: Employee competence 90

Table 10. Descriptive statistics, correlation, composite reliability (CR), and average variance extracted (AVE) 93

Table 11. Heterotrait-Monotrait Ratio (HTMT): Employee competence 94

Table 12. Bootstrapping result for structural model: Employee competence 96

LIST OF FIGURES

Figure 1. Mixed-methods research design 47

Figure 2. Overall research design 48

Figure 3. Research methodology 49

Figure 4. Digital banking and services 51

Figure 5. Research model: Thriving at work 66

Figure 6. Structural model: Thriving at work 74

Figure 7. Research model: Employee competence 91

Figure 8. Structural model: Employee competence 95

CHAPTER I: INTRODUCTION

Today, majority organizations rely on information systems (IS) to manage their data and information which is huge in terms of volume and variety. One of the major challenges with this are the risks related to internal employees of the organization mishandling this sensitive and important information resulting in some risks and dire consequences, including corporate liability, loss of reputation and credibility, and monetary losses (Cavusoglu et al., 2004). One can easily say that ensuring employees fulfil their job responsibility through focused commitment towards how they handle and manage information has become one of the top managerial priorities in many organizations. Although research in IS has focused on information security and security performance of employees in the past, the primary focus has been on the technical issues concerning the design and implementation of the security systems such as advanced technical approaches to prevent intrusion into organizational systems and sophisticated firewall protection (Choo, 2011; Ayuso et al., 2012). Though the technical and technology-based solutions, which are more external in nature are important and, help in improving information security, relying on them entirely would not eliminate the information security completely (Dhillon & Backhouse, 2001; Siponen, 2005).

In this research we focus on the behavioral aspect of information security performance of employees. The overall objective of this research is to explore the factors that enhance the information security job performance using the conceptualization of *thriving at work*. To provide a comprehensive understanding on the concept of information security job performance, we conduct an in-depth case analysis in a large public sector bank in India. The banking industry in India is a relevant case as the employees handle sensitive customer and organizational information. These banks are required to have stringent Information Security Policies to ensure

compliance with the regulations of the Central Bank. However, more recently, these banks have started focusing on providing Information security trainings so that employees are confident and motivated to perform their job responsibilities. The banks are also keen on improving the abilities and competence of their employees to lower the information security incidents at various levels. Through this research, we help address this issue of improving employee competence and information security job performance.

The rest of the chapter explains the overall scope and significance of this study. Section 1.1 presents the problem domain followed by Section 1.2 where we elucidate the definitions of the main concepts used in this research. Section 1.3 describes the significance of this research followed by the scope in Section 1.4. Finally, Section 1.5 provides the overall structure of the thesis.

1.1 Problem domain

According to Haystax's crowd-based research1, employees and contract workers are one of the main causes of information security incidents in organizations after privileged users who have access to sensitive and important information and data. Although major organizations have stringent information security policies in place, still it is believed that the threat posed by regular employees is on a rise as more employees are accessing the sensitive data and networks. Internal employees are individuals (e.g., full-time employees, contract workers, part-time employees, temporary staff) who have access to relevant and sensitive information of the organization as part of their job profile and duties. An organization's information security would be impacted to a great deal by the intentional and non-intentional ways in which information is handled and

[1] http://haystax.com/wp-content/uploads/2017/03/Insider_Threat_Report_2017

managed by the employees while performing their jobs (Im & Baskerville, 2005; Vroom & von Solms, 2004). There are numerous instances where regular employees have inadvertently and without malicious intent caused a data breach (for instance, the Federal Deposit Insurance Corp. data breach in 2016[2], Home Depot data breach in 2014[3]). Given the fact that close to 51 percent of information threats are posed by internal employees, it is crucial to understand how the security job performance can be enhanced to mitigate such threats.

Organizations invest significant resources to keep their data secure. A Gartner report suggests that in 2021 nearly $150.4 billion was spent worldwide to ensure security (Gartner Report, 2021). This figure grew from $123.8 billion in 2020 (Gartner Report, 2021). Despite increased investments cybersecurity incidents and data breaches have been on an increase. A case is point is the Colonial pipeline ransomware attack[4], which highlights the lack of competence and poor job performance. The breach highlights the lack of competence of employees, highlighting poor job performance. The IT employees did not understand the importance of password security and lacked the ability to manage passwords. A Virtual Private Network (VPN) password was never changed, became available on the darknet, which the perpetrators used to gain access resulting in a ransomware attack. The hackers gained access to the Colonial Pipeline's network through a compromised password of a virtual private network (VPN) account which the employees used to remotely access the company's computer network. Although it is not known how the hackers obtained the correct username of the VPN account,

---

[2] https://www.washingtonpost.com/news/powerpost/wp/2016/04/11/inadvertent-cyber-breach-hits-44000-fdic-customers/

[3] https://www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets/?sh=512220fc3e74

[4] https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

they were able to use the password – obtained from the Dark Web- as the employee had not used multifactor authentication, a basic cybersecurity practice and tool. This means that secondary checks - encouraged in organizational security policies - such as security codes sent to mobile phones were not set up by the employee. Therefore, extensive cybersecurity policies are not enough. Now, more than ever, employees need to be competent towards their information security roles and responsibilities, like taking the time to come up with stronger passwords in the Colonial case in order to protect the company's information assets. The Colonial cyberattack also brings out the importance of evaluating the information security job performance of employees based on their responsibility to implement and strengthen the security policies. cyberattack caused a widespread panic over the availability of gasoline across Southeast region of US followed by the cyberattack on a meat processing company that disrupted the company's operations across three countries. Simply put, cutting-edge cybersecurity practices and policies aren't the only solution for information protection.

Organizations must also recognize the role and responsibilities of their employees in information protection. Clearly, there is a gap between the performance of the employees to keep the sensitive information secure which is part of their basic job responsibilities in most organizations that handle data and information. The growing challenge is that almost every employee has an element of information security built into their performance indices but there can still be human lapses. Furthermore, in the work from home scenario, employees have access to data and information with enough protocols and trainings in place. One wrong click can lead to a security threat thereby damaging the entire security ecosystem. Hence, there is an urgent need to focus on the concepts of employee competence and information security job performance.

1.2 Definitions

In this research, we focus on four broad conceptual frameworks. These conceptual understandings are derived from prior research and practice in IS and are the foundation for subsequent chapters.

Information Security Job Performance. This research is focused on the understanding that behavior of employees towards their information security job responsibilities is crucial for the overall information security performance of the organization. One of the primary goals of the organizational scientists is to maximize the employee behavior to achieve the overall organizational goal. However, the domain of information security this translates into employee behavior towards their information security job responsibility. In the domain of organizational studies, employee performance has been one of the most researched outcomes along with psychological resources (Avey et al., 2011). It includes multiple characteristics of performance, such as, performance in sales, related to quality and quantity of manufacturing, and performance in creative tasks, to name a few. In most research, the consistent theoretical proposition is that the mechanisms of psychological resources like self-efficacy, optimism etc., act as individual motivational factors and help in inclination towards effort to succeed. This further results in increased performance outcome. To further understand the broader concept of performance, scholars have used the task proficiency in the job-related roles a measure for evaluating performance. In this research, we explore information security job performance as the execution of information security work tasks with efficiency and precision.

Thriving at Work. As the focus for information security within an organization shifts towards individual and organizational perspectives, the behavioral, philosophical, and psychological aspects of the employees emerge as the key point of understanding. Drawing

insights from the theories of self-adaptation (Tsui & Ashford, 1994), one can argue that information security job performance of employees could improve if employees thrive at work. Thriving is an important domain of inquiry as it is a subjective experience that allows employees to ascertain whether what they are doing and how they are doing it is helping them to develop in a positive manner and become better at their respective jobs and duties. We focus on thriving at work because of two main reasons. Firstly, people are devoting increasing amounts of their time to the work domain of their life and sometimes find work even more attractive relative to home life (Hochschild, 1997). Secondly, in today's information driven world, most of the job roles and profiles have an element of information security related to it. For instance, from IT and information security personnel to data entry operators all employees must log out of their work machines before leaving their desks and refrain from sharing their passwords with other colleagues for convenience. Thriving at work is a psychological state in which individuals experience a sense of vitality and learning at work. Vitality refers to the positive feeling of having energy available to do a certain task which is related to hedonic perspective of psychological development (Nix et al., 1999). It reflects feelings of aliveness in an individual which further helps them grow in work. Learning refers to the sense that one is acquiring, and can apply, knowledge and skills. Through learning, individuals seek to realize their full potential as human beings. Thriving encompasses the joint sense of vitality and learning, which communicates a sense of progress or forward movement in one's self-development. The subjective psychological experience of thriving is essential and interesting as it encompasses both the affective (vitality) and cognitive (learning) dimensions of psychological experience.

Agentic Work Behaviors. Bandura (2001) explained that when individuals act agentically, they are intentional and in control of their own behaviors. Such intentional, self-directed

behavior is more likely to lead to feelings of vitality and the experience of learning at work than reactive, prescribed behavior (Spreitzer & Porath, 2012). This is because, as Bandura (2001) noted, "the capacity to exercise control over the nature and quality of one's life is the essence of humanness" and will therefore be associated with the zest for life and aliveness that is inherent in vitality. Individuals who are self-motivated and agentic at work are also likely to experience learning at work because they are open to finding new ways of doing things rather than just "doing what they are told."

Competence. Over the past several decades there has been research pointing to information security breaches because of inability of employees to adequately perform their work. Such studies have largely suggested extrinsic or intrinsic motivational strategies to ensure compliance with stated security policies. Competence as a concept has been studied well in the organizational behavior field but has not been explored in the context of information security. Furthermore, the National Institute of Cybersecurity Education (NICE) also elaborates that information security competency of employees is crucial when it comes to organizational development. However, there is still a limited understanding of how organizations can enhance the security competencies of their employees. This is crucial as the lack of these competencies can pose major security threats for the organization. This is evident for the fact that although organizations educate and train their employees on security best practices and have elaborate information security policies in place, organizations lost close to 6.3 billion USD due to security issues (2016 ACFE Report to the Nations).

While studies have acknowledged the importance of security education, training and awareness (SETA) programs, there has been limited emphasis on developing competent individuals who perform *par excellence* relative to their security jobs. In this research we argue

that individual security competence leads to superior security job performance. Drawing on the extant literature in this research we also argue that competence is an idiosyncratic combination of what Weick and Roberts (1993) terms as *know-how* and *know-that.*

1.3 Significance of this Study

There is a growing need to understand how organizations can have employees who can excel in their information security job responsibilities. Events that highlight this growing need are:

- The growing concerns of Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) for hiring competent employees
- Industry practitioners claiming the Information Security Awareness and Trainings are not sufficient for reducing security risks and changing employees' security behaviors
- National Institute of Cybersecurity Education (NICE) highlighting that information security competency of employees is crucial for them to perform their job responsibilities.

This increasing need emphasizes the importance of deeper understanding of how the information security job performance of employees can be enhanced. In the past, organizations have been investing huge financial capital on information security awareness and training programs to ensure that employees have relevant knowledge and skills to perform their information security jobs. However, industry practitioners claim that these trainings are not sufficient.

Despite rigorous empirical research in the domain of information security, the focus has generally been on evaluating the compliance of individuals to the Information Security Policy of

the organization. Although compliance is an integral element of information security behavior of employees, it might not be able to fully identify the performance outcome. Similarly, information security scholars have also rightly focused on employees' motivational aspects to predict the information security outcome of individuals. However, information security job performance and its antecedents are much less studied.

To a large extent, this research is a response to the growing need for ensuring that employees excel in fulfilling their information security job responsibilities.

1.4 Scope of this Research

This research falls within the broad domain of 'Human and Behavioral factors of IS security'. However, the focus of this research is specifically on IS security performance of employees. Typically, employee performance towards their job responsibilities is improved by providing them enough trainings so that they develop the necessary knowledge and skills. Furthermore, outcome behavior can also be deliberated through extrinsic motivational factors such as incentives, rewards, etc. In practice, many organizations claim do have specialized information security awareness and training programs in place, but practitioners are beginning to question if there can a 'one-size-fits-all' approach for these trainings across different groups of employees. Although the discussed factors do contribute to performance improvement, practitioners of information security are looking to further explore the factors of ability and competence among the employees.

While the long-term ongoing research goal is to evaluate and enhance the employee behavior towards information security for the comprehensive information security goal of the organization, the scope of this thesis is focused on examining the factors contributing to information security job performance and employee competence. More specifically, this research

comprises of two broad dimensions. The first dimension involves exploring the impact of thriving at work and agentic work behaviors on information security job performance. 21 full-time employees, across three groups (branch managers, IT executives and retail banking executives) working in a large public sector bank were interviewed to identify the antecedents and for developing a research model. The model was empirically tested using the responses from the bank employees. The second dimension focused on the understanding how organizations can build competent employees who have the ability and caliber to excel in their information security job responsibility. 16 supervisor level employees of the same bank were interviewed as part of a case study to explore the factors that could improve employee competence. The research model was developed based on the case study and was empirically tested through the responses of bank employees (supervisors and retail officers).

1.5 Structure of this Thesis

This section summarizes the content of the chapters that follow. The thesis is laid out in seven chapters.

Chapter 1 introduces the research topic and explains the problem that the research addresses to answer. The significance of the research is highlighted along with providing detailed definition of four essential concepts utilized in this research. The section on scope of the research indicates the boundaries of this research.

Chapter 2 presents a review of the literature relevant to the topic of information security and performance. This chapter describes the state of information security research with emphasis scholarly work that focuses on performance as an outcome. The literature on information security is considered under two broad frames for this thesis – that which focuses on thriving at work and the other that pivots around competence and capability. The aim of this review is to

identify the potential gap in the literature and to validate the contribution of this research to both information security theory and practice.

Chapter 3 outlines the theory and conceptualization that underpins and informs the design of this research. This chapter also describes the methodology adopted and the methods used empirically validate and address the research questions.

Chapter 4 describes the first dimension of this research – the impact of thriving at work and agentic work behaviors on information security job performance. This is a detailed account of the research processes that were undertaken to develop the conceptual research model and to empirically test the model. The empirical analysis includes using Partial Least Square based Structural Equation Modeling. Examples of the interviews with the bank employees is also presented in the chapter.

Chapter 5 presents detailed findings of the second dimension of this research – exploring antecedents of employee competence and its impact on information security job performance. This chapter includes a detailed account of the in-depth case study conducted in a large public sector bank in India. A conceptual model is developed based on the case study that is further empirically tested. Data analysis of the quantitative study is done using Partial Least Square based Structural Equation Modeling.

Chapter 6 describes the contribution and implications of studies presented in Chapters 4 and 5. This chapter also extends the discussion on how the two studies answer the broad research questions towards understanding the factors for information security job performance. The findings are also discussed to highlight the contribution to information security theory and practice. The limitations of this research are also presented in this chapter.

Finally, Chapter 7 concludes this thesis by providing an overview of why this research was undertaken, how it was done and how this research contributes to extending information security theory and practice. The methodological contribution of this research is also highlighted in this chapter. The chapter also includes future development of research on information security performance and the resultant research opportunities.

CHAPTER II: A LITERATURE REVIEW OF INFORMATION SECURITY RESEARCH IN INFORMATION SYSTEMS

2.1 Introduction

This chapter reviews prior literature in the field of information security and performance outcomes of information security that is relevant to the topic of this research. The aim of this chapter is to report the literature in the field of information security and the various aspects of performance outcomes. The literature review also presents and identifies the prior contributing research and the future research needs. This approach helps confirm the need of this research by identifying the gap in the literature. The overall research question that this addressed by this research is:

> What are the factors that can enhance the information security job performance of employees in a work situation and understanding the influence of thriving at work and employee competence on information security job performance?

There has been evolving research on the philosophical and psychological dimensions of employee behavior towards their security job roles and responsibilities within organizations. Scholars have argued that in order to encourage employees to perform their security behaviors more efficiently, better ISPs need to be put in place. However, there are two main dimensions that need more elaborate understanding. First pertains to the fact that information security job performance is a multifaceted construct and needs deeper understanding based on both subjective and objective dimensions of employee performance. Secondly, as better performance is a more internal perspective of an individual, psychological capital comprising of hope, self-efficacy, resilience, and optimism would help in better understanding of how the desired outcome of

improved security job performance can be achieved and sustained among employees. In the paragraphs below, while discussing the extant literature on information security job performance and thriving at work, we evaluate the mentioned gaps in literature.

The structure of this chapter comprises three broad sections. The first section explains the extant research undertaken in the domain of information security with special emphasis on performance outcomes like attitude and compliance behavior. The second section is a review of the literature with reference to conceptualizations of thriving at work, including the dimensions of learning and vitality, in the context of information security. And the final section is a review of the relevant information security research literature related to behavioral aspects that emphasize the conceptualization of employee competence and factors that have been studied that could lead to employee competence.

2.2 The State of Information Security Research and Performance Outcomes

Information security is an ever-present problem for organizations and their end-users, namely the employees, the customers, the vendor and suppliers etc. Information systems scholars over the decades have explored many factors, both technical and non-technical, that can play a crucial role in solving this problem. However, the 'human factor' in information security research is less focused on than its technological counterpart. Researchers have also found that the size of the organization or the industry that the organization caters to, do not play a role. Information security incidents have impacted small businesses to big industrial giants across the globe. Similarly, these information incidents, including ransomware and data breaches have targeted organizations across industries including healthcare industry, educational institutions and government agencies. Information security is thus a topic of concern across a wide spectrum of organizations.

Information security is also not restricted to geography. Countries like the United States and Singapore are equally prone to attacks by cybercriminals who might use technological or non-technological sources to expose individual or organizational data and information. There have been incidents where personally identifiable information of individuals, sensitive patent data of organizations as well as personal health information of individuals has been compromised during these information incidents. Indeed, most organizations today have access to or possess sensitive customer information like financial data records, payment card data, medical records etc. along with organizational information like intellectual data or corporate information. Information security incidents within organizations include not just the organization but also the employees who have access to this information or are handling this information. The information security rules have become more diluted during the COVID-19 pandemic where a large majority of organizations shifted to hybrid mode of working or completely work from homework style. The risk of information security incidents is higher when employees are not competent of handling these uncertain situations and might lack the confidence and self-efficacy to handle these information security challenges.

Human and behavioral information security research is a subfield of the broader information security field that focuses on the behaviors of individuals which relate to protecting information and information systems assets, which includes computer hardware, networking infrastructure, and organizational information. A plethora of studies have been published about the behaviors of individuals in protecting these assets. These studies include those that provide insight into insider abuse of information systems (Siponen & Willison, 2009; Willison, 2006; Willison & Backhouse, 2006), as well as applying General Deterrence Theory (GDT) to understand human behavior as it relates to computer crime and intentional abuse (Straub &

Welke, 1998). Further studies have adapted Protection Motivation Theory (PMT) to understand the behaviors of individuals when it comes to the performance of a number of security measures, such as the use of anti-malware software (Johnston & Warkentin, 2010; Lee & Larsen, 2009; Liang & Xue, 2010), compliance with security policies (Herath & Rao, 2009), backing up data (Crossler, 2010), properly securing home wire-less networks (Chan et al., 2005), and adoption of anti-plagiarism software (Lee et al., 2016). Beyond PMT, other empirical studies exist that investigate behavioral factors that affect such areas as security policy compliance (Bulgurcu et al., 2010; Herath & Rao, 2009; Hu et al., 2011, 2012; Siponen & Vance, 2010; Warkentin et al., 2009), information systems misuse (D'Arcy & Hovav, 2007; D'Arcy et al., 2009; Posey et al., 2011), and computer abuse (Posey et al., 2011).

In the behavioral information security literature and industry surveys of IT managers, it is well acknowledged that people within organizations are still the weakest link in the defense against internal and external threats to organizational digital assets in spite of the significant advances in protective technologies and organizational procedures and policies related to information security (Hu et al., 2012; Warkentin & Willison, 2009). Many of the headline security breach incidents would have not been possible without some intentional or unintentional actions by the insiders. In fact, surveys suggest that more information security breaches are caused by the actions of internal employees than by outside hackers. The insider actions that cause direct or indirect threats to organizational digital assets can be classified into two categories: those that are intentional, often labeled as deviant behavior such as sabotage, stealing, and industrial or political espionage and those that are unintentional, often labeled as misbehavior such as selecting a simple password, visiting non-work related websites using corporate computers, inadvertently posting confidential data onto unsecured servers or websites,

or carelessly clicking on phishing links on emails and websites (Guo et al., 2011; Stanton et al., 2005; Willison & Warkentin, 2013). A significant number of information security studies have been conducted investigating the effectiveness of deterrence (D'Arcy et al., 2009; D'Arcy and Hovav, 2007; D'Arcy et al., 2019; Herath & Rao, 2009a; Siponen et al., 2007) on deviant insider behavior. Recently, other cognitive and psychological factors have been included in the increasingly complex insider behavior models, such as rational choice and beliefs (Bulgurcu et al., 2010), neutralization (Siponen & Vance, 2010), fear (Johnston & Warkentin, 2010), self-control and moral beliefs (Hu et al., 2011a; Myyry et al., 2009), accountability (Vance et al., 2011, 2012a), disgruntlement (Willison & Warkentin, 2013), and leadership and organizational culture (Hu et al., 2012).

The findings of such studies have significantly advanced the understanding of insider motivations and psychological processes when evaluating whether or not to comply with established information security procedures and policies. However, in most of these studies no attempt was made to differentiate between the survey samples drawn from those who intentionally violate the procedures and policies and drawn from those who unintentionally violate them. Differentiating these samples is important as the causes of intentional violations of policies likely differ from the causes of unintentional violations, although the outcomes can be just as damaging. For example, deviant insider behavior can cause significant direct damages to organizations, such as loss of revenue, weakened competitive positions, and loss of credibility. On the other hand, insider misbehavior can be equally as damaging, but most often indirectly by creating security weakness that allow outside hackers to invade internal systems, such as infecting corporate computers with Trojan viruses and spyware that allow hackers to bypass the firewall defense and access confidential data.

In the domain of organizational sciences, scholars have defined and studied job attitudes both as a means to an end (i.e., a mechanism for increasing job performance) and, also as an end (or outcome) by itself. This is because job performance of employees is influenced to a great extent by the attitudes they have towards their jobs. According to Aurigemma & Leonard (2015), the research around the concept of job attitude is one of the top topics of investigation in the field of organizational science. Furthermore, Ajzen's (1991) Theory of Planned Behavior has been widely used to explain the concept. According to this theory, behavioral intentions of individuals can be predicted based on attitude. Along with attitude, perceived behavioral control and social norms also influence behavioral intentions. In the domain of organizational sciences, job satisfaction, organizational behavior (Dalal, 2005), and counterproductive work behavior (Dalal, 2005) are some of the concepts that have been found to predict overall job performance. Thus, employees' attitudes toward information security are likely to inform organizations about subsequent information security related behavior as well as help in improving their efficiency and precision towards their information security job roles and responsibilities.

Although job attitudes have been an important research topic in the domain of organizational science, there has not been much research to focus on the factors that could impact the actual work performance related to information security tasks in a work environment. Furthermore, most scholars have focused on the aspect of information security policy compliance which might not be equivalent to actual performance of the information security tasks. For instance, employees might be very well aware of their organization's information security policies and procedures, but that knowledge might not translate into actual behavior and performance. However, researchers have focused on information security perceptions and the adoption of information security policies by organizations or their employees using the

Technology Acceptance Model (e.g., Doherty & Fulford, 2005; Crossler et al., 2014). This model posits that perceived ease of use and perceived usefulness are key in the adoption of technology (David, 2002). Scholars such as Hentea (2005) also argue that constructs like attitude and perceptions are not the same. Some prominent scholars have also studied perceptions of usefulness and ease of use to measure attitudes toward information security policies and procedures. Therefore, there are a wide range of constructs that have been explored and that contribute to the understanding of attitudes towards information security policies and procedures.

2.3 Thriving at Work and Information Security Research

In complex organizations, it is often difficult to assess and measure the job performance of individual employees. One can argue that depending on the domain and requirements of an industry, work outcomes may be dependent on various interdependent work processes. According to Meyer et al. (1989), has been conceptualized as an individual's overall performance or task proficiency. Research related to job performance mostly includes subjective as well as objective measures of job performance which are often measured using supervisor ratings and individual assessment respectively (Siders & George, 2001). In the context of information security, job performance includes the proficiency related to the security component of one's job.

Most organizations now recognize that their employees can be the greatest asset to reduce the risks related to information security (Bulgurcu et al., 2010), but can often also be the weakest link that could pose enormous threats to the organization. In recent times, we have witnessed that due to shifting focus on employees, organizations have been creating and upgrading their information security policies (ISPs) so as to provide better guidelines to their employees to ensure information security. Organizations perhaps believe that more elaborate and employee

focused ISPs are the key socio-organizational resource (Boss & Kirsch, 2007; Siponen et al., 2007) that would lead to improved compliance and fix the weakest link in information security (Warkentin & Willison, 2009).

However, while creating guidelines and policies is an essential starting point, it is not enough to ensure employees' compliance with them. Therefore, an understanding of what factors motivate employees to better perform their security jobs and further comply with their organizations' security policies crucial to understanding the what factors impact employees' information security job performance. This would further help the information security managers to understand what factors influence this performance and how this behavioral issue could be sorted by the information security management. This is interesting because despite the fact that most organizations have stringent information security policies and procedures in place, data breaches and information security incidents are on the rise. Therefore, scholars have started to shift focus on the human perspective of information security job performance. These factors evaluate the behavior of employees along with identifying the factors that lead to information security compliance behavior. According to the literature, most organizations today access to crucial and sensitive information to their employees (Neumann et al., 1999). These employees could potentially pose a threat for the organization if they are not cognizant in the ways they handle this sensitive and crucial information (Siponen et al., 2007). According to an FBI survey, 64 percent of the respondents reported that some of the losses related to information security have been incurred due to the mishandling of sensitive and crucial information by the employees.

Even though most of the information security literature regarding employee performance has focused on abusive behavior and has considered employees to be potential information security risks, it has also recognized that employees can help organizations safeguard

information and technology resources by performing beneficial acts. To encourage such acts, organizations often put together an ISP that stipulates what roles employees should play that is part of their information security job profile or duty. However, the simple existence of these policies does not automatically translate into desirable behaviors because employees may not be motivated to perform the activities required to protect their organization's information and technology resources (Stanton et al., 2005).

Many prior studies have argued the deterrence effects of sanctions could be employed by organizations to discourage employees from diverging from their security behavior at workplaces. Boss & Kirsch (2007) introduced the concept of mandatoriness, which has been shown to motivate individuals to take security precautions. While rewards have not been found to be effective in convincing individuals that security policies are mandatory, specifying policies, evaluating behaviors, and computer self-efficacy have been effective. Later, Boss et al. (2009) showed that mandatoriness mediates the relationship between the control element (specification, evaluation, and reward) and security precautions taken. Pahnila et al. (2007) proposed a theoretical model in which they found that information quality had a significant effect on actual compliance, threat appraisal and facilitating conditions had a significant effect on attitude toward compliance, and sanctions and rewards did not influence intention to comply or actual compliance. In an attempt to understand end-user behaviors in regard to computer technologies that protect data and systems from security-related threats (i.e., protective information technologies), Dinev et al. (2008) posited that cultural differences moderate the strength of such technologies. Myry et al. (2009) suggested that moral reasoning and employees' values can explain their adherence to information security policies and showed that moral reasoning and values explain employees ' adherence to an information security rule prohibiting password

sharing. Herath & Rao (2009), drawing on protection motivation theory which was developed to understand how fear appeal motivates health behavior argued that an employee's attitude toward adopting security technologies and practices is shaped by threat appraisal and coping appraisal processes. They also found that factors rooted in protection motivation theory influence employees' attitudes toward adopting information security procedures and policies.

Finally, despite the importance of information security job performance, there is a paucity of empirical studies that analyze the impact of psychological capital and agentic work factors on information security job performance. Siponen (2000) conceptually analyzed information security awareness and suggested methods to enhance awareness based on several theoretical perspectives. A few conceptual studies (Furnell et al., 2002; Hentea, 2005) have highlighted the importance of information security education and training. Furthermore, D'Arcy et al. (2009) found that organizations can use three security countermeasures-user awareness of security policies; security education, training, and awareness (SETA) programs; and computer monitoring-to reduce user's IS misuse that these measures helped in reducing the information systems misuse intention among users. Table 1 presents a summary of some of the seminal research on information security.

Table 1. Summary of Information Security research

Author/Paper	Theoretical base	Constructs examined	Key findings
Herath & Rao (2009)	Deterrence theory, protection motivation theory	Detection certainty, normative beliefs, punishment severity, response efficacy	Resource availability is a significant factor in enhancing self-efficacy and is a significant predictor of security policy compliance by employees.

Zhang et al (2008)	Risk compensation theory, theory of planned behavior	Attitude and normative beliefs influence the self-efficacy of individuals	Supervisors play a synergistic role by accentuating the positive influence. Results reinforce the importance of both structural and social processes in cultivating employee-organization relationship.
Warkentin et al. (2009)	Social learning theory	Self-efficacy	Findings show that development of policies to improve security practices is improved by comprehensive understanding of how employees perceive security threats.
Siponen et al. (2005)	Protection motivation theory, theory of reasoned action, cognitive evaluation theory	Attitude, normative beliefs, resource vulnerability, response efficacy, rewards, self-efficacy, threat severity	Intrinsic factors such as weakness of will were found to occur widely among individuals, particularly men. It suggests that individuals have different attitudes towards resources and their unauthorized use.
Pahnila et al. (2007)	Protection motivation theory	Resource vulnerability, response efficacy, self-efficacy, threat severity	Threat appraisal and facilitating conditions have significant impact on attitude towards information security policy compliance. Sanctions have insignificant effect on intention to comply with IS security policy.
D'Arcy & Hovav (2007)	Deterrence theory	Detection certainty, punishment expectancy, punishment severity	Results suggest that users' awareness of security-policy statements and guidelines decreases the likelihood that they will engage in IS misuse.

Dinev et al. (2008)	Theory of planned behavior	Attitude, normative beliefs, perceived ease of use, perceived usefulness, self-efficacy, SETA	The perceived need for surveillance is negatively related to privacy concerns and positively related to willingness to disclose information.
Boss et al. (2009)	Social influence theory, organismic integration theory, agency theory, control theory	Detection certainty Reward	The acts of specifying policies and evaluating behaviors are effective in convincing individuals that security policies are mandatory. This perception is effective in motivating individuals to take security precautions.
Bulgurcu et al. (2010)	Theory of planned behavior, rational choice theory, deterrence theory	Attitude, normative beliefs, perceived benefits, punishment expectancy, rewards, response cost, resource vulnerability, self-efficacy, SETA	Information security awareness positively affects both attitude and outcome beliefs of employees following their organizations' information security rules and regulations.

Agentic Work Behavior

Bandura (2001) explained that when individuals act agentically, they are intentional and in control of their own behaviors. Such intentional, self-directed behavior is more likely to lead to feelings of vitality and the experience of learning at work than reactive, prescribed behavior (Spreitzer & Porath, 2013). This is because, as Bandura (2001) noted, “the capacity to exercise control over the nature and quality of one’s life is the essence of humanness” and will therefore be associated with the zest for life and aliveness that is inherent in vitality. Individuals who are self-motivated and agentic at work are also likely to experience learning at work because they are open to finding new ways of doing things rather than just “doing what they are told.”

2.4 Employee Competence and Information Security Research

In today's digital world, keeping sensitive customer and organizational information secure is one of the top priorities of organizations in order to protect them from being exposed to a malicious security incident or breach. Organizations continuously struggle to keep this information safe and in turn make huge investments into technological countermeasures (Spears & Barki, 2010). However, merely focusing on the technical aspects of information security is not enough as information security is multidisciplinary in nature as the human aspect plays a major role in it (Stahl et al., 2012). In other words, employees of the organization do play a critical role in keeping the information of the organization secure and therefore need to be competent in doing so (Siponen and Vance, 2010). ENISA (2019) indicated that about 77% of the companies' data breaches are due to exploitation of human weaknesses. It has also been found that over half of all information incidents involved employees' poor information security compliances and competencies (Humaidi and Balakrishnan, 2015; Waly et al., 2012).

Employees of an organization are very often unconsciously incompetent when it comes to information security practices. They are not aware that they are unskilled in terms of information security. ISP compliance research suggests that the information systems (IS) users make own decisions in their everyday tasks about complying, or not complying, with ISPs in order to protect IS resources. For example, Bulgurcu et al. (2010) use the neoclassical economics rational choice theory and demonstrate that individuals make rational decisions about complying (or not) with security policies, based on the perceived benefits and costs of the compliance/non-compliance behavior (e.g., sanctions). Ng et al. (2009) also advocate that end users make a conscious decision to comply (or not comply) with ISPs, based on the way that they perceive benefits and barriers, own efficacy and other parameters. In another example, scholars (Vance et

al., 2012; Herath and Rao, 2009; Ifinedo, 2012; Siponen et al., 2010) use Protection motivation theory (Vance et al., 2012) and show that individuals make own assessments in threat situations in order to decide if they think that it is necessary to take actions for protecting information assets by complying with the security policy.

On an individual level, competency is used in multiple disciplines to describe a wide range of characteristics related to job performance (McClelland, 1973). Hereby, job performance is commonly defined as "the total expected value to the organization of the discrete behavioral episodes that an individual carries out over a standard period of time" (McClelland, 1973). Accordingly, job performance describes behaviors prescribed by the role in the organization (Katz & Kahn, 1978). Thus, competency can be understood as characteristics of an individual directly influencing the behavior. However, in the field of information security, there is no consistent understanding of what these individual characteristics are (Schippmann et al., 2000). Most existing researchers include knowledge, skills and abilities within the context of competence and argue that these individual characteristics (Cheney et al., 1990; McClelland & Boyatzis, 1982). Some other authors include aspects such as motives, traits or attitudes that impact and predict behavior of individuals (Boyatzis., 2008) while others define competency directly as actual behavior (McClelland, 1973). Based on an extensive literature review, Holtkamp et al. (2014) define competency as a set of knowledge, skills and attitudes to solve a problem in a given context. They defined the term competence as a single stance of competency to fulfill a single task in a given context where knowledge addresses content or technical information that is required to perform a job, skills refer to psychomotor processes manifested in behaviors, and abilities refer to cognitive factors or behaviors that can be seen as the result of personal traits (Cheney et al., 1990; Boyatzis., 2008).

In the organization strategy literature, competence is studied at an organizational level and includes the aspect of developing core abilities through combining processes and resources that could ultimately help the organization gain some competitive advantage (Andreu & Ciborra, 2009). Among prominent organizational studies scholar, McGrath et al. (1995) argued that individual know-how and skills were important elements that linked competence that was crucial to achieve the competitive advantage. Following this argument Weick & Roberts (1993) suggested that another important concept that was important for overall strategic success was purposeful heedful interactions. These interactions are attentive, purposeful, conscientious and considerate (Cohen. 1994). More heedful interactions with other members would result in reduced process errors and more effective adaptation to unexpected events (Weick & Roberts, 1993).

The main strategy organizations utilize to influence employees' information security behavior is security education, training, and awareness programs. The goals of such programs include making employees aware of existing threats to the organization, training employees to perform their cybersecurity roles, and discussing the content of organizational information security policies (Burns et al., 2018; D'Arcy et al., 2009; Straub and Welke, 1998). At least in the U.S., organizations have largely relied on checklists derived from various governmental and industry specifications (e.g., the Federal Information Security Management Act) to inform their decisions regarding employee training, and both the content of these interventions and the frequency with which they are deployed are far from standardized (Yan et al., 2021). A sole focus on complying with government and industry mandates creates a checklist compliance culture (Vance et al., 2012); compliance is not synonymous with risk or harm mitigation (Burns et al., 2018). This area has been well explored by information system scholars specifically

answering the question around the effectiveness of training and other behavioral interventions. For example, some researchers are exploring how to effectively transition an organization steeped in a "checklist compliance" culture to one actively and iteratively attempting to improve protection of important organizational assets. Moreover, because information security is often viewed as a part of the core job function and also a part of the job responsibility of many executive roles, one might want to dwell deeper on the efficiency and outcomes through these organizational security education, training, and awareness interventions. Research on questions such as these has the potential to benefit not just information security training, but also other training efforts studied by organizational scientists that may operate within a suboptimal regulatory compliance (vs. actual risk or harm mitigation) culture.

In addition, intervention research in the information systems is often limited by the ability to accurately and efficiently measure the behavior the interventions are designed to influence. For this reason, much of our knowledge of the effectiveness of interventions is based not on behavior but instead on knowledge tests and attitude measures. However, some of the behaviors included in the training objectives for information security are relatively easy to measure because they include concrete behaviors, such as changing a password, that are documented automatically through the organization's information technology system (e.g., do employees volitionally change their passwords more frequently than required by the organization—and, when they do so, how different are their old and new passwords?). The advantage of ready access to automatically documented behavioral outcomes could allow more robust tests of training intervention approaches, thereby generating new insights into how trainings and behaviors could be effective mechanisms to change behaviors and attitudes. If information systems employees become more knowledgeable about information security training and the

outcomes that can be captured automatically, it would lead to perhaps better performance and competence outcomes of the employees at the workplace. Table 2 provides a summary of the research on human behavioral factors in IS.

Although the conceptualization of competence is well established in the organizational studies literature, there is a limited understanding of this concept in information security. Therefore, in this research we explore the factors that contribute towards building information security competence that further impacts the information security job performance of employees so as to reduce the impact and occurrence of cybersecurity incidents.

Table 2. Summary of Behavioral IS security research on human factors

Thematic	Research focus	Theoretical base	Seminal Papers
INTENTION AND ATTITUDE TOWARDS INFORMATION SECURITY	Compliance intention	Deterrence Theory, Protection Motivation Theory	Herath and Rao, 2009; Bulgurcu et al., 2010; Dhillon et al., 2020; Hu et al., 2012; Pahnila et al., 2007
	Extrinsic motivation factors	Deterrence Theory, Rational Choice Theory, TPB	Bulgurcu et al., 2010; D'Arcy et al., 2009
	Intrinsic motivation factors	Self-efficacy Theory	Anderson and Agarwal, 2010; Herath and Rao, 2009; Rhee et al, 2009
	Psychological empowerment	Kanter's concept of empowerment	Dhillon et al., 2020
	Attitude towards information security	TPB, Cognitive Evaluation Theory	Bulgurcu et al., 2010; Siponen et al., 2005
WORK BEHAVIOR AND HABITS	Insider threat behavior	Causal Reasoning Theory	Posey et al., 2011
	Individual behavioral factors like employee	Conceptual framework	Stanton et al., 2006

	security accountability		
	Deviant insider behavior	Theory of Cognitive Moral Development	Hu et al., 2011; Myyry et al., 2009
	Employee habits	Protection Motivation Theory	Vance et al., 2012
SETA AND IS AWARENESS	SETA	Protection Motivation Theory, Expectancy Theory	Posey et al., 2015; Burns et al.,2018; Dhillon et al., 2020
	User Awareness	General Deterrence Theory	D'Arcy et al., 2009; D'Arcy and Hovav, 2007; Dinev and Hu, 2007
	Information security awareness	Conceptual foundation	Siponen, 2000
	Training programs	Elaboration Likelihood Model	Puhakainen and Siponen, 2010
OTHER FACTORS	Structures of Responsibility	Conceptual framework	Backhouse and Dhillon, 1996
	Normative beliefs	Deterrence Theory, Protection Motivation Theory	Bulgurcu et al., 2010; Dhillon, 2001; Herath and Rao, 2009; Siponen et al., 2005
	Cultural factors	TPB	Hu et al., 2012

2.5 Conclusion

This chapter presents a review of the literature that is believed to be relevant to this current research. It is structures into three broad domains which outline the relevant research that has already been conducted in this domain in information security and also bearing on the 'why' this current research was conducted. The three broad domains that have been covered in this chapter are namely, State of Information Security Research and Performance Outcomes, Thriving at work and Information Security, and Employee Competence and Information Security.

The review of the State of Information Security Research and Performance Outcomes revealed that there has been a plethora of research into the various factors that contribute to information security, including technological and non-technological factors. The 'human factors' in information security has been more focused on evaluating the habits, attitudes, and behaviors of employees. As an outcome measure, most research has evaluated the information security compliance behavior of internal members of an organization. However, through this research we evaluate the information security job performance as an outcome measure which is manifested as the execution of security work responsibilities with efficiency and precision.

The review of the literature on the conceptualization of thriving at work and information security research emphasized that learning has been studies in the prior studies, but it is focused on the security education, training and awareness programs. Prominent scholars and practitioners have acknowledged the contribution of these training and awareness programs but have also revealed that these education, training, and education programs sometimes do not converge into information security outcomes for the employees.

The information security literature has also focused on some conceptualizations related to improving employee competence but there has not been much substantial work on this topic. Prior research in this filed has focused on improving individual motivation through external and internal factors that could impact the employee attitude and behaviors towards compliance with information security policies of the organization. However, understanding and exploring employee competence as a factor that could enhance information security job performance is crucial as emphasized by the National Initiative for Cybersecurity Education (NICE) in 2020.

Therefore, this literature review provides a solid foundation of undertaking this research.

CHAPTER III: THEORY AND RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the informing theories and research methodology for evaluating the factors that impact information security job performance. Through the elaborate literature review presented in the previous chapter, we note that although information security scholars have rightly pointed to the various human and behavioral factors that contribute to the evaluates the antecedents of employee competence and its impact on information security job performance. For the purpose of this research, we have employed a sequential methodology approach where we develop the conceptualizations of thriving at work and employee competence through an in-depth case study undertaken in a large, nationalized bank in India. To empirically test our test our research model using a survey approach where the respondents are the employees from different managerial and work groups of the bank. The case study was done in a large public sector bank in India as the bank has been investing in digitalizing its operations and decentralizing its work. The supervisors and retail executives were interviewed to gain better insight into what according to them contributed towards improving their information security job performance. The public sector bank was chosen for the study because banking industry in India is increasing its digital presence among the customers due to which bank employees have access to sensitive financial information of the customers and the bank. The bank also has a stringent Information Security Policy in place which elaborates information security as part of their job responsibility.

The chapter has two broad focus areas, namely, the informing theories and the research methodologies. Section 3.2 presents the two main theoretical theories that inform this research.

Following sections provide an elaborate account of the research methodology employed in this research.

3.2 Informing Theories

3.2.1 Thriving at Work

In recent years, the conceptualization of thriving at work has received great attention in the field of organizational sciences as it focuses not just on doing a job well by an employee but on the aspect of human thriving (Roberts at al., 2005; Spreitzer et al., 2005, Spreitzer, 1995, 1996). The recent conceptual and empirical research on thriving suggests that when employees thrive at work, they feel a sense of progress and momentum in their work. Thriving is also related to a positive psychological feeling of competence and energy. Thriving is defined as a joint experience that employees witness through learning (growing and getting better at what one does with the job roles and activities) and vitality (feeling energized and positive at work) (Spreitzer et al., 2005). According to the researchers who have explored this concept of thriving at work, it is generally seen to enhance short-term individual functioning as well as long-tern adaptability at work (Spreitzer et al., 2005). For example, researchers have found that individuals who thrive at work are able to achieve higher organizational outcomes and also perform better in their individual tasks (Porath et al., 2012). Moreover, when employees report that they are thriving at work, they can adjust better to life challenges and changes (Spreitzer & Porath, 2012).

While there is research that emphasizes the contribution and effect of thriving at work on task performance and work outcomes, there are some differences that distinguishing ‘thriving’ from other related constructs like flourishing, resilience and well-being. According to Keyes and Haidt (2002), flourishing is related to a state of positive mental health where individuals are able to function to the best of their abilities both psychologically and socially. Flourishing as a sense

of psychological and social well-being is more focused on positive functioning as an outcome. Thriving, more particularly the sense of learning is in fact a part of flourishing. Therefore, one could say that it is possible to flourish without experiencing learning.

Second, thriving is distinct from resilience as resilience focuses more on rebounding in the face of an extreme situation or circumstance that poses a threat to statutory outcomes (Sonenshein et al., 2005). However, thriving can occur with or without being in an adverse situation. The main components of thriving are learning and vitality which can be experienced by an individual without encountering a significant hardship or challenge. For instance, resilience is part of a behavioral capacity of an individual that comes into play when one encounters a new opportunity at the workplace like being assigned a new project or handling a problem that they have not faced in the past (Roberts et al., 2005; Weick et al., 1999). Thriving on the other hand is related to a *psychological capacity* of increased learning and vitality that helps one develop and grow at work. This may include learning the skills and knowledge related to the work or that corresponds to different problem-solving strategies within the organization.

Third, thriving is conceptually different from well-being of individuals. According to Diener et al., (2010), well-being of an individual captures the emotional responses and overall levels of satisfactions of people towards their work, family, life etc. Well-being in general is kind of a scale that individuals might use to measure their overall positive condition in different aspects of life. Thriving, in contrast, is more specific with focus on the domains of learning and vitality. Furthermore, thriving captures both hedonic and eudaimonic aspects of the psychological functioning of the individuals.

Thriving is also distinct from Maslow's (1998) conceptualization of self-actualization. In his work, Maslow indicates that self-actualization only occurs when other needs like

psychological needs, needs of belongingness, safety and esteem are fulfilled for an individual. In fact, Maslow also posits that the percentage of self-actualized individuals is less than 5 percent. However, thriving is a more common and widely visible psychological functionality. Interestingly, Sonenshein et al., 2005 found that most people can identify and narrate some point in their life where they were thriving at work. Also, as thriving is composed of learning and vitality as its integral aspects, people can experience thriving even their other core psychological needs are not met. For instance, individuals can learn and thrive even when they are going through a phase of illness (Paterson et al., 2004).

Agentic Enablers of Thriving

For individuals to thrive in a work environment, Spreitzer (2005) highlights three agentic behaviors that act as an engine or enablers for inculcating thriving. These three enablers are *task focus*, *exploration* and *heedful interactions*. Task focus describes the degree to which individuals focus on the assigned work and responsibilities (Prem et al., 2017). Exploration is another enabler of thriving as it captures the discovery and innovative behaviors of individuals that help them innovate and grow in their work (Rahaman et al., 2022; Rego et al., 2021). Finally, individuals pay close attention to those around them. Heedful interactions happen when employees interact with others in the workplace by subordinating their idiosyncratic intentions to the effective functioning of the system (Weick & Roberts, 1993). In the paragraphs that follow, we explain how these agentic enablers can help employees experience thriving at work.

Task Focus: In order to fulfill the job responsibilities and work activities, employees must focus on the task at hand. This makes them feel that they are thriving at work. Task focus contributes to a sense of learning and vitality among employees. When employees focus on their assigned task and job responsibilities, they are likely to develop routines and capabilities in order

to do the task to the best of their abilities and make sure that they do their work effectively and efficiently. This step contributes to learning and a feeling of competence. On the other hand, a failure to meet the require task goals can lead to a sense of incompetence that is related to not learning. Task focus also promotes the experience of vitality. When employees focus on the tasks and activities assigned to them, they usually get absorbed in their work and feel energized (Şahin et al., 2020; Shahid et al., 2020 Ryan & Deci., 2001). Furthermore, when these employees are successful in completing their tasks and responsibilities, they are likely to feel a sense of accomplishment which also energizes them. This creates a sense of vitality. Not meeting their tasks goals can make them feel helpless and deplete their energies. Therefore, employees are more likely to thrive at work through task focus which is one of the engines of thriving.

Exploration: Employees are more likely to thrive at work when they engage in exploratory behaviors that inspires their curiosity and makes them feel energetic. When employees explore new ways of working, they are likely to come up with novel ideas and creative strategies for doing work. This exposure to novelty improves their energy and increases vitality (Spreitzer et al., 2005). Exploration also increases learning because when employees explore new ideas and strategies, they increase their knowledge and skills related to their responsibilities and activities. Interestingly exploration also helps employees learn through mistakes that they encounter during the process of exploring new ideas and strategies (Abid et al., 2021).

Heedful Interaction: The last enabler of thriving at work is heedful interaction. Employees experience thriving at work when they heedfully relate with their co-worker's and feel that they understand their job activities and responsibilities well. This further leads them to feel a sense of accomplishment of goals that are set by the organization. Heedful interaction can

promote learning as individuals heedfully relate to their co-workers and supervisors to explore the strategies and approaches used to fulfill the job roles (Bandura,1977). This gives the employees a sense of responsibility towards the larger organizational system and further challenges them to extend beyond the boundaries of their focused work responsibilities (Alikaj et al., 2021). Heedful interactions also promote vitality among employees as it enables them to help other co-workers and provide social support which further increases effectiveness and energy (Brown et al, 1991, 2003). Therefore, heedful interaction enables employees to experience both vitality and learning.

3.2.2 Psychological Capital

In today's competitive environment, organizations might find it challenging to gain competitive advantages by simply concentrating on traditional resources like advanced technologies, financial and economic capital etc. Competitive strategies that rely on improving and accumulating these traditional resources are perhaps no longer effective in providing a distinct advantage that organizations can sustain over a long term. This is specifically true when technology is also changing and improving at a fast pace. Today, employees within organizations have an added responsibility to keep the data and information secure in order to have an advantage over their competitors. Therefore, one can easily argue that an interesting and sustainable way to gain competitive advantage is through context-specific and hard-to-imitate factors (Luthans and Youssef, 2004). One of the ways to gain this kind of advantage is by investing in developing the psychological capital of individuals within on organization.

This psychological capital approach is based on research that posits that most organizations today are unable to utilize and capture the full potential of their work force (Avolio, 2005). Human resource is an indispensable resource that is part of most organizations

but unfortunately this resource is not effectively developed and managed. More so in the technology and information sensitive organizations, not much investment is being made to improve the competence of human resources through effective interactions with other core organizational values and practices (Bagozzi, 2011). As a result of less focus on the human resource factors and improving them further, information sensitive organizations fall prey to information related issues like data breaches and cybersecurity threats. Therefore, organizations today must recognize the need to develop competent human resource that is not just adequate in talent but is also competent and psychologically capable to manage the growing challenges of various industries. This new paradigm thinking will help researchers and managers find ways of enhancing notable 'competencies' among employees that cannot be copied easily by the competitors. Although organizations would still continue to invest in technical trainings and creative pay and benefit packages, but the need for a more consistent and integrated framework can be realized to a great extent through the context of psychological capital.

The concept of psychological capital is made up of the positive organizational behavior criteria meeting capacities of self-efficacy, optimism, hope, and resiliency. specifically, psychological capital is a higher order core construct that integrates the various positive organizational behavior criteria-meeting capacities synergistically. Therefore, the resulting impact of investing in and building the psychological capital of employees within organizations can lead to better performance, outcomes and improved attitudes among these individuals. Overall psychological capital is the sum of an individual's self-efficacy, optimism, hope, and resiliency. The positive psychological capacities under psychological capital are expected to have a significant impact on work and performance outcomes. Researchers who have studied psychological capital in the past posit that psychological capital does have performance

orientation on work related initiatives such as those coming out of positive organizational scholarships (Cameron et al., 2003). Research has also found positive organizational behaviors including psychological capital to demonstrate impact related to performance. In the nest paragraphs we will focus on the four dimensions of psychological capital self-efficacy, optimism, hope, and resiliency.

Self-Efficacy: Albert Bandura (1997) referred to the probability of how people take on a particular task as an estimate of their self-efficacy and further is also the probability of being successful in their endeavors. For instance, if we ask employees how capable they are to get their jobs done and to solve their problems and issues in new ways then their level of self-efficacy is the probability that these employees associate with doing the above tasks. Researchers have associated self-efficacy with a generalized level of recognition of handling challenges and tasks at the workplace (Parker,1997).

Psychological capital self-efficacy can be defined as "Once conviction about his or her abilities to mobilize the motivation, cognitive resources, and courses of action needed to successful execute a specific task within a given context (Stajkovic and Luthans, 1998 p.66). In the more applied domains like business performance, scholars like Kanter (2004) have also commonly used term confidence interchangeably with conviction. Self-efficacious people can be distinguished by these five characteristics: 1) They are highly self-motivated. 2) They thrive on challenge. 3) They set high goals for themselves and appreciate difficult tasks.4) They invest in necessary efforts to accomplish their goals., and 5) They persevere when they face obstacles. These five characteristics help employees with high efficacy to perform their job responsibilities independently and effectively and achieve individual and organizational goals. These employees are competent to overcome challenging goals that they set for themselves. Bandura (1988, 2001)

also found that emotions like self-doubt, negative feedback and repeated failures have little impact on highly efficacious individuals. This can be helpful within an organizational setting where job activities and responsibilities can get challenging due to factors like uncertain environments and changing industry regulations. One such prominent case in hand was the COVID-19 pandemic that forced employees to adapt to the challenging work from home scenario. The employees had to depend on their self- efficacy to ensure that they followed the information security policies to avoid any cyber security issues.

Optimism: According to most people optimism is related to positive and desirable events in the future. However psychological capital Optimism is not just about positive and good things but depends on the reasons and attributions an individual use to explain the positive or negative events in their lives. Based on his view researchers have argued that optimists are responsible for the positive happenings in their lives. Furthermore, optimists expect the desirable events to continue existing in the future and these events can be useful in handling other situations across different domains like work and related challenges. This optimistic style helps them internalize the good aspects of their lives. For instance, when optimistic employees receive positive feedback and recognition from their supervisor, they believe to be able to continue this positive movement in their work. They can assure themselves that they will be able to work hard and be successful not only in this job or in his particular activity, but also in any future endeavor. Similarly, when these employees receive negative feedback regarding a work, they can easily rationalize the negative feedback and not have an overall bad feeling.

Psychological capital optimism is an interesting construct to study in relation to employees specifically in today's functioning environment where change and uncertainty are the norms. With changing job responsibilities which are becoming challenging due to advent of big

data and employees having access to sensitive and critical information, employees need to be optimistic about their evolving and changing job roles and responsibilities to match the turbulent environment Luthans et al., (2007) in their study found that when employees are able to accept and capitalize their changing job roles and responsibilities, the organization is able to stay on top with respect to their value-based strategies and practices. These optimistic employees are able to deal with their changing roles head on and allow their organization to stay on top and gain competitive advantage. Interestingly, Gullapalli (2005) also observed the same in traditionally stable and structured workplaces like in accounting firms. Similarly, technology workers who usually think that they have cutting edge knowledge more often than not end up realizing the knowledge to be obsolete due o new advances on a regular basis.

Hope: Hope as a dimension of psychological capital is more than psychological strength and wishful thinking. Researchers support hope as the idea of a cognitive or thinking state in which an individual is capable of setting realistic but challenging goals and expectations and then reaching out for those with a sense of determination and energy. Some scholars also refer to this as agency or will power. Psychological capital scholars separate hope from other dimensions like self-efficacy, optimism and resiliency. The upward spiral of hope within individuals is actually a continuous reiteration between agency and pathways (Snyder et al., 1991; Snyder, 2002). This will power and determination helps develop pathways that ignite one's energy and sense of control.

Many prior studies in the field of positive psychological research have found a dominant relationship between hope and performance in many life domains such as academic achievement and wellbeing outcomes (Snyder, 2002; Kwon, 2000). Researchers are also beginning to support a positive relationship between work and employee performance at workplaces (Youssef and

Luthans, 2006; Luthans and Youssef, 2004). For instance, studies have found a positive relationship between employee hope and organizational profitability (Avolio & Gardner, 2005) and between hope levels of entrepreneurs and expressed satisfaction with business ownerships (Jensen and Luthans, 2002). Youssef (2004) in a study also found that hope level of managers and employees is positively related to their performance, job satisfaction, organizational commitment, and work happiness. Therefore, one can argue that psychological capital hope is important and related to work performance and researchers must explore ways to develop hope among employees.

Hope as a dimension of psychological capital is not just beneficial but a necessary characteristic of employees. In fact, effective managers can proactively nurture and reinforce hope in their employees and make them better equipped to face challenging tasks and responsibilities at the workplace. Hopeful employees are independent thinkers and have an internal locus of control. Due to this they utilized their sense of agency and have high degree of autonomy. Oldham and Hackman (1980) found that hopeful employees are intrinsically motivated and have a strong need for growth and achievement. These employees tend to be creative and resourceful and can also be risk takers in order to solve organizational problems and challenges. Therefore, in most technology and information sensitive industries employees with psychological hope could be an asset in the long run.

Resiliency: In the field of positive organizational behavior psychological capital resiliency is defined as "a class of phenomenon characterized by patterns of positive adaptations in the context of significant adversity or risk". Positive psychological research has found that resiliency within individuals enhances their human functioning especially related to adaptation and coping (Avery et al., 2009). In fact, Luthans et al (2005) also found a positive relationship

between resiliency and workplace performance outcomes. The concept of resiliency is of considerable interest in today's workplace environment due to competitive, changing and uncertain times. Today's organizational employees must be competent and capable of hoping and adapting to unfriendly, stressful and uncertain environments. The top performers within organizations are ones who can thrive on chaos and proactively learn and grow through hardships and inevitable setbacks. The organizations expect their employees to not only survive and cope but also thrive and flourish through inevitable difficulties and uncertainties that they face due to competition or uncertain changing environments. Psychological capital resiliency is not just coping with difficult times but also proactive capacity to reach out and pursue new knowledge and experiences and meaningful relationship with others at workplaces. In the technology and information industry resiliency has an even important role to play because adversities and cyber security threats are just around the corner due to the changing nature of technology.

In the light of the changing organizational environment, organizational leaders are looking for employees who have the ability to endure challenges and work through them in a proactive manner. Such employees can be assets for an organization and can serve as representatives of value and capabilities. These resilient employees can help their coworkers see threats as opportunities and further discourage ethically questionable behaviors during challenging times. We can apply this understanding to technology and information sensitive organizations where employee misbehavior could lead to data breaches and cyber security threats. Resilient employees can be caring leaders and can help with mentoring opportunities within organizations. Therefore, researchers need to focus on developing psychological capital

resiliency among employees to enhance employee behavior that adheres to the organization's values and goals.

3.2.3 Competence

The organization strategy literature helps us explain and enhance the competencies within organizations to achieve competitive advantage. These competencies also impact performance of the organization within the industry. Prior scholars have organized the strategy literature into two major paradigms: 1) the industrial organization economics paradigm emphasizes that certain organizations have 'structural impediments to competitive forces' that further helps them maintain competence, and 2) the idiosyncratic paradigm suggesting that organizations establish 'distinctive competencies' through a unique combination of tangible and intangible resources (Teece et al., 1991; Dhillon, 2008). Proponents of the organizational level competencies also argue that managers must identify and develop competence within an organization in a way that would lead to superior levels of performance and therefore sustained competitive advantage (Andreu & Ciborra, 2009).

From a strategic perspective, organizations are facing a major IS security challenge as there is limited focus on hiring and training employees towards better competence to perform their information security jobs. Weick & Roberts (1993) state that competence includes the elements of individual know-how and know-that along with mindful interactions that can enable individuals to be more competent. While competence is an integral factor for improving end-user performance, behavioral IS security research has paid limited attention to it. The focus area of many behavioral IS security research relates to understanding the different dimensions of 'end-user" behavior (Spears & Barki, 2010), including the factors that contribute to misbehavior (Willison & Warkentin, 2013). Associated with this work, IS scholars have evaluated how

individuals within organizations (insiders) are both a threat (Willison, 2006) and an asset (Posey et al., 2013), particularly related to IS security. For instance, Posey et al. (2011) found that environmental factors and negativity (i.e., employees focusing on the negative aspects of life) are attributed to lower levels of trust in the organizational IS security measures. Although IS security literature recognizes that employees can be motivated to engage in positive IS security behaviors, the question how individual competence can be developed to ensure IS security job performance remains unanswered.

Various IS security scholars have recognized the importance of enhanced IS security knowledge and skills (components of employee competence) and hence increased protection. For example, Hu et al. (2021) note that SETA is an approach that facilitates the learning process and hence positively affects the IS security-related intentions of employees. However, there are other factors, beyond developing IS security knowledge and skills such as collaborative learning techniques, that can also influence employee IS security performance. Similarly, Puhakainen and Siponen (2010) suggest that active participation of employees and senior management in IS security discussions improve the efforts made by employees towards IS security management. Even the National Initiative for Cybersecurity Education (NICE) framework released a Workforce Framework for Cybersecurity that elaborates on employee competencies associated with tasks, knowledge and skills which can be used to assess security capabilities. While scholars have made a call for examining factors different from the traditional learning approaches to improve IS security performance of employees, not many studies have focused their investigation on improving performance by nurturing IS security competence of employees.

Subsequently, given the state of security incidents that organizations face, one might argue if the SETA programs are indeed effective in improving the security performance of

employees. Perhaps organizations need to focus beyond SETA programs to strengthen competence of IS security employees. The conceptualization of competence is well studied in the organizational strategy domain and includes developing core abilities among individuals by focusing on the *know-how* and *know-that* elements of knowledge creation (McGrath et al., 1995). Furthermore, Weick & Roberts (1993) suggest that purposeful, attentive, and conscientious interactions among group members would result in reduced process errors. IS security research to far has focused on SETA programs that build necessary skills and provide information security knowledge that are crucial for keeping the sensitive information secure. However, it does not address the other parts of competence building process such as prior information security experiences of employees and heedful interactions with other colleagues that can further improve their abilities and competence. Hence, identifying the factors that increase employee capabilities and competence is central to expanding the understanding on IS security performance of employees. In this research, we dwell into the concept of employee competence and explore its antecedents.

3.3 Study methodology

The word 'methodology' can be interpreted in numerous ways, often depending on the context in which used or the person doing the interpreting. In the generic research context, it usually means the study of, or knowledge of, the various methods of doing research. However, some Information Systems authors have a broader interpretation of what the term 'methodology' means by including the theory and philosophy that underpin the research (Guba & Lincoln, 1994; Morgan, 2007). To avoid any ambiguity, this thesis adopts Crotty's (1998) definition of 'methodology' as:

> The strategy or plan of action, process, or design lying behind the choice and use of particular methods and linking the choice and use of methods to desired outcomes (p.3).

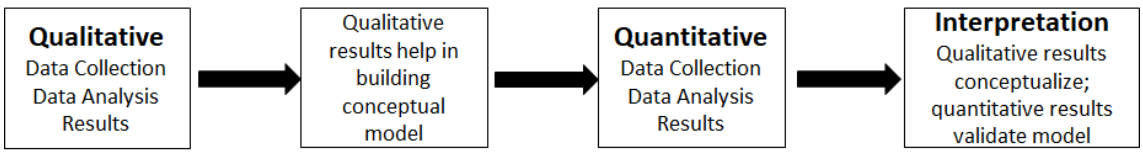
The strategy or plan of action for this research is described as a two-step sequential qualitative-quantitative approach with the objective being to identify the factors that contribute towards improvement of information security job performance and to identify the antecedents of employee competence.

Unlike most of the prior research in the information security domain, this research focuses on the human and behavioral aspects relating to the information security performance. Traditionally, most of the previous research in information security has concentrated on the technological components to improve information security performance by individuals.

3.4 Mixed methods research design

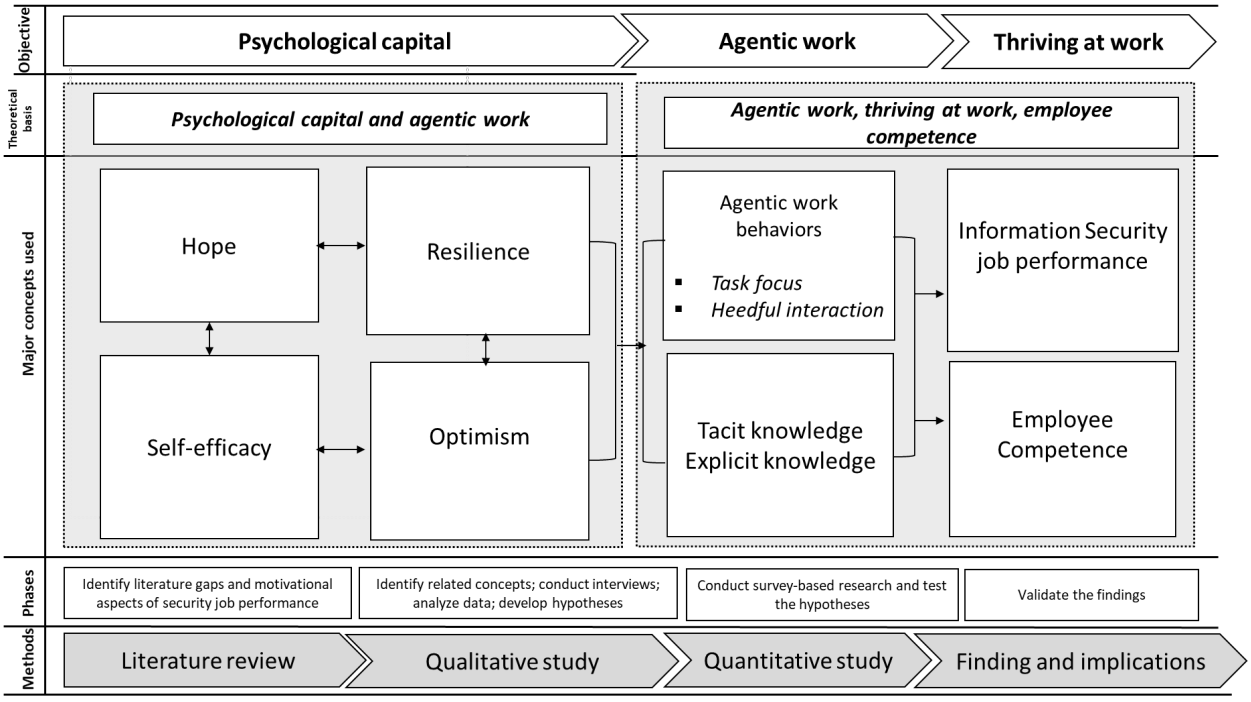
In the field of IS, mixed methods design combines both qualitative and quantitative approaches (Tashakkori & Teddlie, 1998). Given the changing and evolving nature of the field of IS, this method of study provides an opportunity to researchers where it is difficult to draw significant insights and conclusions from existing theories. Mixed methods design (see Figure 1) in general provides a deeper understanding to the researchers who are investigating concepts studied in other domains and fields (Venkatesh et al. 2013).

Figure 1. Mixed-methods research design



Mixed methods design offers an interesting dimension to the research as it helps to "provide stronger inferences than a single method or worldview." (Venkatesh et al. 2016). Given the general paucity of studies on thriving at work in the IS field, a mixed-methods design is well suited to our work. For our mixed-method study, we choose a general context whereby we conduct a qualitative study first and use the results from this phase to develop the hypotheses and the research model to be tested in the second phase of research (Tashakkori and Teddlie 1998; Venkatesh et al. 2013; Venkatesh et al. 2016). During the qualitative phase, we take an interpretive perspective while during the quantitative phase, we adopt a positivist approach. Figure 2 below provides an overview of the research design.

Figure 2. Overall research design



The methodology can be classified as "mixed-methods multistrand" (Venkatesh et al. 2016). The inductive qualitative study (Study 1) helped contextualize our theorizing based on the concepts that emerged through the study (cite context-specific theorizing paper). Based on the

analysis of our qualitative study and the extant literature, we build our research model. In Study 2, we empirically test our model using a survey approach and analyze our data using structural equation modeling.

3.4.1 Qualitative Case Study

The goal of this research is to identify the factors that impact and can further enhance information security job performance of employees. The conceptualization of thriving at work provided us with the theoretical background to start our investigation. We also focused on the theoretical underpinning of competence provided by McGrath et al. (1995). Our qualitative study, helps answer the following question: What factors impact the security job performance of employees in an organization? To answer this question, we interview employees of a leading public sector bank in India. Participants of the study are all employees who have a job with an element of information security in their job profile.

Figure 3. Research methodology

Research Method	Phase	Method	Objective	Procedure	Reference
Qualitative study	Phase 1	In-depth interview with a case study set-up	Identified the relevant constructs and items	Ensure that identified constructs are relevant and adequate to the dimensions of phenomenon under study	Califf et al., 2020
	Phase 2		Model development	Building and hypothesizing the research model	Califf et al., 2020
Quantitative study		Survey	Testing our hypotheses	Empirically test our research model developed based on the qualitative study	Califf et al., 2020; Wunderlich et al., 2019

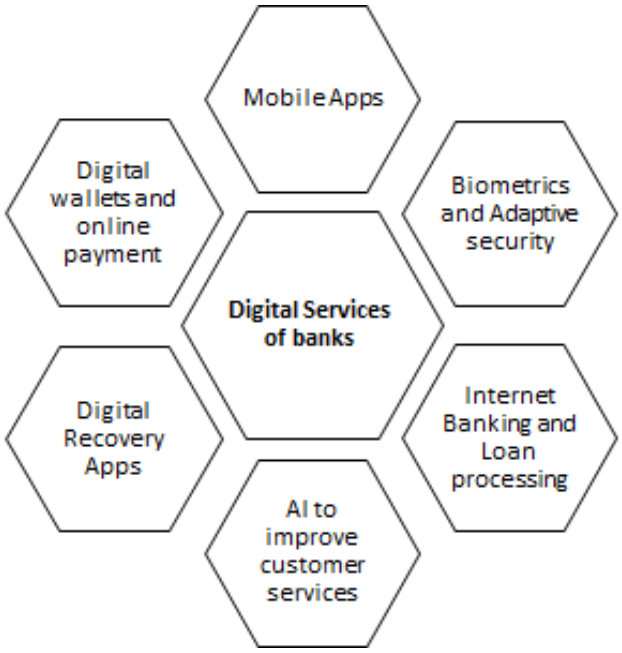
The interviews are structured based on Woodside (2013) guidelines. Participants are asked some basic questions related to their job profiles to make sure that they fit the criteria of information security context. Interviews are conducted in a written format and have open-ended questions. Once the data is collected, the empirical analysis is performed by an iterative process

of reading the responses, coding, and interpreting the interviews (Myers & Newman, 2007). The analysis is used to develop the hypotheses and the research model (see Figure 3).

General Banking Sector in India

The growth in retail banking segment in India has been facilitated by the growth in banking technology and automation of banking processes that enable extension of reach and rationalization of costs. ATMs have emerged as an alternative banking channel, which facilitate low-cost transactions vis-a-vis traditional branches. Although it has the advantage of reducing branch traffic, it also makes the customers vulnerable to security frauds. Customers' growing use of digital channels for banking and their demand for an individualized experience has forced many banks to revisit their data and information security policies. In the face of increasing competition from emerging digital banks, which are redefining customer experience and luring younger customers, traditional public sector banks have been forced to leverage digital technologies to create a more rewarding customer experience. These comprehensive digital services have added to the sensitive data and information of customers that the bank now has access to (see Figure 4).

Figure 4. Digital banking and services



Public and private sector banks have made significant investments in the realm of keeping the sensitive information secure through more stringent security policies for their customers and employees and developing security strategies that are better aligned with their business objectives and regulatory requirements. However, the more traditional public banks still struggle to ensure the security of sensitive data and information.

In order to better understand how these traditional banks can improve the performance of the employees to keep the sensitive customer and organization data secure, we conduct in-depth interviews with the employees of a public sector bank in India. We select this particular bank as it is a large, nationalized bank in India with a large financial asset and has huge, digitalized networks that offer customers digital services like mobile banking, internet banking, and digitalized banking services. Interviews were conducted for key internal regular employees, including branch managers, front-end staff, and IT executives. We used semi-structured interviews to allow for flexibility in probing respondents.

The Case of a Public Sector Bank in India

Alpha Bank (pseudonym) is one of the leading public sector banks of India. Two other government-owned banks were amalgamated into Alpha in early 2020. The bank has a network of 9300+ domestic branches, 11800+ ATMs serving over 120 million customers with 77000+ employees. The financial assets of the bank are worth USD 160 billion. The bank offers numerous digital banking services to its customers and was among the first public sector banks in India to offer 'Anytime and Anywhere' banking along with Telebanking. In 2012, the bank inaugurated its first 'Talking ATM' specially made for the benefit of the visually challenged. To better serve the changing needs and demands of its customers, the bank offers digitalized services like online account opening, mobile banking, internet banking, online loan processing to name a few. As a large organization with access to sensitive customer data, the bank has an elaborate Information Security Policy in place which is reviewed yearly to keep pace with the technological developments. The Chief Information Security Officer (CISO) heads the Information Security Committee and reviews the Information Security Management Systems performance.

With regard to information security and security of the sensitive data that the bank has access to, the bank has detailed responsibility for every person within the bank that is part of the performance of the internal employees. For instance, the bank has outlined performance responsibilities for 'information owners' and 'information custodians' that includes maintaining the accuracy, completeness, and integrity of the information. The bank evaluates these performance responsibilities regularly to avoid potential information security breaches and incidents.

3.4.2 Quantitative Study

Our proposed quantitative study is based on explanatory survey research (Malhotra & Grover, 1998). For our empirical study, we follow Malhotra and Grover (1998) guidelines for conducting survey research. In accordance with Hair et al. (2019) suggestions, this study analyzes the observations and tests the research hypotheses using partial least squares based structural equation modeling (PLS-SEM). After developing the instrument in Qualtrics survey software, we pretest the questionnaire with four doctoral students from the business school. Based on the feedback received from the pretest, we revise the questions for better clarity of context and validity. After finalizing the initial questionnaire, we run a pilot study with 35 bank employees.

After designing and developing our final survey questionnaire, we make the questionnaire available online by using the Qualtrics online software. The final questionnaire demonstrated validity and reliability of the instrument. We collected our data by distributing the online questionnaire to the bank employees and the responses were collected through the Qualtrics software. The survey instrument for the study includes items that are adapted from the extant literature. We measure all constructs using a 7-point Likert scale (ranging from 1-Strongly disagree to 7-Strongly agree). Data collection occurred between June 2020 to January 2021. We examined the common method bias (CMB) using two techniques: (1) Harman's one-factor test to identify common method variance (Podsakoff et al., 2003); (2) PLS Marker variable approach to analyze data contaminated with method variance (Lindell and Whitney, 2001).

3.5 Conclusion

This chapter presents an elaborate account of the informing theories and the research methodology adopted in this research. The theoretical conceptualization of thriving at work and

employee competence has been used earlier in the organizational studies field but not in the context of information security and its outcomes in a work situation. As we did have a conceptual framework in our mind, we did not start the case study in the nationalized bank in India with a clean state. The nature of the research problem guided the design of this research as we adopt a sequential approach to better understand the conceptualizations of thriving at work and employee competence in the context of information security. Even though we use a sequential approach to deepen our understanding of the conceptualization of thriving at work and employee competence, we have a same research question that guides both the in-depth case study and the quantitative analysis. For both the case study and the empirical analysis, the respondents are bank employees who handle and have access to sensitive employee information. The limitations of the methodology are discussed in Chapter 7 as no research is entirely appropriate.

CHAPTER IV: THRIVING AT WORK AND INFORMATION SECURITY JOB PERFORMANCE

4.1 Introduction

The study described in this chapter explores the conceptualization of thriving at work and its impact on information security job performance. Thriving is a positive psychological state that is characterized by learning and vitality. Conventional wisdom, recent research in information systems security and managerial experience indicate that thriving benefits the employees as well as helps the organization achieve its long-term mission and goals. This study specifically tests thriving at work in the field of information security. In order to develop deeper insights on the conceptualizations in the context of information security, a large, nationalized bank in India was sampled out. Banks in India have been focusing on digitalization of their financial and banking services in past decade. Also, there has been an initiative in the nationalized banks to decentralize their operations and as a result, bank employees at the branch level have been given access to sensitive customer information and data.

This chapter discusses in detail the contextual understanding and insights that were gained through the in-depth case-study conducted in the nationalized bank. Section 4.2 describes briefly the theoretical background of thriving at work conceptualization. Section 4.3 presents the analysis of the case study that was used to develop our research model. Section 4.4 shows the empirical results of the research model that was tested through the respondents form Alpha Bank followed by the contribution of the study in Section 4.5. Section 4.6 finally concludes the interpretations of the study.

4.2 Background

In recent years, the concept of thriving at work has received significant attention, especially in organizational studies (Spreitzer & Porath, 2012). Thriving at work is characterized by a joint experience of vitality and learning (Spreitzer et al., 2005). When employees in an organization experience vitality, they feel positive based on available energy and feeling of aliveness (Porath et al., 2012). The experience of learning gives the employees a sense of continually improving and getting better at what they do (Porath et al., 2012). Spretizer et al. (2005) emphasized that a sense of progressing, and self-development can be based only on the joint experience of vitality and learning as they constitute the hedonic and eudaimonic perspectives of psychological functioning respectively.

Thriving at work as a construct is quite distinct from related constructs of flourishing, flow, subjective well-being, and work engagement which are important psychological concepts in organizational studies. For example, thriving and flourishing share similarities as they both focus on positive states of human functioning (Diener et al., 2010). Similarly, thriving at work and work engagement both involve some amount of vitality and vigor but work engagement does not require a joint experience of learning (Spretizer et al., 2010). Porath et al. (2012) has shown that thriving at work is related to better well-being, less strain, and lower levels of burnout among individuals. As thriving at work is positively associated with career and self-development initiatives, it encourages individuals to thrive even outside of work. This is beneficial not only for the employees themselves but also for the organizations they work in. In addition, thriving at work also leads to increased proactivity among employees and better job performance (Paterson et al., 2014; Porath et al., 2012).

Based on extant literature, positive psychology is an ideal and essential component of IS security research because it focuses on the positive functioning of ordinary people (Sheldon & King, 2001) and makes it suitable for understanding and exploring of information security-behaviors of employees in the organization. Psychological capital is an interesting construct that focuses on optimal functioning (Posey et al., 2013). As a higher-order construct, psychological capital comprises of different, yet related, core factors of positive psychology: hope, resilience, optimism, and self-efficacy. Further, psychological capital introduces an important broad-based, work-related positive psychological resource to the IS security literature, which has still not been fully understood. There is still a knowing-doing gap (Cox, 2012).

Role related resources, such as psychological capital, are uniquely positioned for use in contemporary organizational IS security research because they relate to a broader set of tasks rather than an employee's technical job requirements. Hope, the first of the four psychological capital subconstructs, is a "positive motivational state that is based on an interactively derived sense of successful (a) agency (goal-directed energy) and (b) pathways (planning to meet the goals)" (Snyder et al., 1991). Resilience is characterized by positive coping and adaptation in the face of significant risk or adversity" (Luthans et al., 2007). Resilience is also "the positive psychological capacity to rebound, to 'bounce back' from adversity, uncertainty, conflict, failure, or even positive change, progress and increased responsibility" (Luthans, 2002). Optimism, as a first-order variable of psychological capital, is the characteristic of individuals who "expect things to go their way, and generally believe that good rather than bad things will happen to them" (Scheier & Carver, 1985). Finally, self-efficacy is a role-breadth characteristic and is defined as an "employee's perceived capability of carrying out a broader and more proactive set of work tasks that extend beyond prescribed technical requirements" (Parker, 1998).

Although a relatively new construct, psychological capital has already been well accepted in the field of organizational behavior and other fields including information security (Posey et al., 2013; Luthans et al., 2007). A primary reason for this acceptance is that psychological capital's characteristics are state-like rather than trait-like (Posey et al., 2013). State-like characteristics of psychological capital is crucial because it allows intervention in an individual's course of action. Thus, the impact that psychological capital has on the employees has an interesting dimension as its applicability for IS security. For example, psychological capital can be developed within the organization through targeted interventions (Luthans et al., 2006) or as a higher-order factor through supportive organizational climate (Luthans et al., 2008). Researchers who have studied psychological capital have shown that this psychological functionality can lead to development of successful strategies for better performance in the workplace (Luthans et al., 2007a, 2008). Psychological capital is a higher-order reflective construct, which means that its subconstructs vary together in the same direction (Bagozzi, 2011). Psychological capital has also been considered as a psychological resource by organizational scholars (Avey et al., 2009). Researchers have used the resource theory and argued that psychological capital is an adaptive resource as it not only embodies a positive psychological state but also serves meaningful ends as a psychological construct (Luthans et al., 2007; Hobfoll, 2002). For instance, previous research shows that psychological capital provides the requisite psychological capacity or resources for psychological well-being and positive functioning.

Whether one views psychological capital as a psychological resource or simply as a psychological state, it is important to highlight the previously established links between psychological capital and organizational outcomes. For our purposes, it is also imperative to relate the established relationships of psychological capital to IS security. The existing body of

psychological capital literature has uncovered a positive relationship between psychological capital and increases in positive organizational and personal outcomes, as well as decreases in negative organizational and personal outcomes. For example, studies show that psychological capital increases job performance and satisfaction (Luthans et al., 2007a), as well as organizational commitment and citizenship (Avey, Reichard, Luthans, & Mhatre, 2011). On the contrary, studies have also shown that psychological capital reduces unfavorable outcomes, such as absenteeism (Avey, Patera, & West, 2006), and stress (Avey et al., 2009).

It is evident from the literature review that information security job performance, thriving at work, and psychological capital are concepts of growing interest to IS researchers and practitioners given its applicability to security challenges. While the literature provides enough evidence that information security job performance is a crucial outcome for an organization, researchers are yet to fully understand the multifaceted and complex nature of the construct. Also, researchers in the field of IS have not explored the positive psychological facility of psychological capital and the construct of thriving at work which is a well investigated concept in organizational studies. To fill this void in the extant literature, we develop a holistic theoretical model that integrates the psychological dimension of psychological capital and thriving at work into providing a more robust and elaborate understanding of the complex construct of information security job performance.

4.3 Qualitative Case Study

The growth in retail banking segment in India has been facilitated by the growth in banking technology and automation of banking processes that enable extension of reach and rationalization of costs. ATMs have emerged as an alternative banking channel, which facilitate low-cost transactions vis-a-vis traditional branches. Although it has the advantage of reducing

branch traffic, it also makes the customers vulnerable to security frauds. Customers' growing use of digital channels for banking and their demand for an individualized experience has forced many banks to revisit their data and information security policies. In the face of increasing competition from emerging digital banks, which are redefining customer experience and luring younger customers, traditional public sector banks have been forced to leverage digital technologies to create a more rewarding customer experience. These comprehensive digital services have added to the sensitive data and information of customers that the bank now has access to.

Public and private sector banks have made significant investments in the realm of keeping the sensitive information secure through more stringent security policies for their customers and employees and developing security strategies that are better aligned with their business objectives and regulatory requirements. However, the more traditional public banks still struggle to ensure the security of sensitive data and information.

In order to better understand how these traditional banks can improve the performance of the employees to keep the sensitive customer and organization data secure, we conduct in-depth interviews with the employees of a public sector bank in India. We select this particular bank as it is a large, nationalized bank in India with a large financial asset and has huge, digitalized networks that offer customers digital services like mobile banking, internet banking, and digitalized banking services. Interviews were conducted for key internal regular employees, including branch managers, front-end staff, and IT executives. We used semi-structured interviews to allow for flexibility in probing respondents.

At Alpha Bank, the information security policies are formulated and documented at the Bank Headquarters and are then made available to all employees through the Bank's internal

system. All employees are expected to go through the security policies regularly as they are modified and updated on a need basis and to remain compliant with the security policies of the central bank. However, with the emphasis of the bank to make the operations more decentralized, the employees at the branch level are exposed to more sensitive information. At the branch level - the basic unit of operations - the employees are expected to have skills and knowledge to manage the sensitive financial and personal information of the customers. The managers of the branches were of the opinion that this involves learning and re-learning for the employees at a regular basis as information security in the banks is ever evolving. For instance, whenever an information security incident takes places in any of the bank branches, more stringent rules are enforced by the IT department and the information security managers. Managers observed that employees who display a sense of self-efficacy and resilience towards these information security incidents have more inclination towards their information security task at hand and are better learners. To highlight the importance of optimism and resilience (aspects that lead to psychological capital), a Branch Manager of the bank commented:

> …in the branch employees who have a personally faced or heard of a fraud incident think that these incidents can be easily avoided if their branch colleagues are focused on what the information they are providing to the customer or officer…

These employees have a higher sense of self-efficacy as described by their managers and are confident that they are competent of doing their information security task with focus and attention. In the bank branch, this task focus manifests as being aware of the information they are providing to the customers. For instance, bank employees must perform due diligence when a customer approaches them to seek information about a bank account which belongs to one of the

family members. Although the bank's information security policy mandates that employees should not disclose financial information of a customer to even the closest family member, some employees are less focused on the task at hand. These incidents could later lead to information frauds where legitimate moneys are lost. To further validate the importance of learning and task focus, one of the bank employees explained:

> …we always feel more capable of handling customers who might be looking for ways to get some sensitive information like Aadhar numbers linked to another bank account when we are more focused in our work…we share our experiences with other staff members so they also know what are the latest modus operand of fraud customers…it is part of learning process...

The importance of the learning among different employee groups and stakeholders of the bank was also highlighted by the employees. The Loan Officer, who has access to critical customer data noted:

> …I have personally learned the most about the details of my organization's security policies by interacting with other colleagues and my manager…the experiences shared by my manager add to my knowledge...it also gives me a sense that I can now handle a bank situation with more confidence…

Therefore, the doubts and dilemma of the employees as to how crucial it is for them to comply with security policies is taken care of by the interactions amongst employees with varied job responsibilities. Employees feel more confident and assertive when these security responsibilities are communicated to them through formal or informal ways. These interactions also result in improving not just the know-how and skills of the employees but also helps them

better conceptualize the process of keeping the information secure. Information security within an organization is a process, dysfunction of which causes a security incident.

Within the context of the bank, employees with past experience with handling an information security incident showed higher levels of confidence in performing their security jobs. It was evident that different stakeholders explicitly mentioned how their past experiences along with the policy guidelines of the bank helped them in being more vigilant about the sensitive data and information. These employees were also reported to share the experiences with other colleagues at the bank through interactions in the morning *'huddle'* sessions. A Branch Manager commented:

> …employees who come with first-hand experience in information security somehow are able to deal with customer information and queries more effectively…experienced employees contribute to branch performance by sharing their experiences with subordinates which encourages them to ask more questions...

Although the Branch Managers would have regular meetings and sessions with other employees of the branch to convey the security policies of the bank, there was a disconnect among the front desk employees as to how the security policies worked in the bigger scheme of things. This disconnect seemed to be resolved through the interactions they had with their managers and other colleagues that came with prior experience. Through the experience, they were able to share insights on how following some basic steps like verifying the ID of the customer asking for account details and fulfilling know-your-customer formalities could avoid information frauds at a branch level.

This was reiterated by the information security officer as well as they emphasized that the employees who come with prior experience have a sense of optimism and resilience in handing their information security tasks. These employees are also seen to have an inquisitive mind and learn better. An IS executive explained:

> …these are employees who join with prior experience have a feeling that they can handle customers who come with an intention of fraud…they are more eager to learn and usually are winners of our information security quiz…

Consistent with Venkatesh et al. (2013), the statements from the interviews helped explore the different concepts. These concepts complement the extant research on thriving and particularly learning and vitality and its antecedents. Most importantly, our findings from the in-depth case study highlighted the important concepts of psychological capital, task focus, heedful interactions, learning, and thriving in the context of information security. Managers and IT executives emphasized that when employees felt more competent to perform their duties to keep data and information safe when there was task focus and heedful interactions among the members of the branches. Our qualitative study (see Table 3) also suggested that exploratory behavior along with SETA enhanced information security job performance and information security competence among employees.

Table 3. Sample interview quotes for emergent concepts: Thriving at work

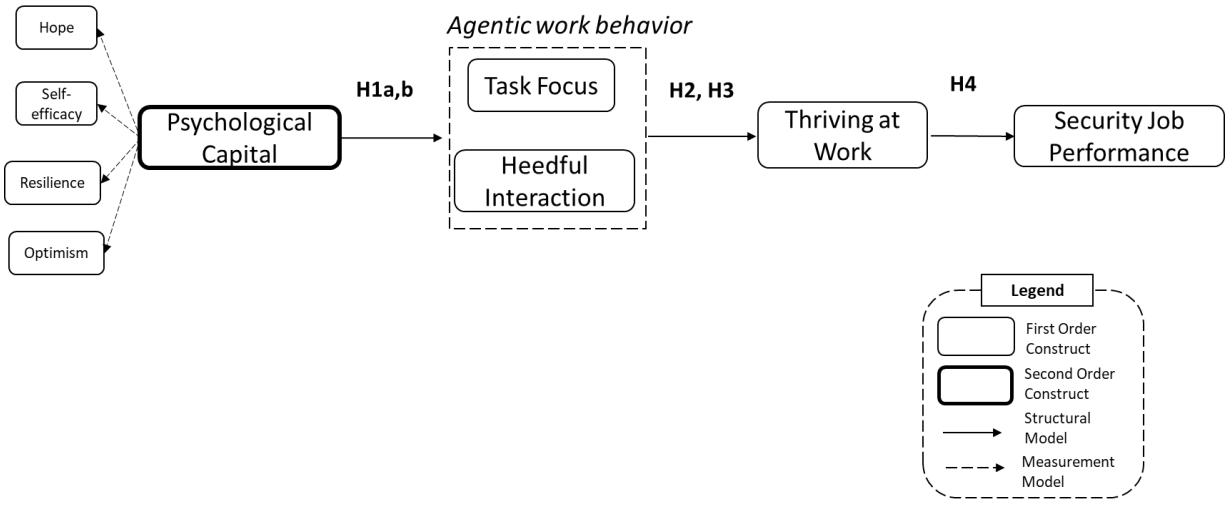
Emergent concept	**Definition**	**Sample interview quotes**
Psychological capital	An individual's positive psychological factors such as hope, optimism, resilience and self-efficacy when doing information security tasks at work place.	*'…in the branch employees who have a personally faced or heard of a fraud incident think that these incidents can be easily avoided if their branch colleagues are focused on what the information they are providing to the customer or officer…'*

Task focus	An individual's focus and engagement towards their information security tasks at hand in their work environment.	*'...we always feel more capable of handling customers who might be looking for ways to get some sensitive information like Aadhar numbers linked to another bank account when we are more focused in our work...we share our experiences with other staff members so they also know what are the latest modus operand of fraud customers...it is part of learning process...'*
Heedful interactions	When individuals invest in purposeful and heedful interactions with others and work towards developing a collective mind towards information security tasks.	*'...I have personally learned the most about the details of my organization's security policies by interacting with other colleagues and my manager...the experiences shared by my manager add to my knowledge...it also gives me a sense that I can now handle a bank situation with more confidence...'*
		'...employees who come with first-hand experience in information security somehow are able to deal with customer information and queries more effectively...experienced employees contribute to branch performance by sharing their experiences with subordinates which encourages them to ask more questions...'
Thriving at work	A psychological state in which individuals experience both a sense of vitality and learning while performing their information security tasks.	*'...these are employees who join with prior experience have a feeling that they can handle customers who come with an intention of fraud...they are more eager to learn and usually are winners of our information security quiz...'*

4.4 Hypotheses development

Two main theoretical concepts inform this work – the concept of thriving at work and psychological capital. Researchers in the fields of organizational studies have focused on how thriving at work as a concept impacts individual outcomes in the work environment. In this study we explore the impact of psychological capital on agentic work behaviors and thriving at work. The central premise of our holistic theoretical model is that when employees are situated in a particular work context, they are likely to thrive, and this further influences their work outcomes in terms of their work performance. We present our initial research model in Figure 5.

Figure 5. Research model: Thriving at work



4.4.1 Psychological capital and agentic work behaviors

Psychological capital consists of hope, efficacy, resiliency, and optimism (Luthans, Youssef et al., 2007) and has been conceptually and empirically demonstrated to be a state-like, second-order, core construct predictive above and beyond its four individual components (Luthans, Avolio et al., 2007). Luthans, Avolio, et al. (2007) stated that psychological capital is one's "positive appraisal of circumstances and probability for success based on motivated effort and perseverance", and a recent meta-analysis indicates it has a significant impact on desired work attitudes, behaviors, and performance (Avey et al., 2011). This "positive appraisal" also leads to a higher sense of intrinsic motivation among individuals. When employees consider whether or not to devote their full attention and focus to task performance, a key deciding factor may be hoe motivated they feel towards their work and completion of the task. Those with high levels of psychological capital are confident that they can be successful in task accomplishment (efficacy), harness goal-directed energy and proactively plan for alternative pathways for task accomplishment (hope), persevere in the face of obstacles (resiliency), and attribute positive outcomes to self and negative outcomes to circumstances (optimism). These factors combine to

make an employee with high levels of psychological capital likely to exhibit higher levels of intrinsic motivation.

Bandura (2001) explained that when individuals act agentically, they are intentional and in control of their own behaviors. Such intentional, self-directed behavior is more likely to lead to feelings of vitality and the experience of learning at work than reactive, prescribed behavior (Spreitzer & Porath, 2013). This is because, as Bandura (2001) noted, "the capacity to exercise control over the nature and quality of one's life is the essence of humanness" and will therefore be associated with the zest for life and aliveness that is inherent in vitality. Individuals who are self-motivated and agentic at work are also likely to experience learning at work because they are open to finding new ways of doing things rather than just "doing what they are told." Thus, we hypothesize:

H1a: Psychological capital will be positively associated with task focus.

H1b: Psychological capital will be positively associated with heedful interaction.

4.4.2 Thriving at work

Prior research indicates that thriving at work predicts individual job performance above and beyond common attitudinal variables such as job satisfaction and organizational commitment (Porath et al., 2012; Spreitzer et al., 2012). Because of the generative nature of thriving, it has also been shown to play a critical role in the generation of innovative and creative ideas (Carmeli & Spreitzer, 2009). Thriving at work has also been linked to important individual outcomes such as overall health (Porath et al., 2012), burnout and strain (Porath et al., 2012; Spreitzer et al., 2012), and thriving in family, social, and community relationships (Spreitzer et al., 2012). Even though theorized (Spreitzer et al., 2005), the relationship with self-development is missing from the empirical research on thriving at work. Conceptually, thriving was described

by Spreitzer et al. (2005) as “an adaptive function that helps individuals navigate and change their work contexts to promote their own development.” As employees act agentically when they are performing their jobs, the agentic work behaviors of employees is the main source and guiding factor for their self-development. These agentic behaviors contribute to the vitality and learning dimensions of progress and improvement. Thus, we hypothesize:

H2: Task focus will be positively associated with thriving at work.

H3: Heedful interaction will be positively associated with thriving at work.

4.4.3 Information security job performance

Thriving at work finally leads to individual outcomes in order to pursue growth and development as a result of their thriving (Spreitzer et al., 2005). In the information security work context, the outcome is related to how they perform their information security job. The outcome also includes the knowledge and skills that employees imbibe during their learning. Once employees experience the positive energy associated with heightened levels of learning, this energy translates into better involvement in their information security job and ensuring more competence in their work. Thus, we hypothesize:

H4: Thriving at work will be positively associated with information security job performance.

The hypotheses are summarized in Table 4.

Table 4. Summary of hypotheses: Thriving at work

Hypotheses	Description
H1a	Psychological capital is positively associated with task focus. Individuals who have higher psychological capital in terms of being more hopeful and optimistic will have higher agentic work behaviors.
H1b	Psychological capital is positively associated with heedful interactions. Individuals who have higher psychological capital in terms of being more hopeful and optimistic will have more heedful and purposeful interactions with others.

H2	Task focus will be positively associated with thriving at work. When employees are able to focus on their information security task at hand, it leads to them learning and thriving in the work environment.
H3	Heedful interaction will be positively associated with thriving at work. When employees have purposeful and heedful interactions with other co-workers, they are able to learn better and thrive in the work environment.
H4	Thriving at work will be positively associated with information security job performance. Individuals who focus on learning and vitality in their information security job are able to perform better.

4.5 Empirical analysis

Our proposed quantitative study is based on explanatory survey research (Malhotra & Grover, 1998). For our empirical study, we follow Malhotra & Grover (1998) guidelines for conducting survey research. In accordance with Hair et al. (2019) suggestions, this study analyzes the observations and tests the research hypotheses using partial least squares based structural equation modeling (PLS-SEM). After developing the instrument in Qualtrics survey software, we pretest the questionnaire with four doctoral students from the business school. Based on the feedback received from the pretest, we revise the questions for better clarity of context and validity. After finalizing the initial questionnaire, we run a pilot study with 35 bank employees.

4.5.1 Data collection

After designing and developing our final survey questionnaire, we make the questionnaire available online by using the Qualtrics online software. The final questionnaire demonstrated validity and reliability of the instrument. We collected our data by distributing the online questionnaire to the bank employees and the responses were collected through the Qualtrics software. The survey instrument for the study includes 65 items that are adapted from the extant literature. The measurement items for the constructs are adapted from published literature on thriving at work and information security job performance (see Appendix A). We

measure all constructs using a 7-point Likert scale (ranging from 1-Strongly disagree to 7-Strongly agree).

Data collection occurred between June 2020 and January 2021. We started with our exploratory data collection for 35 participants for a pilot. The pilot reveals that the scales are reliable and valid. Through the online Qualtrics survey, we collected responses from 321 bank employees. On average, the participants took about 15 minutes to complete their response. We examined the common method bias (CMB) using two techniques: (1) Harman's one-factor test to identify common method variance (Podsakoff et al., 2003); (2) PLS Marker variable approach to analyze data contaminated with method variance (Lindell and Whitney, 2001). The former confirmed that none of the factors individually explain the majority of the variance. The latter added a theoretically irrelevant marker variable in the research model, obtaining 0.008 (0.8%) as the maximum shared variance with other variables, a value that can be considered low. Hence, no significant CMB was found.

The respondents were 63% males, 37% females, and between 25 and 55 years. The majority of them were highly educated (47% with a bachelor's degree, and 23% with post-graduate degree).

4.5.2 Data analysis

In this study, we use partial least squares (PLS) regression to conduct our analysis. Prior literature suggests that PLS approach works well if the research model has not been tested in prior studies and if it is necessary to prevent restrictive distributional assumptions when determining path coefficients that are significantly different from zero (Lathan et al., 1979; Fornell and Bookstein, 1981). Hence, we use Smart PLS 3.3.3 to empirically estimate our research model (Ringle et al., 2012).

4.5.3 Measurement model

A measurement model analysis (see Table 5) is conducted to assess the construct reliability, convergent validity, indicator reliability, and discriminatory validity of scales for the reflective constructs. Construct reliability was tested using composite reliability (CR). The CR results were higher than 0.7 for all constructs, which indicates the internal consistency and appropriateness of the constructs (Straub, 1989; Henseler et al., 2009). Convergent validity was demonstrated using the average variance extracted (AVE). The AVE values are higher than 0.50 for all constructs, and thus the convergent validity of the measurement model is established. For indicator reliability, the loading should be higher than 0.7 (Henseler et al., 2009). We see that all loadings are higher than 0.7, and consequently, the reliability indicator is satisfied.

Table 5. Descriptive statistics, correlation, composite reliability (CR), and average variance extracted (AVE)

Construct	Mean	SD	CR	HOP	SEF	RES	OPT	PSY	TAS	HED	TAW	PER
Hope (HOP)	0.487	0.358	0.957	**0.888**								
Self-efficacy (SEF)	0.251	0.532	0.956	0.873	**0.902**							
Resilience (RES)	0.597	0.478	0.933	0.879	0.792	**0.881**						
Optimism (OPT)	0.362	0.583	0.927	0.805	0.748	0.764	**0.872**					
Psychological Capital (PSY)	0.227	0.601	0.976	0.969	0.879	0.921	0.879	**0.825**				
Task Focus (TAS)	0.579	0.202	0.956	0.822	0.777	0.711	0.639	0.807	**0.920**			
Heedful interaction (HED)	0.143	0.805	0.964	0.746	0.769	0.663	0.689	0.778	0.650	**0.903**		
Thriving at work (TAW)	0.211	0.361	0.949	0.743	0.797	0.642	0.695	0.782	0.640	0.858	**0.852**	
Information Security Job Performance (PER)	0.690	0.433	0.953	0.745	0.79	0.663	0.708	0.807	0.726	0.687	0.716	**0.864**

Note: Values in diagonal (bold) are the AVE square root; standard deviation (SD)

To evaluate the discriminatory validity (see Table 6), we use three criteria: (1) Fornell-Larcker matrix, (2) Cross-loadings, and the (3) Heterotrait-Monotrait ratio (HTMT) (Henseler et

al., 2009). In the Fornell-Larcker criterion, we examine each construct's discriminant validity using the correlation between constructs and the root square of the AVE. As shown in Table above, the AVE square root of each construct (diagonal elements) is higher than the correlations between the constructs. Hence, the first criterion for the constructs' discriminant validity is supported. Using the criteria of Cross-loading numbers (see Appendix C), we determined that all the loadings of the constructs were higher than the cross-loading numbers (Chin, 1998). Finally, based on Table 6, all values of Heterotait-Monotrait ratio (HTMT) are lower than the threshold of 0.9, except for second-order constructs. Therefore, the discriminant validity of the constructs is confirmed.

Table 6. Heterotrait-Monotrait (HTMT): Thriving at work

Construct	HOP	SEF	RES	OPT	PSY	TAS	HED	TAW	PER
Hope (HOP)									
Self-efficacy (SEF)	0.905								
Resilience (RES)	0.879	0.850							
Optimism (OPT)	0.874	0.814	0.705						
Psychological Capital (PSY)	0.945	0.969	0.908	0.914					
Task Focus (TAS)	0.872	0.825	0.767	0.696	0.841				
Heedful interaction (HED)	0.785	0.809	0.701	0.744	0.804	0.685			
Thriving at work (TAW)	00.787	0.846	0.686	0.758	0.814	0.678	0.809		
Information Security Job Performance (PER)	0.788	0.838	0.710	0.771	0.821	0.767	0.724	0.76	

4.5.4 Structural model

We test the multicollinearity of all constructs before assessing the structural model. For that we use variance inflaction factor (VIF). Our results show all the construct VIFs are close to or lower than 3, meaning the absence of multicollinearity among the variables (Hair et al., 2019).

The structural model results are presented on Figure 6. The statistically significance level of path coeficients were performed using bootstraping with 5000 resamples.

Our model explains 65.2% of the variation in task focus and 60.5% of the variation in heedful interaction which are the two agentic work behaviors in our model. We hypothesize psychological capital is positively associated with task focus and heedful interaction. We found the association between psychological capital and task focus ($\hat{\beta} = 0.807$; $p < 0.05$) to be statistically significant as hypothesized. We also found the association between psychological capital and heedful interaction ($\hat{\beta} = 0.778$; $p < 0.05$) as statistically significant as hypothesized.

Our model explains 74.7% of the variation in thriving at work. We hypothesize that task focus and heedful interaction are positively associated with thriving at work. We found the association between task focus and thriving at work ($\hat{\beta} = 0.143$; $p < 0.05$), and between heedful interaction to thriving at work ($\hat{\beta} = 0.143$; $p < 0.05$) are statistically significant as hypothesized.

Finally, our model explains 51.2% of the variation in information security job performance. We hypothesize thriving at work is positively associated with information secuirty job performance. We have found the associations from thriving at work to information job performance ($\hat{\beta} = 0.716$; $p < 0.05$) as statisfically significant.

Figure 6. Structural model: Thriving at work

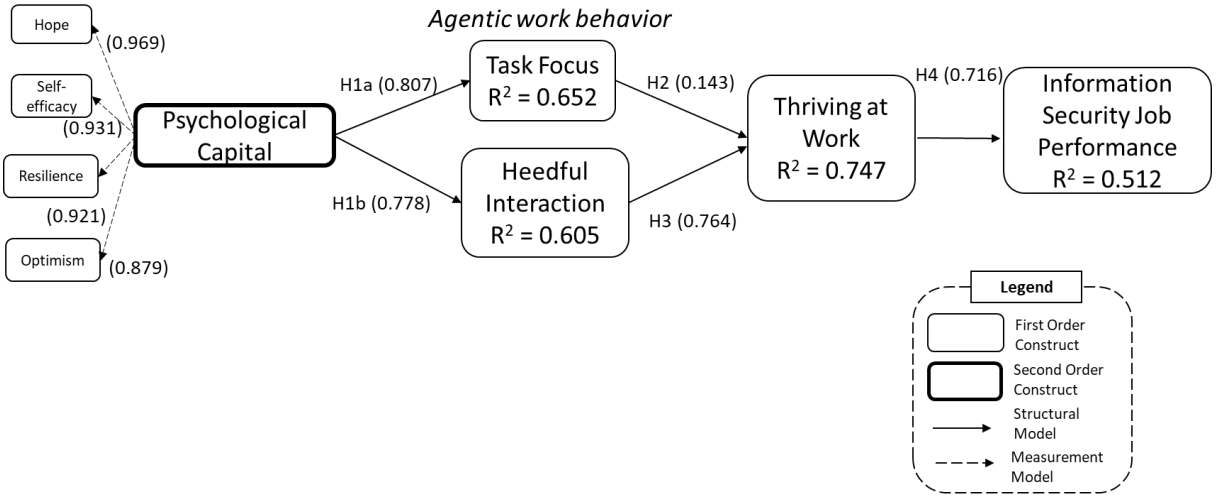


Table 7 below sumarizes the supported hypotheses along with direct and total effects.

Table 7. Bootstrapping result for structural model: Thriving at Work

	Hypotheses	Hypothesized Direction	Direct effect	p-Value	Conclusion
H1a	Psychological Capital → Task Focus	Positive	0.807	0.000	**Supported**
H1b	Psychological Capital → Heedful interaction	Positive	0.778	0.000	**Supported**
H2	Task Focus → Thriving at work	Positive	0.143	0.028	**Supported**
H3	Heedful interaction → Thriving at work	Positive	0.747	0.000	**Supported**
H4	Thriving at work → Information Security Job Performance	Positive	0.716	0.000	**Supported**

p-value < 0.05

4.6 Contribution

This study contributes to the better understanding of thriving at work to a theoretically important outcome variable, which is information security job performance, understanding its relationship with agentic work behaviors (task focus and heedful interaction) and proposing and empirically testing its relationship with Psychological Capital as an antecedent variable. The empirical results have supported the hypothesized relationships.

The findings of this study have several theoretical and practical implications. Perhaps the most significant contribution is the application of the conceptualization of thriving at work construct in the domain of information security. Spreitzer et al. (2005) laid emphasis on the individual enabler psychological capital and the agentic work behaviors as the 'engines of thriving' in a social embedded structure. Specifically, this study provides evidence that psychological capital, a "positive appraisal of circumstances and probability for success based on motivated effort and perseverance" (Luthans et al., 2007), results in significantly higher levels of agentic work behaviors and thus contributes to thriving at work. This study is perhaps the first study to empirically test and evaluate this relationship in the context of information security job performance being an outcome of the thriving. These conceptualizations are particularly interesting as both psychological capital and thriving at work have been conceptually developed and empirically tested in the context of a bank where information security is part of the basic job responsibility of the employees. (Luthans, 2002; Spretizer et al., 2005). Therefore, a meaningful implication of this study is the evaluation of nature of these constructs in a recognized information security work environment. The findings of this study also support organizational studies research that suggest that employees can take active role in learning and thus support

superior outcomes (Roberts et al., 2005). In this study the outcome of the thriving was an improvement in the information security job performance of the employees in the work situation.

4.7 Conclusion

This chapter attempted to describe in detail the first study of this research where the main objective was to explore the conceptualization of thriving at work by undertaking an in-depth case study in a large, nationalized bank in India to develop our research model. Using a sequential research methodology, as described in Chapter 3, we explore the factors that contribute to thriving at work that further improves information security job performance of employees. For the in-depth case study, we interviewed the employees of the nationalized bank in India to gain better understanding of the factors that they believed helped in manifesting better efficiency and precision in their information security tasks and job responsibilities. Based on the findings of the interview and the broad conceptualization of thriving at work, we developed our research model that included an individual contributor (psychological capital) and agentic work behaviors (task focus and heedful interaction) as the antecedents of thriving at work. The outcome of thriving at work in our research is the information security job performance of employees in the bank. The model was then empirically tested, and all hypothesized relationships were supported. The findings from this study revealed that employees who feel a sense of thriving in their security tasks and work have a higher information security job performance. Employees with a higher sense of psychological capital (individuals that display hope, self-efficacy, resilience and optimism) are more focused towards their tasks. Also, an interesting finding was the role of heedful interaction among the employees and its role in helping employees experience a sense of learning and vitality, that are the components of thriving. Overall, in the managerial scenario, thriving employees are better performers in their

security job roles and responsibilities. Therefore, managers need to incorporate opportunities of learning and vitality into the task and work schedules that require them to keep the data and information they are handling safe and secure.

CHAPTER V: EMPLOYEE COMPETENCE AND INFORMATION SECURITY JOB PERFORMANCE

5.1 Introduction

The research described in this chapter evaluates the antecedents of employee competence and its impact on information security job performance. In order to develop deeper understanding on the antecedents of employee competence, we undertake an in-depth case study to build a conceptual model that constitutes the antecedents of employee competence. The case study was done in a large public sector bank in India supervisors and retail executives were interviewed to gain better insight into what according to them contributed towards employee competence. The public sector bank was chosen for the study because banking industry in India is increasing its digital presence among the customers due to which bank employees have access to sensitive financial information of the customers and the bank. The bank also has a stringent Information Security Policy in place which elaborates information security as part of their job responsibility.

Over the past several decades there have been studies pointing to security breaches because of inability of employees to adequately perform their security work responsibilities (Backhouse and Dhillon, 1996; Spears and Barki, 2010; Dhillon et al., 2021; Dalal et al., 2022). Such studies have largely suggested extrinsic (Herath and Rao, 2009) or intrinsic (Dhillon et al., 2020) motivational strategies to ensure compliance with stated security policies. While studies have acknowledged the importance of security education training and awareness (SETA) programs (Puhakainen and Siponen, 2010; Hu et al., 2021; D'Arcy et al., 2009; Dhillon et al., 2020), there has been limited emphasis on developing competent individuals who perform *par*

excellence relative to their security jobs. In this research we argue that individual IS security competence leads to superior IS security job performance. Drawing on the extant literature we also argue that competence is an idiosyncratic combination of what Weick and Roberts (1993) terms as *know-how* and *know-that*.

Since the relationship between antecedents of individual competence and security job performance has not been well studied, at least in the IS security literature, we conduct our argument using a sequential mixed-methods approach (Venkatesh et al., 2013). Our study is situated in a large public sector bank in India. To explore the theoretical constructs of IS security competence and IS security job performance, we first undertake an in-depth interpretive case study. This allowed us to explicate the relationships between different constructs and develop our initial research model. The model is then tested through an extensive survey of employees in the same bank who are responsible for IS security. A similar approach has been adopted by other IS scholars, where sequential mixed methods design is used to validate a contextual model (see Patrick et al., 2021; Califf and Sarkar, 2020; Wunderlich et al., 2019). This research thus addresses the following overall research question:

How nurturing employee competence enhances IS security job performance?

5.2 The concept of information security compliance

The organization strategy literature helps us explain and enhance the competencies within organizations to achieve competitive advantage. These competencies also impact performance of the organization within the industry. Prior scholars have organized the strategy literature into two major paradigms: 1) the industrial organization economics paradigm emphasizes that certain organizations have ‘structural impediments to competitive forces’ that further helps them maintain competence, and 2) the idiosyncratic paradigm suggesting that organizations establish

‘distinctive competencies’ through a unique combination of tangible and intangible resources (Teece et al., 1991; Dhillon, 2008). Proponents of the organizational level competencies also argue that managers must identify and develop competence within an organization in a way that would lead to superior levels of performance and therefore sustained competitive advantage (Andreu & Ciborra, 2009).

What is of concern to us in this paper is how organizations can enhance employee information security performance, which would help generate a competitive advantage in data sensitive industries. In the dominant IS security literature, good security performance has often been equated to complying with IS security policies A principal mechanism through which IS scholars measure information security performance is evaluating the intentions of the individuals to comply with organizational IS Security Policies (Bulgurcu et al., 2010; Herath and Rao, 2009; Dhillon et al., 2020). IS security researcher have also focused on work-related behavior of employees (Stanton et al., 2006; Hu et al., 2011) and the role of SETA (Security Education, Training and Awareness) programs on building employee security knowledge and skills. Some prominent researchers also posit that organizations can improve IS security policy compliance by providing insights on what is IS security and how individuals can achieve it (Hu et al., 2021; D’Arcy et al., 2009; Puhakainen and Siponen, 2010). While these studies have rightly recognized that employees are an integral resource for improving the overall organizational security performance, there is still a limited understanding of how employee competence impacts IS security job performance.

5.3 Qualitative Case Study

5.3.1 Context – General Banking Sector in India

The growth in retail banking segment in India has been facilitated by the growth in banking technology and automation of banking processes that enable extension of reach and rationalization of costs. ATMs have emerged as an alternative banking channel, which facilitate low-cost transactions vis-a-vis traditional branches. Although it has the advantage of reducing branch traffic, it also makes the customers vulnerable to security frauds. Customers' growing use of digital channels for banking and their demand for an individualized experience has forced many banks to revisit their data and information security policies. In the face of increasing competition from emerging digital banks, which are redefining customer experience and luring younger customers, traditional public sector banks have been forced to leverage digital technologies to create a more rewarding customer experience. These comprehensive digital services have added to the sensitive data and information of customers that the bank now has access to.

Public and private sector banks have made significant investments in the realm of keeping the sensitive information secure through more stringent security policies for their customers and employees and developing security strategies that are better aligned with their business objectives and regulatory requirements. However, the more traditional public banks still struggle to ensure the security of sensitive data and information. (PMC bank fraud)

In order to better understand how these traditional banks can improve the performance of the employees to keep the sensitive customer and organization data secure, we conduct in-depth interviews with the employees of a public sector bank in India. We select this particular bank as it is a large, nationalized bank in India with a large financial asset and has huge, digitalized

networks that offer customers digital services like mobile banking, internet banking, and digitalized banking services. Interviews were conducted for key internal regular employees, including branch managers, front-end staff, and IT executives. We used semi-structured interviews to allow for flexibility in probing respondents.

5.3.2 Design and Procedure – Case of a Public Sector Bank in India

Alpha (pseudonym) is one of the leading public sector banks of India. Two other government-owned banks were amalgamated into Alpha in early 2020. The bank has a network of 9300+ domestic branches, 11800+ ATMs serving over 120 million customers with 77000+ employees. The financial assets of the bank are worth USD 160 billion. The bank offers numerous digital banking services to its customers and was among the first public sector banks in India to offer 'Anytime and Anywhere' banking along with Telebanking. In 2012, the bank inaugurated its first 'Talking ATM' specially made for the benefit of the visually challenged. To better serve the changing needs and demands of its customers, the bank offers digitalized services like online account opening, mobile banking, internet banking, online loan processing to name a few. As a large organization with access to sensitive customer data, the bank has an elaborate Information Security Policy in place which is reviewed yearly to keep pace with the technological developments. The Chief Information Security Officer (CISO) heads the Information Security Committee and reviews the Information Security Management Systems performance.

With regard to information security and security of the sensitive data that the bank has access to, the bank has detailed responsibility for every person within the bank that is part of the performance of the internal employees. For instance, the bank has outlined performance responsibilities for 'information owners' and 'information custodians' that includes maintaining

the accuracy, completeness, and integrity of the information. The bank evaluates these performance responsibilities regularly to avoid potential information security breaches and incidents.

5.3.3 Analysis and Findings – Security job performance in Alpha Bank

The interviews are structured based on Woodside (2013) guidelines. Participants are asked some basic questions related to their job profiles to make sure that they fit the criteria of information security context. Interviews are conducted in a written format and have open-ended questions. Once the data is collected, the empirical analysis is performed by an iterative process of reading the responses, coding, and interpreting the interviews (Myers & Newman, 2007). The analysis is used to develop the hypotheses and the research model.

The in-depth case study of Alpha Bank presents some interesting aspects that contribute to and are critical for enhancing information security outcome of the employees. In Table 8, we present a few sample responses from the qualitative interviews.

Table 8. Sample interview quotes for emergent concepts: Employee competence

Emergent Concepts	Definition	Interviewee	Sample interview quotes
Tacit knowledge	The knowledge is embedded through experience and insights - (Knowing-how)	Branch Manager	*"…employees who come with first-hand experience in information security somehow are able to deal with customer information and queries more effectively…"*
		Retail banker	*"…I generally reach out to my colleague who have experience in dealing with the issues that I face regarding customer information and data…"*
		IT executive	*"…it is really easy to train and educate employees who have an internal interest in organization's information security and according to me these are employees who join with prior experience…"*
Explicit knowledge	The knowledge is codified and recorded so it	Bank Operations Manager	*"…We ensure that at a branch level, all the employees have access to the security policies*

	can be shared - (Knowing-that)		*and responsibilities so that each individual is sure of what and how to comply with…"*
		Information Security Officer	*"…Regardless of the job and designation, employees are more clear about their responsibilities through the security policy statements that are also updated regularly…"*
		Cashier	*"…I can better perform my duties when I have a written policy of the organization with me that I can refer to…"*
Purposeful heedful interactions	When facts and knowledge are communicated and incorporated into the group's collective mind	Regional Manager	*"…I have found that branches with best performance work as effective groups where the managers interact with their subordinates on a regular basis and have daily huddle sessions…"*
		Loan Officer	*"…I have personally learned the most about the details of my organization's security policies by interacting with other colleagues and my manager…"*
		Information Security Executive	*"…we always encourage managers and executives to have regular interactions about the latest security enhancements and policies so the other members know whom to reach out to if needed…"*

Determinants of Employee Competence

Employees feel more confident and assertive when the security responsibilities are communicated to them through formal or informal ways (Williams and Anderson 1991). These interactions also result in improving not just the know-how and skills - tacit knowledge - of the employees but also helps them better conceptualize the process of keeping the information secure through explicit knowledge (Puhakainen and Siponen 2010). This leads to employees feeling more competent about their information security responsibilities.

The employees with tacit knowledge will be able to show better information security competence based on their previous insights and skills developed through skills. Explicit knowledge that is based on the codified knowledge also encouraged employees to be more competent towards their security performance (Bock et al. 2005).

At Alpha Bank, the information security policies are formulated and documented at the Bank Headquarters and are then made available to all employees through the Bank's internal system. All employees are expected to go through the security policies regularly as they are modified and updated on a need basis and to remain compliant with the security policies of the central bank. At the branch level - the basic unit of operations - the security policies are discussed by the Branch Manager so that employees who deal with sensitive customer data on a daily basis do not fail in maintaining the confidentiality and integrity of the information. To highlight the importance of these interactions, the Regional Manager of the bank commented:

> …I have found that branches with best performance work as effective groups where the managers interact with their subordinates on a regular basis and have daily huddle sessions reiterating the importance of following the bank's security policies…this improves the knowledge of the employees...

These interactions have a specific purpose to achieve that is critical to the functioning of the bank. The Information Security Managers fulfill their responsibilities by making sure that the security policies are current and can be deciphered easily even the front-end employees who may not have enough exposure to IT security. However, adequate compliance with the policies can only be achieved if the employees abide by them. Over a period of time, the IS managers have also realized that interactions among employees improve the performance towards keeping information safe. The IS manager explained:

> …we always encourage experienced managers and executives to have regular interactions about the latest security enhancements and policies, so the other staff members know whom to reach out to if needed…they feel more confident to ask managers with experience...

The importance of the interaction among different stakeholders of the bank exclusively on how best to keep the information secure and comply with the security policies was also highlighted by the employees who manage the information. The Loan Officer, who has access to critical customer data noted:

> …I have personally learned the most about the details of my organization's security policies by interacting with other colleagues and my manager…the experiences shared by my manager add to my knowledge...

Therefore, the doubts and dilemma of the employees as to how crucial it is for them to comply with security policies is taken care of by the interactions amongst employees with varied job responsibilities. Employees feel more confident and assertive when these security responsibilities are communicated to them through formal or informal ways. These interactions also result in improving not just the know-how and skills of the employees but also helps them better conceptualize the process of keeping the information secure. Information security within an organization is a process, dysfunction of which causes a security incident.

Within the context of the bank, employees with better knowledge about the security policies and who came with experience showed higher levels of confidence in performing their security jobs. It was evident that different stakeholders explicitly mentioned how their past experiences along with the policy guidelines of the bank helped them in being more vigilant about the sensitive data and information. A Branch Manager commented:

> …employees who come with first-hand experience in information security somehow are able to deal with customer information and queries more effectively…experienced employees contribute to branch performance by sharing

their experiences with subordinates which encourages them to ask more questions...

Although the Branch Managers would have regular meetings and sessions with other employees of the branch to convey the security policies of the bank, there was a disconnect among the front desk employees as to how the security policies worked in the bigger scheme of things. This disconnect seemed to be resolved through the interactions they had with their managers and other colleagues that came with prior experience. Through the experience, they were able to share insights on how following some basic steps like verifying the ID of the customer asking for account details and fulfilling know-your-customer formalities could avoid information frauds at a branch level. This was reiterated by the information security officer as well as they emphasized the ease to train employees who come with prior experience. An IS executive explained:

> …it is really easy to train and educate employees who have an internal interest in organization's information security and according to me these are employees who join with prior experience…

Consistent with Venkatesh et al. (2013), the statements from the interviews helped explore the different concepts that have been highlighted in Table 8. These concepts complement the extant research on competence and its antecedents. Most importantly, our findings from the in-depth case study highlighted the important concepts of tacit knowledge, explicit knowledge and purposeful heedful interactions in the context of information security competence. Managers and IT executives emphasized that when employees felt more competent to perform their duties to keep data and information safe when there were purposeful heedful interactions among the

members of the branches. Our qualitative study also suggested that tacit and explicit knowledge of the employees is integral in building employee competence.

5.4 Emergent Conceptual Model and Hypotheses

5.4.1 Purposeful heedful interactions

Based on the case of the Alpha Bank, we observed that the managers had made a strong case for purposeful heedful interactions among the bank staff members. Constructive conversations among the bank employees during the work hours of the organization had an impact on the competence of the employees that was mentioned by the supervisors and managers. When the employees of the bank, especially the new joining members were told about the benefits and importance of following the bank's security policies, they felt more confident in the knowledge that they already had.

These heedful interactions were not just beneficial to individual employees, but also improved the group competence of the management group of the branch. The group was more informed about the security policies that were to be followed at a branch level. Therefore, these interactions added to the knowledge that the employees already possessed through their past experience along with details of this particular organization. Hence, we hypothesize:

H1a: Purposeful heedful interactions among employees positively influences tacit knowledge.

H1b: Purposeful heedful interactions among employees positively influences explicit knowledge.

5.4.2 Tacit knowledge

Individuals that work at an organization do possess the know-how based on their past experiences and understandings. In the context of organizational level competencies, the

individual know-how and skills include the knowledge and perspectives that the employees of the organization bring with them. In Alpha Bank, we observed that employees who came with a better knowledge about the security policies and importance of following the organizations' security regulations, felt a better sense of competence to abide by those regulations. Even the managers and supervisors of these employees agreed to the advantage of having prior tacit knowledge. Based on this, we hypothesize:

H2: Tacit knowledge positively influences employee competence.

5.4.3 Explicit knowledge

Explicit knowledge can help employees within an organization share valuable information with their coworkers and superiors. Transferring explicit knowledge to others with the organization allows employees to learn new information that can help them to do their jobs effectively, thus reducing errors and chances of information leak. In our qualitative study at Alpha Bank, the managers suggested that having access to the bank information security policies helped the employees make better decisions towards their roles and responsibilities. It was also highlighted that employees could share their explicit knowledge and understandings with other members of the branch and made them feel more competent towards their duties. Through purposeful interactions among the branch employees, they were able to create a source of collective knowledge that enhanced employee competence. Hence, we hypothesize:

H3: Explicit knowledge positively influences employee competence.

5.4.4 Information security job performance

According to the qualitative study and the theoretical lens of competence, more competent employees are able to perform their job responsibilities better (Holtkamp et al., 2014). When employees who are handling sensitive organizational and customer data feel more

competent towards fulfilling their duties well, they will make sure they understand the security protocols and policies well so that information security is maintained. Also, competent employees share their knowledge and experiences with their fellow coworkers so that the entire team or group is able to perform at their optimum levels through this shared knowledge. Based on this understanding, we hypothesize:

H4: Higher the employee competence, higher will be security job performance of employees.

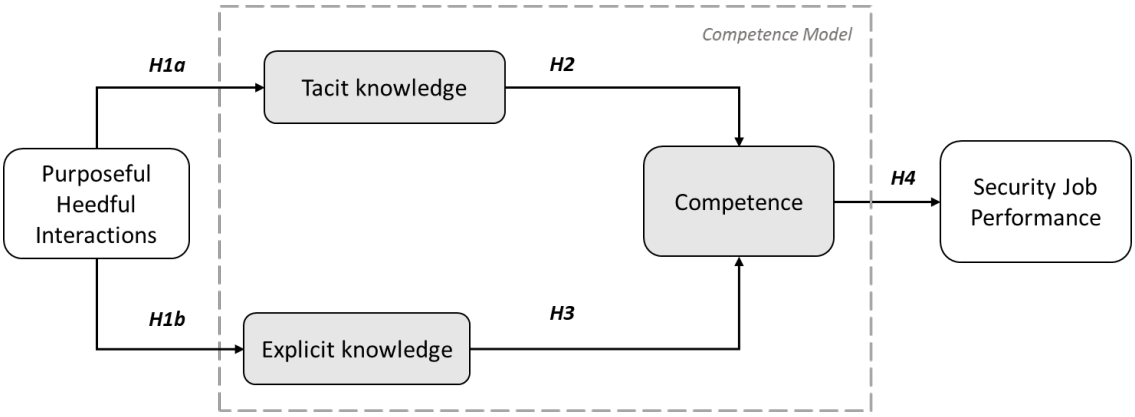
The hypotheses for employee competence study are summarized in Table 9.

Table 9. Summary of hypotheses: Employee competence

Hypotheses	Description
H1a	Purposeful heedful interactions among employees positively influences tacit knowledge. When employees have purposeful and heedful interactions with other co-workers, they are able to better share and enhance the know-how.
H1b	Purposeful heedful interactions among employees positively influences explicit knowledge. When employees have purposeful and heedful interactions with other co-workers, they are able to better share codified knowledge.
H2	Tacit knowledge positively influences employee competence.
H3	Explicit knowledge positively influences employee competence.
H4	Higher the employee competence, higher will be security job performance of employees.

We present our complete research model in Figure 7. While the focus of our qualitative case study is on understanding and determining the components of employee competence, specifically in the context of information security job performance, our quantitative study tests the impacts of these components on information security job performance. Therefore, this study encapsulates the understanding of employee competence by first focusing on the factors that determine employee competence and then empirically testing the impact of these constructs on information security job performance of employees.

Figure 7. Research model: Employee competence



5.5 Empirical Analysis

Our proposed quantitative study is based on explanatory survey research (Malhotra & Grover, 1998). For our empirical study, we follow Malhotra and Grover (1998) guidelines for conducting survey research. In accordance with Hair et al. (2019) suggestions, this study analyzes the observations and tests the research hypotheses using partial least squares based structural equation modeling (PLS-SEM). After developing the instrument in Qualtrics survey software, we pretest the questionnaire with four doctoral students from the business school. Based on the feedback received from the pretest, we revise the questions for better clarity of context and validity. After finalizing the initial questionnaire, we run a pilot study with 35 bank employees.

5.5.1 Design and procedure

After designing and developing our final survey questionnaire, we make the questionnaire available online by using the Qualtrics online software. The final questionnaire demonstrated validity and reliability of the instrument. We collected our data by distributing the online questionnaire to the bank employees and the responses were collected through the Qualtrics software. The survey instrument for the study includes 65 items that are adapted from

the extant literature. The measurement items for the constructs are adapted from published literature on competence and information security job performance (see Appendix B). We measure all constructs using a 7-point Likert scale (ranging from 1-Strongly disagree to 7-Strongly agree).

Data collection occurred between July and December 2021. We started with our exploratory data collection for 35 participants for a pilot. The pilot reveals that the scales are reliable and valid. Through the online Qualtrics survey, we collected responses from 356 bank employees. On average, the participants took about 15 minutes to complete their response. We examined the common method bias (CMB) using two techniques: (1) Harman's one-factor test to identify common method variance (Podsakoff et al., 2003); (2) PLS Marker variable approach to analyze data contaminated with method variance (Lindell and Whitney, 2001). The former confirmed that none of the factors individually explain the majority of the variance. The latter added a theoretically irrelevant marker variable in the research model, obtaining 0.008 (0.8%) as the maximum shared variance with other variables, a value that can be considered low. Hence, no significant CMB was found.

The respondents were 61% males, 39% females, and between 26 and 54 years. The majority of them were highly educated (49% with a bachelor's degree, and 27% with post-graduate degree).

5.5.2 Analysis

In this study, we use partial least squares (PLS) regression to conduct our analysis. Prior literature suggests that PLS approach works well if the research model has not been tested in prior studies and if it is necessary to prevent restrictive distributional assumptions when determining path coefficients that are significantly different from zero (Lathan et al., 1979;

Fornell and Bookstein, 1981). Hence, we use Smart PLS 3.3.3 to empirically estimate our research model (Ringle et al., 2012).

Measurement Model

A measurement model analysis is conducted to assess the construct reliability, convergent validity, indicator reliability, and discriminatory validity of scales for the reflective constructs. Construct reliability was tested using composite reliability (CR). The CR results were higher than 0.7 for all constructs, which indicates the internal consistency and appropriateness of the constructs (Straub, 1989; Henseler et al., 2009). Convergent validity was demonstrated using the average variance extracted (AVE). The AVE values are higher than 0.50 for all constructs (Table), and thus the convergent validity of the measurement model is established. For indicator reliability, the loading should be higher than 0.7 (Henseler et al., 2009). We see that all loadings are higher than 0.7, and consequently, the reliability indicator is satisfied.

Table 10. Descriptive statistics, correlation, composite reliability (CR), and average variance extracted (AVE)

Construct	Mean	SD	CR	PHI	TCK	EXK	COMP	PERF
Purposeful heedful interactions (PHI)	0.678	0.542	0.926	**0.871**				
Tacit knowledge (TCK)	0.590	0.328	0.935	0.092	**0.821**			
Explicit knowledge (EXK)	0.361	0.533	0.941	0.129	0.287	**0.917**		
Competence (COMP)	0.573	0.476	0.938	0.423	0.223	0.159	**0.914**	
Information Security Job Performance (PERF)	0.520	0.205	0.893	0.203	0.185	0.082	0.273	**0.822**

Notes: Values in diagonal (bolt) are the AVE square root; standard deviation (SD).

To evaluate the discriminatory validity, we use three criteria: (1) Fornell-Larcker matrix, (2) Cross-loadings, and the (3) Heterotrait-Monotrait ratio (HTMT) (Henseler et al., 2009). In the

Fornell-Larcker criterion, we examine each construct's discriminant validity using the correlation between constructs and the root square of the AVE. As shown in Table above, the AVE square root of each construct (diagonal elements) is higher than the correlations between the constructs. Hence, the first criterion for the constructs' discriminant validity is supported. Using the criteria of Cross-loading numbers (see Appendix D), we determined that all the loadings of the constructs were higher than the cross-loading numbers (Chin, 1998). Finally, based on Table 11, all values of Heterotait-Monotrait ratio (HTMT) are lower than the threshold of 0.9, except for explicit knowledge. Therefore, the discriminant validity of the constructs is confirmed.

Table 11. Heterotrait-Monotrait Ratio (HTMT): Employee competence

Construct	PKI	TCK	EXK	COMP	PERF
Purposeful heedful interactions (PHI)					
Tacit knowledge (TCK)	0.662				
Explicit knowledge (EXK)	0.835	0.838			
Competence (COMP)	0.880	0.684	0.901		
Information Security Job Performance (PERF)	0.738	0.724	0.738	0.847	

Structural Model

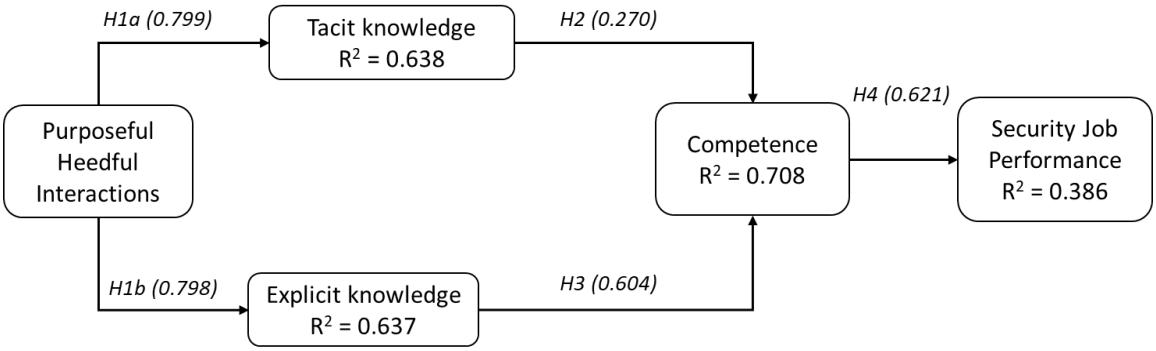
We test the multicollinearity of all constructs before assessing the structural model. For that we use variance inflaction factor (VIF). Our results show all the construct VIFs show the absence of multicollinearity among the variables (Hair et al., 2019). The structural model results are presented on Figure 8. The statistically significance level of path coeficients were performed using bootstraping with 5000 resamples.

Our model explains 63.8% of the variation in tacit knowledge. We hypothesize purposeful heedful interaction is positively associated with tacit knowledge. We found the association between purposeful heedful interaction and tacit knowledge ($\hat{\beta} = 0.799$; $p < 0.05$) to be statistically

significant as hypothesized.

Our model explains 63.7% of the variation in explicit knowldge. We hypothesize that purposeful heedful interaction is positively associated with explicit knowledge. We found the association between purposeful heedful intercation and explicit knowledge ($\hat{\beta}$ = 0.789; p < 0.05) is statistically significant as hypothesized.

Figure 8. Structural model: Employee competence



Our model explains 23.3% of the variation in competence. We hypothesize tacit knowledge and explicit knowledge are positively associated with competence. We found the associations from tacit knowledge to competence ($\hat{\beta}$ = 0.270; p < 0.05), and explicit knowledge to competence ($\hat{\beta}$ = 0.604; p < 0.05) are statistically significant.

Finally, our model explains 38.6% of the variation in information security job performance. We hypothesize employee comptence is positively associated with information secuirty job performance. We have found the associations from comptence to information job performance ($\hat{\beta}$ = 0.621; p < 0.05) as statisfically significant.

Table 12 below sumarizes the supported hypotheses along with direct and total effects.

Table 12. Bootstrapping result for structural model: Employee competence

	Hypotheses	Hypothesized Direction	Direct effect	Total effect	Conclusion
H1a	Heedful Interaction → Tacit Knowledge	Positive	0.799	0.799	**Supported**
H1b	Heedful Interaction → Explicit Knowledge	Positive	0.798	0.798	**Supported**
H2	Tacit Knowledge → Competence	Positive	0.270	0.270	**Supported**
H3	Explicit Knowledge → Competence	Positive	0.604	0.604	**Supported**
H4	Competence → Information Security Job Performance	Positive	0.621	0.621	**Supported**

p-value < 0.05

5.6 Contributions

5.6.1 Theoretical Contribution

In this study we set out to investigate the factors that are vital in building employee security competence and its further impact on IS security job performance. We found that employee competence is a complex construct and presence of both tacit and explicit knowledge along with purposeful interactions helps employees accomplish higher security competence, thus improving employee IS security performance. In this section we discuss the theoretical and practical implications of our findings.

First, we enhance the current understanding of the role that SETA programs play in increasing IS security job performance. This is particularly of value since, as Hu et al., 2021 note, concerns around SETA programs not being sufficient and "very-effective" is on the rise. While most organizations have a SETA program that is important to mitigate security risks in organizations, the effectiveness of these programs is questionable as employees continue to

engage in unsafe IS security practices. A possible solution to boost IS security performance is to focus on the tacit and explicit knowledge of employees that will result in higher competence. Our study contributes to this ongoing effort of understanding how to improve employee competency and knowledge towards IS security roles and responsibilities that consequently results in better security performance. We build on the conceptualization of competence (Weick and Roberts, 1993; McGrath et al., 1995) and operationalize the construct in the domain of IS security. In doing so, this study extends prior research on building the skills and knowledge of employees as related to IS security threats and risks. We believe that our conceptualization of employee competence and IS security job performance will be useful in guiding both research and practice in tailoring IS security measures that encourage effective security.

Second, this study contributes to the IS security literature by exploring the construct of employee competence. While competence as a construct has been well studied in the strategic management domain and is a crucial resource for competitive advantage (Dhillon, 2008; Bhatt and Grover, 2005) and organizational performance (Peppard and Ward, 2004), its role in IS security needs further understanding. In this regard, we undertake an in-depth interpretive case study in a large public sector bank in India. Our qualitative study with the bank employees suggests that when employees interact with other group members, they are able to better comprehend the organization's vision towards security performance and feel more capable of handling information security pressures. This further helps them connect the knowledge gained through past experiences with the newer security technologies and procedures of the organization, thus giving them a sense that they are competent to keep the information safe and deal with a security threat if need arises.

5.6.2 Practical Contribution

From a practitioner's perspective, our findings provide valuable insights that security managers and executives can utilize to enhance employee security performance. First, this study suggests that organizations also need to focus on improving employee competence along with providing their enough training and awareness. Simply providing instructional tools to understand an organization's IS security policy might not be sufficient. Managers must leverage the employee knowledge gained through past IS security experiences and encourage a group mindset towards handling IS security responsibilities. Second, our results show that heedful interactions among employees at different hierarchical levels impacts the competence of employees. They are able to interrelate their cognitive understanding of past IS security experiences along with acquired security skills and training to do the "right thing" to fulfil their security responsibilities. Lastly, our findings also strongly suggest that competent employees demonstrate a higher sense of responsibility towards their security jobs. A recruitment strategy that focuses on hiring individuals that display higher levels of competence could substantially reduce the risks of IS security incidents that are waiting to happen.

5.7 Conclusion

This chapter attempted to describe in detail the second study of this research where the main objective was to explore the antecedents of employee competence and empirically test the impact of employee competence in information security job performance. The study was conducted using a sequential mixed-methods approach as discussed in Chapter 3. In in-depth case study was conducted in a large, public-sector bank in India where we interviewed employees across three groups (managers, retail executives, and IT executives) to find out what according to them contributed towards employee competence. The factors that emerged from the

analysis of the first part of the study were *tacit knowledge*, *explicit knowledge*, and *purposeful heedful interactions*. Furthermore, we empirically tested the research model. The findings from both the qualitative and quantitative studies revealed that managers in the bank considered that competent employees perform better in their information security jobs and responsibilities. This is more than mere compliance with the bank's information security policies. For instance, purposeful heedful interactions among the managers and their subordinates in the bank led to the executives feeling more confident of handling information security queries of the customers. They also felt more competent to deal with an information security threat and better followed cybersecurity practices and protocols that is part of their job responsibilities. Competent employees are surely an asset to an organization as they help in achieving the long-term organizational security goals.

CHAPTER VI: INTERPRETING IMPACT OF THRIVING AT WORK AND EMPLOYEE COMPETENCE ON INFORMATION SECURITY

6.1 Introduction

This chapter brings together the important implications of the two conceptualizations studied in this research, namely thriving at work and employee competence. Although, information security literature in the past has explored various approaches for protecting and mitigating the threats to the information assets within organizations, this research investigates two different constructs. More specifically, the aim of this research is to investigate the impact of thriving at work and agentic work behaviors on information security job performance and enhancing employee competence. Previous chapters described how that data were collected and analyzed. This chapter takes the results of these data analyses and interprets them in the context of our overall research question.

6.2 Evaluation of Thriving at Work and Agentic Work Behaviors

Thriving describes an individual's experience of learning and vitality in the work situation. Organizational studies have captured and studies thriving in various work contexts. Thriving is an important domain as it also highlights the perspective that individuals have a sense of self-regulation and drive the outcome through the idea of learning and vitality. In the first study, we explore thriving at work in the context of information security. Information security job performance of employees is a valuable outcome that could enhance the overall information security performance of the organization. This could be case as employees who are able to perform their information security job roles and responsibilities well would be an asset to the organization in curbing information security incidents like data breaches and cybersecurity

attacks. It is even more crucial as remote working has become more prevalent and thus employees must perform their security tasks, like being vigilant about phishing emails and follow and respect the information security policies and procedures laid down by the organization.

To better explore the factors that could enhance the information security job performance of the employees in a work situation, this study used a sequential methodology where the first step was to conduct an in-depth case study in a nationalized bank in India to develop a conceptual understanding of the what the managers and employees considered as important factors towards improving their security job performance. This was followed by a qualitative analysis of the research model. The results of the study showed that employees who have a sense of thriving are able to perform better towards their security job performance through enhanced task focus and heedful interactions with other colleagues in the bank.

In the following sections, we elaborate on the different factors that contribute to information security job performance of employees in the bank through thriving at work and agentic work behaviors. The findings show that agentic work behaviors of task focus and heedful interactions contribute to the sense of thriving and further has a positive impact on the performance outcome of employees. When thriving, employees tend to focus on their work tasks and heedfully interact with their colleagues and mangers in order to produce efficient and precise results and performance.

6.2.1 Thriving and information security outcomes

Thriving as a construct has been well studied in the organizational studies field. In their initial works Spreitzer et al (2005) described how thriving at work is different from other feelings of wellbeing and resilience among individuals. The key distinguishing characteristic of

thriving at work is the combination of learning and vitality. Both these factors are necessary for employees to thrive in the work situation. In the context of information security this manifests as constantly learning and growing in regard to the information security practices and procedures that are most relevant to the bank. Alpha bank, a large, nationalized bank in India has been investing rapidly in the digitalization of their banking processes for the organization as well as the customers.

In the last few years, the bank updated their information security policies on a regular basis to ensure that sensitive financial information of the customers was safe in the hands of the employees handling it. For example, a bank executive was now able to have access to sensitive financial data of all the customers of the bank at the click of the button. This sensitive financial information included Credit card details, details of financial transactions made in the last ten years, mortgage details, and some personal identifiable information like Name, Date of birth, Govt ID number and their signatures. As inappropriate access to this information could cause financial as well as personal damage to the customers, it is essential that bank employees take all measures to handle this information with care and keep it secure. There have been instances in bank branches where employees were observed to share their work passwords or personal identifiable information of some known acquaintances even though there are stringent rules against doing so. Furthermore, it is part of the job responsibility of the bank employee to ensure that bank and customer information, which is part of the information asset of the organization, must be kept secure at all times. Although the bank employees undergo security training, the information breach incidents through the employees continue to take place.

In the case of the Alpha bank the scenario presented above came to light through interviews conducted with employees from different work groups. Managers of the bank

identified that learning was directly related to the security performance of the employees. For instance, employees who would regularly read the e-mails sent by the IT and information security department, would adhere to even the small practices like non sharing of work password. These employees would also take small but essential steps like locking their work computers before leaving their assigned seats in the bank. Thus, following these basic information security practices was considered a step towards curbing information security incidents at the branch level. Managers in the IT and information security department also reported that employees who are constantly learning about information security at the bank also apply their new knowledge and skills in their tasks. These attributes in the employees result in better job performance which in this case also includes reducing information frauds in the bank. Some of the bank employees who were interviewed reiterated this point.

6.2.2 Agentic work behaviors

At the branch level the Alpha bank employees recognize that focus towards the bank tasks contributes to their information security job performance. The rationale behind this is that the employees who focus more on their tasks are more attentive and alert during the performance of their work-related t asks. They utilize their cognitive, emotional, and physical capacities to ensure that they are able to fulfil their work roles and responsibilities. For instance, Branch Managers reported that the high performing employees in the bank are the ones who fully engage in the task at hand by voluntarily and intentionally driving their cognitive energy into the work task. Interestingly to ensure task focus, the information security department at the bank would intentionally send fraudulent URL links to the email IDs of the bank employees. It was observed that employees who were more focused towards their bank tasks assigned during the day were able to identify these fraudulent links and did not open them. Another active step to ensure better

security performance of the employees was the regular testing of employee knowledge in the form of quiz. The results of these activities were reported not just to the branches but were circulated at the national level. In the interviews conducted with the managers and the employees the above point was highlighted clearly.

Discussions with the managers and employees at the bank revealed an interesting component that encouraged learning and application of knowledge among the employees. One of the employees commented and said, "learning is equal to interesting conversations with my manager and fellow colleagues". Implicitly this meant that attentive and conscious interactions among bank employees enhanced their information security learning process which is ever evolving. The employee also said that these interactions made him cognizant of the probable information security threats at the branch levels. One such specific instance was narrated by the employee where the manager of his branch shared with him an information security breach incident. In his previous branch the branch manager had witnessed an information security lapse. The lapse came to light when one of the customers came to the bank to claim the money in his Fixed Deposit Account. The Fixed Deposit Account of the customer was created two years back by two bank employees without debiting the actual money from the customer's account. The investigation of this lapse brought to light that a major information security practice was not followed. One of the bank employees whose system ID was used to create the Fixed Deposit Account was not present in the bank at that time. The employee had shared his password with another colleague which at times is considered an acceptable practice. When the branch manager shared this incident with his current employees, they paid heed to it and reported that it was a moment of learning for them. Some of the branches of the Alpha bank have recently started the practice of having '*huddle sessions'* where managers and other employees are encouraged to

share these experiences which promote learning related to better information security procedures and due diligence among employees.

6.2.3 Individual enablers contribute to thriving

With respect to the employees in the Alpha bank, their sense of resilience and optimism was shown to impact their learning and skills. Psychological resources like hope, resilience and self-efficacy were reported to promote thriving at work in the context of information security performance of employees. Positive psychological aspects promote individual behaviors in a positive manner and thus contribute to higher work performance. In the case of Alpha bank, it was observed by the managers that employees with higher positive psychological resources like resilience and optimism were able to better handle the information security challenges. For instance, an information security manager said that bank employees can make a security error as they handle close to 150-200 customers on a busy day. However, bank employees who have a sense of resiliency and optimism are quick to learn from these minor errors. The information security manager was able to report this based on a report generated by the information security department which includes the data about these minor errors. The bank keeps a track of security errors made by employees and sends them an email the next day. For instance, if a bank employee tries to open a URL link through the bank's secure network, the employee along with the branch manager would receive an email the next day. Another interesting incident that came to light during the interview was when one of the information security officers visited a bank branch posing as a dummy customer and tried to get some sensitive financial information of an acquaintance. The bank employee assumed that the gentleman was authentic and agreed to share the information. Later during the day, the bank employee and his branch manager received an email that if gone unchecked, such lapses could lead to more serious information security

incidents. The bank employee showed a sense of optimism and was quick to learn his lesson. The information security department kept a track of this employee and did not see the security lapse from his side. On the other hand, the department has also observed that employees with a negative psychological inclination continue making the security errors.

6.3 Evaluation of Employee Competence

In the second study we set out to investigate the factors that are vital in building employee security competence and its further impact on IS security job performance. We found that employee competence is a complex construct and presence of both tacit and explicit knowledge along with purposeful interactions helps employees accomplish higher security competence, thus improving employee IS security performance. In the following sections we discuss the theoretical and practical implications of our findings.

6.3.1 A step beyond Security Education Training and Awareness (SETA)

Through this research we enhance the current understanding of the role that SETA programs play in increasing IS security job performance. This is particularly of value since, as Hu et al., 2021 note, concerns around SETA programs not being sufficient and "very-effective" is on the rise. While most organizations have a SETA program that is important to mitigate security risks in organizations, the effectiveness of these programs is questionable as employees continue to engage in unsafe IS security practices. A possible solution to boost IS security performance is to focus on the tacit and explicit knowledge of employees that will result in higher competence. Our study contributes to this ongoing effort of understanding how to improve employee competency and knowledge towards IS security roles and responsibilities that consequently results in better security performance. We build on the conceptualization of competence (Weick and Roberts, 1993; McGrath et al., 1995) and operationalize the construct in

the domain of IS security. In doing so, this study extends prior research on building the skills and knowledge of employees as related to IS security threats and risks. We believe that our conceptualization of employee competence and IS security job performance will be useful in guiding both research and practice in tailoring IS security measures that encourage effective security.

6.3.2 Impact of employee competence on performance outcome

This research contributes to the IS security literature by exploring the construct of employee competence. While competence as a construct has been well studied in the strategic management domain and is a crucial resource for competitive advantage (Dhillon, 2008; Bhatt & Grover, 2005) and organizational performance (Peppard & Ward, 2004), its role in IS security needs further understanding. In this regard, we undertake an in-depth interpretive case study in a large public sector bank in India. Our qualitative study with the bank employees suggests that when employees interact with other group members, they are able to better comprehend the organization's vision towards security performance and feel more capable of handling information security pressures. This further helps them connect the knowledge gained through past experiences with the newer security technologies and procedures of the organization, thus giving them a sense that they are competent to keep the information safe and deal with a security threat if need arises. We also empirically tested our research model developed from the case study to study the impact of the antecedents of employee competence on information security job performance. Our empirical results indicate that employees with a higher sense of competence demonstrate better performance at their security jobs and feel more confident in handling their security responsibilities. Finally, employees with higher levels of security competency and performance could be the core building blocks of an organization to reduce data breaches and

cyber incidents. To further validate our theoretical claim, one of the managers of our focus group commented:

> …In this branch we asked our employees to share with their colleagues one important daily practice to keep customer data safe. For the Loan officer, it was having a strong password for his Finacle account and not sharing it with his colleagues when he is not at his desk…the practice of sharing passwords among colleagues reduced in the branch after this exercise…this is mentioned in our bank's security policy…

Another theoretical implication of this research is the contribution to the behavioral IS security literature by exploring the conceptualizations of employee competence and IS security job performance which have not been studied previously. As discussed in the literature review section, prior IS security literature has rightly found that human and behavioral aspects are important features of IS security (Crossler et al., 2013; Dhillon et al., 2021). Although Backhouse and Dhillon (1996) do emphasize the importance of individual responsibility and accountability for effective IS security, not many studies have further investigated this aspect. In addition, Dhillon et al., (2021) present the opportunity for advancing IS security research around the *people* component of the socio-technical system to further understand the interactive nature of IS security threats. Dhillon et al., (2021) note:

> Current emphasis [of IS security research] has focused on individual elements of the socio-technical system. …. while focusing on structures, people, technology, and tasks was important, IS security attacks typically occur when the subsystems interact (pg. 13).

In response to the calls made by IS security scholars, we investigate the notion of individual security competence is intricately linked to individual security performance. Employee security competence is a consequence of what Weick & Roberts (1993) describe as *know-how* (employees' tacit knowledge including their experience) and *know-that* (explicit knowledge including technology skills and access to security knowledge). It also encompasses the element of heedful interactions (in terms of interrelating and comprehending security responsibilities as a group) that improves comprehension of security task at hand. Consequently, competent employees have a higher level of security performance at a practical level.

6.3.3 Competent employees and management

From a practitioner's perspective, the findings of this research provide valuable insights that security managers and executives can utilize to enhance employee security performance. First, this study suggests that organizations also need to focus on improving employee competence along with providing their enough training and awareness. Simply providing instructional tools to understand an organization's IS security policy might not be sufficient. Managers must leverage the employee knowledge gained through past IS security experiences and encourage a group mindset towards handling IS security responsibilities. Second, our results show that heedful interactions among employees at different hierarchical levels impacts the competence of employees. They are able to interrelate their cognitive understanding of past IS security experiences along with acquired security skills and training to do the "right thing" to fulfil their security responsibilities. Lastly, our findings also strongly suggest that competent employees demonstrate a higher sense of responsibility towards their security jobs. A recruitment strategy that focuses on hiring individuals that display higher levels of competence could substantially reduce the risks of IS security incidents that are waiting to happen.

6.4 Conclusion

This chapter discussed the implications of the findings of this research which set out to evaluate the information security job performance of employees in a work situation with focus on the concepts of thriving and competence. In a more general sense, this research found that employees, across three work groups, at the bank reported that their information security job performance improved when they were more agentically inclined towards their jobs. At the bank, these employees handle sensitive financial information of the customers on a daily basis and therefore, must adhere to the stringent information security rules and protocols of the bank. But mere compliance to the information security policies is not sufficient to achieve the overall bank's information security goal. The employees are also expected to integrate the security processes, like avoiding unauthorized modification of the financial data, that is part of their job responsibility. Furthermore, this research also found that competent employees, who applied both tacit and explicit knowledge to their work, perform better in their information security job component.

CHAPTER VII: CONCLUSION

7.1 Introduction

Information security research for many years has been focusing on finding ways to enhance the security outcome of individuals at workplaces and continues to do so. More recently, behavioral information security research has started focusing on deeper understanding individual and employee behaviors which manifest in protecting organizational information and information assets (Crossler et al., 2013). Most of these empirical studies have investigated the behavioral factors and attitudes of individuals, employees and end-users within an organization that handle the information assets (Siponen and Vance, 2010; Bulgurcu er al., 2010; Hu et al., 2011). A vast majority of these empirical studies have investigated the negative behaviors which are generally labelled as information security policy non-compliance. In this research, we explore a step further from the compliance behavior of employees in a work situation.

Our overall research is based on the argument that information security roles and responsibilities of employees are not restricted to just the compliance with the stringent security regulations and protocols. Employees must be cognizant of the connection between the information and the processes to keep the information safe and secure based on their access and authorization. We recognize that information security job performance is a more elaborate for evaluating the information security outcome of employees. It can be predicted through the elements of psychological resources, learning and competencies of the employees towards information security.

7.2 Overview

The overall objective of this research has been to expand the information security literature beyond the realms of security policy compliance of the individuals and end-users. Information security within organizations is not just restricted to employees complying with the stringent information security regulations and protocols abut also encapsulates the information assets and security processes that are aligned to overall information security goals of the organization. Information security job performance is an interesting and essential criterion as it encompasses the security outcomes of the employees relevant to the organization's security processes.

The research deployed a sequential mixed-method approach to examine the behavioral antecedents of information security job performance of employees in a work situation. The goal was to explore the information security outcome of performance, which has not been deeply studies in the context of information security. The conceptualizations of thriving at work and employee competence provided the theoretical lens used as the starting point of the conceptual framework. These theoretical underpinnings were used as these conceptualizations have been well explored in the organizational studies domain but not in information security. The first phase of the qualitative in-depth case study was conducted to develop a deeper understanding of the constructs in the conceptual model and to hypothesize the relationship of the constructs. This was followed by empirically testing the research model and the hypotheses using survey-based approach. Overall, in this research, we focus on two broad conceptualizations, namely, thriving at work and employee competence that influence information security job performance of employees.

7.2.1 Thriving at work and agentic work behaviors

Thriving at work is a factor that has been well explored in the organizational studies domain and encompasses an individual's experience of learning and vitality in the work situation. In this research, we focus on the aspect of thriving as it leads to performance outcome. In the realm of a financial organization, information security job performance is a crucial aspect as it goes beyond simple compliance with the information security policy laid down by the organization. The foundational individual factor that is considered for thriving are the psychological resources of an individual that include the sense of hope, self-efficacy, resilience, and optimism. We also explore the factors that constitute agentic work behaviors where employees use self-adaptive feelings that help them thrive in the tasks at hand. These agentic work behaviors play an essential role in enhancing how the individuals perform in their work responsibilities. This research found that bank employees with higher psychological resources like hope, self-efficacy, resilience, and optimism were able to act more agentically in their work situation. These agentic feelings lead to a sense of thriving which included learning and vitality. Bank employees were able to appreciate and learn about the ever-evolving information security policies revised by the bank at a regular interval but also the processes that helped keep the sensitive financial information safe and secure.

7.2.2 Employee competence

In this study, the main objective was to explore the antecedents of employee competence and empirically test the impact of employee competence in information security job performance. The study was conducted using a sequential mixed-methods approach as discussed in Chapter 3. In in-depth case study was conducted in a large, public-sector bank in India where we interviewed employees across three groups (managers, retail executives, and IT executives)

to find out what according to them contributed towards employee competence. The factors that emerged from the analysis of the first part of the study were *tacit knowledge*, *explicit knowledge*, and *purposeful heedful interactions*. Furthermore, we empirically tested the research model. The findings from both the qualitative and quantitative studies revealed that managers in the bank considered that competent employees perform better in their information security jobs and responsibilities. This is more than mere compliance with the bank's information security policies. For instance, purposeful heedful interactions among the managers and their subordinates in the bank led to the executives feeling more confident of handling information security queries of the customers. They also felt more competent to deal with an information security threat and better followed cybersecurity practices and protocols that is part of their job responsibilities. Competent employees are surely an asset to an organization as they help in achieving the long-term organizational security goals.

7.2.3 Summary of contributions of this research

This research makes theoretical as well as practical contributions to the field of information security. The first study contributes to the better understanding of thriving at work to a theoretically important outcome variable, which is information security job performance, understanding its relationship with agentic work behaviors (task focus and heedful interaction) and proposing and empirically testing its relationship with Psychological Capital as an antecedent variable. The empirical results have supported the hypothesized relationships. One of the most significant contribution of this study is the application of the conceptualization of thriving at work construct in the domain of information security. Spreitzer et al. (2005) laid emphasis on the individual enabler psychological capital and the agentic work behaviors as the 'engines of thriving' in a social embedded structure. Specifically, this study provides evidence

that psychological capital, a "positive appraisal of circumstances and probability for success based on motivated effort and perseverance" (Luthans et al., 2007), results in significantly higher levels of agentic work behaviors and thus contributes to thriving at work. This study is perhaps the first study to empirically test and evaluate this relationship in the context of information security job performance being an outcome of the thriving. These conceptualizations are particularly interesting as both psychological capital and thriving at work have been conceptually developed and empirically tested in the context of a bank where information security is part of the basic job responsibility of the employees. (Luthans, 2002; Spretizer et al., 2005).

In the second study, we set out to investigate the factors that are vital in building employee security competence and its further impact on IS security job performance. We found that employee competence is a complex construct and presence of both tacit and explicit knowledge along with purposeful interactions helps employees accomplish higher security competence, thus improving employee IS security performance. Through this part of our research, we enhance the current understanding of the role that SETA programs play in increasing IS security job performance. This is particularly of value since, as Hu et al., 2021 note, concerns around SETA programs not being sufficient and "very-effective" is on the rise. While most organizations have a SETA program that is important to mitigate security risks in organizations, the effectiveness of these programs is questionable as employees continue to engage in unsafe IS security practices. A possible solution to boost IS security performance is to focus on the tacit and explicit knowledge of employees that will result in higher competence. Our study contributes to this ongoing effort of understanding how to improve employee competency and knowledge towards IS security roles and responsibilities that consequently results in better

security performance. We build on the conceptualization of competence (Weick and Roberts, 1993; McGrath et al., 1995) and operationalize the construct in the domain of IS security.

7.3 Limitations of this research

In this section, we identify the limitations of this research which can be mitigated by the steps for future research. We start this research with the objective to theorize and test the conceptualizations related to enhancing the information security job performance of employees in a work situation. We particularly focus on the concepts of thriving at work and employee competence that have been well studied in the field of organizational studies to improve the improve the outcome and performance component. Though we used a sequential mixed method approach to better understand the concepts in the domain of information security, our quantitative study is a cross-sectional survey. We could not test if there was a difference in the information security job performance of the employees over a period of time.

This research also evaluates the influence of psychological resources and agentic work behaviors on the sense of thriving among employees in a work situation. The psychological aspects that were considered in this research were hope, self-efficacy, resilience, and optimism. However, there are many other psychological factors that information security literature has evaluated in prior studies. Due to this limitation, the implications of other psychological resources could not be evaluated.

Finally, our quantitative approach used a survey method where employees self-reported about their performance. The bias created through a self-reporting instrument could not be mitigated in this research. Furthermore, the information security performance was a subjective evaluation of the performance of the employees.

7.4 Opportunities for future research

The most obvious opportunities that follow on from this research would be replication or extension of this study in a range of different type of organizations. For example, it would be interesting to study the individual and agentic work behavior factors and its impact on thriving at work in a healthcare work environment. The human and behavioral aspects of security are necessary in all industries and therefore, we could extend this research in other industries like IT where technology and information are used to drive organizational goals. In these scenarios, although the advantage derived from information does lead to financial gains, but it is prudent that employees handing the sensitive information are required to perform their information security roles well.

Future research would also be needed to examine other psychological resources that could act as individual contributors that lead to a sense of thriving through learning and vitality. In this research, we focused on the construct of psychological capital, but information systems and information security literature in particular has looked at other psychological factors like emotions, fear, etc., on the behavioral outcomes of individuals. This will extend the understand beyond the psychological resources of hope, self-efficacy, resilience, and optimism and expand the scope of this stream of study.

Opportunity for future research also exist in the methodological domain. In this research, we use a sequential mixed-methods approach where the conceptual model is developed based on the in-depth case study conducted in the bank. This is followed by a quantitative approach to empirically test the research model. Perhaps it would be interesting to also analyze the time dimension in the study by collecting data at two different times. This would be possible with a

longitudinal data collection method to better evaluate how the information security job performance of employees changes over time.

Finally, further research could be conducted in terms of exploring other agentic work behaviors and factors that could contribute to thriving at work and employee competence. These factors would broaden our understanding of the human and behavior factors contributing to the overall information security performance of individuals.

7.5 Summary

The current research explores an information security outcome in a work situation that has been of concern for a long time but was not studied at depth. Information security scholars have been rightly focused on the aspect of the information compliance behavior as an outcome measure, but we needed to go a step further. The human and behavioral aspect of information security is considered to be an area of great potential by both information systems scholars and practitioners.

This research contributes to the information security literature because it explores the information security job performance as an outcome measure at a workplace. Furthermore, the concepts of thriving at work and employee competence were applied to the context of information security. The findings of this research not only provide a way forward for additional research in the domain of human and behavioral aspects in information security, but also provide management ways to improve the overall organization's information security

REFERENCES

Abid, G., Arya, B., Arshad, A., Ahmed, S., & Farooqi, S. (2021). Positive personality traits and self-leadership in sustainable organizations: Mediating influence of thriving and moderating role of proactive personality. *Sustainable Production and Consumption*, *25*, 299-311.

Abid, G., Ahmed, S., Elahi, N. S., & Ilyas, S. (2020). Antecedents and mechanism of employee well-being for social sustainability: A sequential mediation. *Sustainable Production and Consumption*, *24*, 79-89.

Alikaj, A., Ning, W., & Wu, B. (2021). Proactive personality and creative behavior: examining the role of thriving at work and high-involvement HR practices. *Journal of Business and Psychology*, *36*(5), 857-869.

Amabile, T. M. (1993). Motivational synergy: Toward new conceptualizations of intrinsic and extrinsic motivation in the workplace. *Human Resource Management Review*, *3*(3), 185-201.

Andreu, R., & Ciborra, C. U. (2009). Organizational learning and core capabilities development: the role of IT. In *Bricolage, Care and Information* (pp. 189-205). Palgrave Macmillan, London.

Aurigemma, S., & Leonard, L. (2015). The influence of employee affective organizational commitment on security policy attitudes and compliance intentions. *Journal of Information System Security*, *11*(3).

Avery, D. R., Richeson, J. A., Hebl, M. R., & Ambady, N. (2009). It does not have to be uncomfortable: The role of behavioral scripts in Black–White interracial interactions. *Journal of applied Psychology, 94*(6), 1382.

Avey, J. B., Patera, J. L., & West, B. J. (2006). The implications of positive psychological capital on employee absenteeism. *Journal of Leadership & Organizational Studies, 13*(2), 42-60.

Avey, J. B., Reichard, R. J., Luthans, F., & Mhatre, K. H. (2011). Meta-analysis of the impact of positive psychological capital on employee attitudes, behaviors, and performance. *Human Resource Development Quarterly, 22*(2), 127-152.

Avolio, B. J., & Gardner, W. L. (2005). Authentic leadership development: Getting to the root of positive forms of leadership. *The Leadership Quarterly*, *16*(3), 315-338.

Ayuso, P. N., Gasca, R. M., & Lefevre, L. (2012). FT-FW: A cluster-based fault-tolerant architecture for stateful firewalls. *Computers & Security, 31*(4), 524-539.

Bagozzi, R. P. (2011). Measurement and meaning in information systems and organizational research: Methodological and philosophical foundations. *MIS Quarterly*, 261-292.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191.

Bandura, A. (1988). Self-regulation of motivation and action through goal systems. In *Cognitive perspectives on emotion and motivation* (pp. 37-61). Springer, Dordrecht.

Bandura, A. (2001). Social cognitive theory of mass communication. *Media Psychology, 3*(3), 265-299.

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly*, 413-438.

Bassellier, G., Reich, B. H., & Benbasat, I. (2001). Information technology competence of business managers: A definition and research model. *Journal of Management Information Systems*, *17*(4), 159-182.

Bassellier, G., & Benbasat, I. (2004). Business competence of information technology professionals: Conceptual development and influence on IT-business partnerships. *MIS Quarterly*, 673-694.

Bergland, Å., & Kirkevold, M. (2001). Thriving–a useful theoretical perspective to capture the experience of well-being among frail elderly in nursing homes?. *Journal of Advanced Nursing*, *36*(3), 426-432.

Bhatt, G. D., & Grover, V. (2005). Types of information technology capabilities and their role in competitive advantage: An empirical study. *Journal of Management Information Systems*, *22*(2), 253-277.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837-864.

Boyatzis, R. E. (2008). Competencies in the 21st century. *Journal of Management Development*, *27*(1), 5-12.

Brockner, J., & Higgins, E. T. (2001). Regulatory focus theory: Implications for the study of emotions at work. *Organizational Behavior and Human Decision Processes*, *86*(1), 35-66.

Brown, J. S., & Duguid, P. (1991). Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation. *Organization Science*, *2*(1), 40-57.

Brown, K. W., & Ryan, R. M. (2003). The benefits of being present: mindfulness and its role in psychological well-being. *Journal of Personality and Social Psychology*, *84*(4), 822.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 523-548.

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209.

Burton-Jones, A., McLean, E. R., & Monod, E. (2015). Theoretical perspectives in IS research: from variance and process to conceptual latitude and conceptual fit. *European Journal of Information Systems*, *24*(6), 664-679.

Caldeira, M., & Dhillon, G. (2010). Are we really competent? Assessing organizational ability in delivering IT benefits. *Business Process Management Journal*.

Cameron, K., & Dutton, J. (Eds.). (2003). *Positive organizational scholarship: Foundations of a new discipline*. Berrett-Koehler Publishers.

Carmeli, A., & Spreitzer, G. M. (2009). Trust, connectivity, and thriving: Implications for innovative behaviors at work. *The Journal of Creative Behavior, 43*(3), 169-191.

Carver, C. S. (1998). Resilience and thriving: Issues, models, and linkages. *Journal of Social Issues*, *54*(2), 245-266.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 70-104.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, *1*(3), 18-41.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4), 49-87.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, *29*(3), 157-188.

Chen, Y. A. N., Ramamurthy, K., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11-19.

Cheney, P. H., Hale, D. P., & Kasper, G. M. (1990). Knowledge, skills and abilities of information systems professionals: past, present, and future. *Information & Management*, *19*(4), 237-247.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447-459.

Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security*.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

Christianson, M., Spreitzer, G., Sutcliffe, K., & Grant, A. (2005). An empirical examination of thriving at work. National Acad. In *Management Meeting, Hawaii*.

Churchill Jr, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64-73.

Cram, W. A., Brohman, K., & Gallupe, R. B. (2016). Information systems control: A review and framework for emerging information systems processes. *Journal of the Association for Information Systems*, *17*(4), 2.

Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605-641.

Crossler, R. E., & Bélanger, F. (2009). The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage. *Journal of Information System Security*, *5*(3).

Crossler, R. E. (2010, January). Protection motivation theory: Understanding determinants to backing up personal data. In *2010 43rd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209-226.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior, 28*(5), 1849-1858.

Dalal, R. S. (2005). A meta-analysis of the relationship between organizational citizenship behavior and counterproductive work behavior. *Journal of Applied Psychology*, *90*(6), 1241.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285-318.

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43-69.

D'Arcy, J., & Teh, P. L. (2019a). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, *56*(7), 103151.

David, J. (2002). Policy enforcement in the workplace. *Computers & Security*, *21*(6), 506-513.

Deci, E. L., & Ryan, R. M. (2000). The" what" and" why" of goal pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry*, *11*(4), 227-268.

Dhillon, G. (1997). Managing Information Security. Macmillan, London.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Dhillon, G. (2008). Organizational competence for harnessing IT: A case study. *Information & Management*, *45*(5), 297-303.

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *The Journal of Strategic Information Systems*, *30*(4), 101693.

Diener, E., Wirtz, D., Tov, W., Kim-Prieto, C., Choi, D.-w., Oishi, S., & Biswas-Diener, R. (2010). New well-being measures: Short scales to assess flourishing and positive and negative feelings. *Social Indicators Research, 97*(2), 143-156.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 23.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, *19*(4), 391-412.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295-316.

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: an exploratory analysis. *Information Resources Management Journal (IRMJ)*, *18*(4), 21-39.

Dutton, J. E., Roberts, L. M., & Bednar, J. (2010). Pathways for positive identity construction at work: Four types of positive identity and the building of social resources. *Academy of Management Review*, *35*(2), 265-293.

Dweck, C. S. (1986). Motivational processes affecting learning. *American Psychologist*, *41*(10), 1040.

Elahi, N. S., Abid, G., Arya, B., & Farooqi, S. (2020). Workplace behavioral antecedents of job performance: Mediating role of thriving. *The Service Industries Journal*, *40*(11-12), 755-776.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Fredrickson, B. L. (1998). What good are positive emotions?. *Review of General Psychology*, *2*(3), 300-319.

Fredrickson, B. L. (2003). The value of positive emotions: The emerging science of positive psychology is coming to understand why it's good to feel good. *American Scientist*, *91*(4), 330-335.

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983-988.

Guan, X., & Frenkel, S. (2020). Organizational support and employee thriving at work: exploring the underlying mechanisms. *Personnel Review*.

Gullapalli, D. (2005). Take this job and… file it; burdened by extra work created by the Sarbanes-Oxley Act, CPAs leave the Big Four for better life. *The Wall Street Journal*.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242-251.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203-236.

Hackman, J. R., & Oldham, G. R. (1980). Work design in the organizational context. *Research in Organizational Behavior*, *2*(2), 7-278.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science, 40*(3), 414-433.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*.

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, *66*, 52-65.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In *New challenges to international marketing*: Emerald Group Publishing Limited.

Hentea, M. (2005). A Perspective on Achieving Information Security Awareness. *Issues in Informing Science & Information Technology, 2*.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Herath, T., Yim, M. S., D'Arcy, J., Nam, K., & Rao, H. R. (2018). Examining employee security violations: Moral disengagement and its environmental influences. *Information Technology & People*.

Hobfoll, S. E. (2002). Social and psychological resources and adaptation. *Review of general psychology, 6*(4), 307-324.

Hochschild, A. R. (1997). When work becomes home and home becomes work. *California Management Review, 39*(4), 79.

Holtkamp, P., Jokinen, J. P., & Pawlowski, J. M. (2015). Soft competency requirements in requirements engineering, software design, implementation, and testing. *Journal of Systems and Software*, *101*, 136-146.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research, 26*(2), 282-300.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM*, *54*(6), 54-60.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, *31*(4), 6-48.

Hu, S., Hsu, C., & Zhou, Z. (2021). Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems*, 1-13.

Huselid, M. A. (1995). The impact of human resource management practices on turnover, productivity, and corporate financial performance. *Academy of Management Journal, 38*(3), 635-672.

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: the enduring problem of human error. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 36*(4), 68-79.

Imran, M. Y., Elahi, N. S., Abid, G., Ashfaq, F., & Ilyas, S. (2020). Impact of perceived organizational support on work engagement: Mediating mechanism of thriving and flourishing. *Journal of Open Innovation: Technology, Market, and Complexity*, *6*(3), 82.

Inceoglu, I., Thomas, G., Chu, C., Plans, D., & Gerbasi, A. (2018). Leadership behavior and employee well-being: An integrated review and a future research agenda. *The Leadership Quarterly*, *29*(1), 179-202.

Jensen, S. M., & Luthans, F. (2006). Relationship between entrepreneurs' psychological capital and their authentic leadership. *Journal of Managerial Issues*, 254-273.

Jiang, Z., Di Milia, L., Jiang, Y., & Jiang, X. (2020). Thriving at work: A mentoring-moderated process linking task identity and autonomy to job satisfaction. *Journal of Vocational Behavior*, *118*, 103373.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework. *MIS Quarterly*, *39*(1), 113-134.

Johnston, A. C., Wech, B., & Jack, E. (2000). Engaging remote employees: The moderating role of "remote" status in determining employee information security policy awareness. *Journal of Organizational and End User Computing (JOEUC)*, *25*(1), 1-23.

Kahn, W. A. (1990). Psychological conditions of personal engagement and disengagement at work. *Academy of Management Journal, 33*(4), 692-724.

Kanfer, R. (1990). Motivation and individual differences in learning: An integration of developmental, differential and cognitive perspectives. *Learning and Individual Differences*, *2*(2), 221-239.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139-154.

Kark, R., & Carmeli, A. (2009). Alive and creating: The mediating role of vitality and aliveness in the relationship between psychological safety and creative work involvement. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, *30*(6), 785-804.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security*, *24*(3), 246-260.

Katz, D., & Kahn, R. L. (1978). Organizations and the system concept. *Classics of Organization Theory*, *80*, 480.

Keyes, C. L. M., Hysom, S. J., & Lupo, K. L. (2000). The positive organization: Leadership legitimacy, employee well-being, and the bottom line. *The Psychologist-Manager Journal*, *4*(2), 143.

King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*, *28*(3), 308-319.

Kirsch, L., & Boss, S. (2007). The last line of defense: motivating employees to follow corporate security guidelines. *ICIS 2007 Proceedings*, 103.

Kleine, A. K., Rudolph, C. W., & Zacher, H. (2019). Thriving at work: A meta-analysis. *Journal of Organizational Behavior*, *40*(9-10), 973-999.

Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493-508.

Kolb, D. A. (1984). Experience as the source of learning and development. *Upper Sadle River: Prentice Hall*.

Kossek, E. E., & Perrigino, M. B. (2016). Resilience: A review using a grounded integrated occupational approach. *Academy of Management Annals*, *10*(1), 00-00.

Kwon, P. (2000). Hope and dysphoria: The moderating role of defense mechanisms. *Journal of Personality*, *68*(2), 199-223.

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, *59*, 60-70.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187.

Li, N., & Wang, Q. (2008). Beyond separation of duty: An algebra for specifying high-level security policies. *Journal of the ACM (JACM)*, *55*(3), 1-46.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 71-90.

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 1.

Liang, H., Xue, Y., & Wu, L. (2013). Ensuring employees' IT compliance: carrot or stick?. *Information Systems Research*, *24*(2), 279-294.

Liao, Q., Gurung, A., Luo, X., & Li, L. (2009). Workplace management and employee misuse: does punishment matter?. *Journal of Computer Information Systems*, *50*(2), 49-59.

Losada, M., & Heaphy, E. (2004). The role of positivity and connectivity in the performance of business teams: A nonlinear dynamics model. *American Behavioral Scientist*, *47*(6), 740-765.

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193-273.

Lowry, P. B., Posey, C., Roberts, T. L., & Bennett, R. J. (2014). Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *Journal of Business Ethics*, *121*(3), 385-401.

Luthans, F. (2002). The need for and meaning of positive organizational behavior. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior, 23*(6), 695-706.

Luthans, F., Avolio, B. J., Avey, J. B., & Norman, S. M. (2007). Positive psychological capital: Measurement and relationship with performance and satisfaction. *Personnel Psychology, 60*(3), 541-572.

Luthans, F., Norman, S. M., Avolio, B. J., & Avey, J. B. (2008). The mediating role of psychological capital in the supportive organizational climate—employee performance relationship. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior, 29*(2), 219-238.

Luthans, F., Vogelgesang, G. R., & Lester, P. B. (2006). Developing the psychological capital of resiliency. *Human Resource Development Review, 5*(1), 25-44.

Luthans, F., Avey, J. B., Avolio, B. J., Norman, S. M., & Combs, G. M. (2006a). Psychological capital development: toward a micro-intervention. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior, 27*(3), 387-393.

Luthans, F., Youssef, C. M., & Avolio, B. J. (2007a). Psychological capital: Developing the human competitive edge.

Luthans, F., Youssef, C. M., & Avolio, B. J. (2007b). Psychological capital: Investing and developing positive organizational behavior. *Positive Organizational Behavior, 1*(2), 9-24.

Luthans, F., Youssef, C. M., & Avolio, B. J. (2015). *Psychological capital and beyond*. Oxford University Press, USA.

McClelland, D. C. (1973). Testing for competence rather than for" intelligence.". *American Psychologist*, *28*(1), 1.

McClelland, D. C., & Boyatzis, R. E. (1982). Leadership motive pattern and long-term success in management. *Journal of Applied Psychology*, *67*(6), 737.

McGrath, R. G., MacMillan, I. C., & Venkataraman, S. (1995). Defining and developing competence: A strategic process paradigm. *Strategic Management Journal*, *16*(4), 251-275.

McGrath, R. G. (2001). Exploratory learning, innovative capacity, and managerial oversight. *Academy of Management Journal*, *44*(1), 118-131.

Malhotra, M. K., & Grover, V. (1998). An assessment of survey research in POM: from constructs to theory. *Journal of Operations Management, 16*(4), 407-425.

Maslow, A. H. (1998). A theory of human motivation. *Personality: Critical concepts in psychology*, 169-188.

Masten, A. S., & Reed, M. G. J. (2002). Resilience in development. *Handbook of Positive Psychology*, *74*, 88.

May, D. R., Gilson, R. L., & Harter, L. M. (2004). The psychological conditions of meaningfulness, safety and availability and the engagement of the human spirit at work. *Journal of Occupational and Organizational Psychology, 77*(1), 11-37.

Meyer, J. P., Paunonen, S. V., Gellatly, I. R., Goffin, R. D., & Jackson, D. N. (1989). Organizational commitment and job performance: It's the nature of the commitment that counts. *Journal of Applied Psychology, 74*(1), 152.

Moquin, R., & Wakefield, R. L. (2016). The roles of awareness, sanctions, and ethics in software compliance. *Journal of Computer Information Systems*, *56*(3), 261-270.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization, 17*(1), 2-26.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139.

Neumann, J. E., Miller, E. J., & Holti, R. (1999). Three contemporary challenges for OD practitioners. *Leadership & Organization Development Journal*.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

Nix, G. A., Ryan, R. M., Manly, J. B., & Deci, E. L. (1999). Revitalization through self-regulation: The effects of autonomous and controlled motivation on happiness and vitality. *Journal of Experimental Social Psychology, 35*(3), 266-284.

Orlikowski, W. J. (2002). Knowing in practice: Enacting a collective capability in distributed organizing. *Organization Science*, *13*(3), 249-273.

Parker, S. K., Wall, T. D., & Jackson, P. R. (1997). "That's not my job": Developing flexible employee work orientations. *Academy of Management Journal*, *40*(4), 899-929.

Paterson, T. A., Luthans, F., & Jeung, W. (2014). Thriving at work: Impact of psychological capital and supervisor support. *Journal of Organizational Behavior, 35*(3), 434-446.

Pathari, V., & Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security*.

Porath, C., Spreitzer, G., Gibson, C., & Garnett, F. G. (2012). Thriving at work: Toward its measurement, construct validation, and theoretical refinement. *Journal of Organizational Behavior, 33*(2), 250-275.

Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, *30*(6-7), 486-497.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, 1189-1210.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214.

Prem, R., Ohly, S., Kubicek, B., & Korunka, C. (2017). Thriving on challenge stressors? Exploring time pressure and learning demands as antecedents of thriving at work. *Journal of Organizational Behavior*, *38*(1), 108-123.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 757-778.

Rahaman, H. S., Stouten, J., Decoster, S., & Camps, J. (2022). Antecedents of employee thriving at work: The roles of formalization, ethical leadership, and interpersonal justice. *Applied Psychology*, *71*(1), 3-26.

Rego, A., Cavazotte, F., Cunha, M. P. E., Valverde, C., Meyer, M., & Giustiniano, L. (2021). Gritty leaders promoting employees' thriving at work. *Journal of Management*, *47*(5), 1155-1184.

Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership?. *Information Management & Computer Security*.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826.

Roberts, L. M., Dutton, J. E., Spreitzer, G. M., Heaphy, E. D., & Quinn, R. E. (2005). Composing the reflected best-self portrait: Building pathways for becoming extraordinary in work organizations. *Academy of Management Review*, *30*(4), 712-736.

Ryan, R. M., & Deci, E. L. (2001). On happiness and human potentials: A review of research on hedonic and eudaimonic well-being. *Annual Review of Psychology*, *52*, 141.

Ryff, C. D. (1989). Happiness is everything, or is it? Explorations on the meaning of psychological well-being. *Journal of Personality and Social Psychology*, *57*(6), 1069.

Şahin, S., Arıcı Özcan, N., & Arslan Babal, R. (2020). The mediating role of thriving: Mindfulness and contextual performance among Turkish nurses. *Journal of Nursing Management*, *28*(1), 175-184.

Scheier, M. F., & Carver, C. S. (1985). Optimism, coping, and health: assessment and implications of generalized outcome expectancies. *Health Psychology, 4*(3), 219.

Seibert, S. E., Wang, G., & Courtright, S. H. (2011). Antecedents and consequences of psychological and team empowerment in organizations: a meta-analytic review. *Journal of Applied Psychology*, *96*(5), 981.

Shahid, S., Muchiri, M. K., & Walumbwa, F. O. (2020). Mapping the antecedents and consequences of thriving at work: A review and proposed research agenda. *International Journal of Organizational Analysis*.

Sheldon, K. M., & King, L. (2001). Why positive psychology is necessary. *American Psychologist, 56*(3), 216.

Siders, M. A., George, G., & Dharwadkar, R. (2001). The relationship of internal and external commitment foci to objective job performance measures. *Academy of Management Journal, 44*(3), 570-579.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). *Employees' adherence to information security policies: an empirical study.* Paper presented at the IFIP International Information Security Conference.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*.

Siponen, M. T. (2005). An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems, 14*(3), 303-315.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical opinion Are employees putting your company at risk by not following information security policies?. *Communications of the ACM*, *52*(12), 145-147.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 487-502.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224.

Siponen, M., & Vance, A. (2014a). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems*, *23*(3), 289-305.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64-71.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267-270.

Snyder, C. R., Harris, C., Anderson, J. R., Holleran, S. A., Irving, L. M., Sigmon, S. T., . . . Harney, P. (1991). The will and the ways: development and validation of an individual-differences measure of hope. *Journal of Personality and Social Psychology, 60*(4), 570.

Snyder, C. R. (2002). Hope theory: Rainbows in the mind. *Psychological Inquiry*, *13*(4), 249-275.

Sonenshein, S., Dutton, J., Grant, A., Spreitzer, G., & Sutcliffe, K. (2005). Narratives of growth at work: Learning from employees' stories. *Ann Arbor, MI: Ross School of Business of Business, University of Michigan*.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, 503-522.

Spreitzer, G., & Porath, C. (2012). Creating sustainable performance. *Harvard Business Review, 90*(1), 92-99.

Spreitzer, G., Sutcliffe, K., Dutton, J., Sonenshein, S., & Grant, A. M. (2005). A socially embedded model of thriving at work. *Organization science, 16*(5), 537-549.

Spreitzer, G. M. (2008). Taking stock: A review of more than twenty years of research on empowerment at work. *Handbook of Organizational Behavior*, *1*, 54-72.

Spreitzer, G. M., Lam, C. F., & Fritz, C. (2010). Engagement and human thriving: Complementary perspectives on energy and connections to work. *Work engagement: A handbook of essential theory and research*, 132-146.

Spreitzer, G. M. (1995). Psychological empowerment in the workplace: Dimensions, measurement, and validation. *Academy of Management Journal*, *38*(5), 1442-1465.

Spreitzer, G. M. (1996). Social structural levers to individual empowerment in the workplace. *Academy of Management Journal*, *39*(2), 483-504.

Stajkovic, A. D., & Luthans, F. (1998). Self-efficacy and work-related performance: A meta-analysis. *Psychological Bulletin*, *124*(2), 240.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS quarterly*, 147-169.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 441-469.

Tashakkori, A., Teddlie, C., & Teddlie, C. B. (1998). *Mixed methodology: Combining qualitative and quantitative approaches* (Vol. 46): Sage.

Teh, P. L., Ahmed, P. K., & D'Arcy, J. (2015). What drives information security policy violations among banking employees?: insights from neutralization and social exchange theory. *Journal of Global Information Management (JGIM)*, *23*(1), 44-64.

Tsui, A. S., & Ashford, S. J. (1994). Adaptive self-regulation: A process view of managerial effectiveness. *Journal of Management, 20*(1), 93-121.

Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal, 48*(6), 1143-1158.

Usman, M., Liu, Y., Li, H., Zhang, J., Ghani, U., & Gul, H. (2021). Enabling the engine of workplace thriving through servant leadership: The moderating role of core self-evaluations. *Journal of Management & Organization*, *27*(3), 582-600.

Vaast, E. (2007). Danger is in the eye of the beholders: social representations of information systems security in healthcare. *The Journal of Strategic Information Systems*, *16*(2), 130-152.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, *15*(10), 2.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263-290.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

Vardi, Y., & Weitz, E. (2003). *Misbehavior in Organizations: Theory, research, and management*: Psychology Press.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 21-54.

Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems, 17*(7), 2.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Wade, M., & Hulland, J. (2004). The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS Quarterly*, 107-142.

Walumbwa, F. O., Muchiri, M. K., Misati, E., Wu, C., & Meiliani, M. (2018). Inspired to perform: A multilevel investigation of antecedents and consequences of thriving at work. *Journal of Organizational Behavior*, *39*(3), 249-261.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, 25-35.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101-105.

Weick, K. E., & Roberts, K. H. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *Administrative Science Quarterly*, 357-381.

Weick, K. E., Sutcliffe, K. M., & Obstfled, D. (1999). Organizing for high reliability: processes of collective mindfulness" in Research in Organizational Behaviour, 21, R.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization*, *16*(4), 304-324.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems*, *15*(4), 403-414.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 1-20.

Wood, R., & Bandura, A. (1989). Social cognitive theory of organizational management. *Academy of Management Review*, *14*(3), 361-384.

Woodside, A. G. (2013). Moving beyond multiple regression analysis to algorithms: Calling for adoption of a paradigm shift from symmetric to asymmetric thinking in data analysis and crafting theory. In: Elsevier.

Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research*, *22*(2), 400-414.

Yan, A., Tang, L., & Hao, Y. (2021). Can corporate social responsibility promote employees' taking charge? The mediating role of thriving at work and the moderating role of task significance. *Frontiers in Psychology*, *11*, 613676.

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36-46.

Youssef, C. M. (2004). *Resiliency development of organizations, leaders and employees: Multi-level theory building and individual-level, path-analytical empirical testing*. The University of Nebraska-Lincoln.

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems, 24*(1), 34.

Zhang, A. Y., Tsui, A. S., Song, L. J., Li, C., & Jia, L. (2008). How do I trust thee? The employee-organization relationship, supervisory support, and middle manager trust in the organization. *Human Resource Management: Published in Cooperation with the School of Business Administration, The University of Michigan and in alliance with the Society of Human Resources Management, 47*(1), 111-132.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*.

APPENDIX A: MEASUREMENT ITEMS FOR THRIVING AT WORK STUDY

Construct	Code	Instrument	Source
Psychological capital (PC): Self-efficacy	PCSE1	I feel confident analyzing an information security problem to find a solution	Burns et al. (2017)
	PCSE2	I feel confident in representing my information security work in meetings with management	
	PCSE3	I feel confident contributing to discussions about the organization's strategy on data/information security	
	PCSE4	I feel confident helping to set targets/goals in the area of information security	
	PCSE5	I feel confident presenting information on data security to a group of colleagues	
(PC) Hope	PCH1	If I am stuck in a data/information security problem, I could think of many ways to get out of it	
	PCH2	At the present time, I am energetically pursuing my goals in information security	
	PCH3	There are lots of ways around any problem related to data/information security	
	PCH4	Right now, I see myself as being pretty successful in data/information security	
	PCH5	I can think of many ways to reach my current goals in information security	
	PCH6	At this time, I am meeting the information security goals that I have set for myself	
(PC) Resilience	PCR1	I usually manage difficulty in information security one way or another	
	PCR2	I usually take stressful things in information security in stride	
	PCR3	I can get through information security challenges because I've experienced difficulty before	
	PCR4	I feel I can handle many things at a time related to information security	
(PC) Optimism	PCO1	When things are uncertain for me in information security, I usually expect the best	

	PCO2	I always look at the bright side of things regarding information security	
	PCO3	I am optimistic about what will happen to me in the future as it pertains to information security	
	PCO4	I approach information security as if "every cloud has a silver lining"	
Agentic work behavior (AWB): Task focus	TF1	I spend a lot of time thinking about information security concerning my work	Rothbard et al. (2011)
	TF2	I focus a great deal of attention on information security concerning my work	
	TF3	I concentrate a lot on information security related to my work	
	TF4	I pay a lot of attention to information security related to my work	
(AWB) Heedful interaction	HI1	I help to clarify the idea of another group member so that we all understand her/his idea about information security.	Karahanna et al. (2006)
	HI2	I rephrase what a group member says so that I can check my understanding of his/her idea about information security.	
	HI3	I ask a group member to elaborate on his/her idea so that I can make sure I understand what he/she is saying about information security.	
	HI4	I carefully explain a concept to a group member who does not understand the concept on information security.	
	HI5	I carefully contribute relevant examples in my group related to information security	
	HI6	I try to think about how I can connect my ideas to ideas offered by other group members on information security.	
Thriving at work	TW1	I feel alive and vital when dealing with information security issues	Porath et al. (2012)
	TW2	I have energy and spirit working with information security concerns	
	TW3	I am looking forward to each new day when working towards information security	
	TW4	I feel alert and awake working in information security domain	
	TW5	I do not feel very energetic working in information security domain	

	TW6	I continue to learn more as time goes by regarding information security	
	TW7	I am not learning about information security (R)	
	TW8	I am developing a lot as a person learning about information security	
	TW9	I find myself learning often about information security	
	TW10	I see myself continually improving in information security	
Information security job performance	IS1	I adequately complete duties assigned in information security	William & Anderson (1991)
	IS2	I fulfill my responsibilities specified in job description related to information security	
	IS3	I perform tasks that are expected from me in information security	
	IS4	I meet information security requirements of the job	
	IS5	I engage in information security activities that will directly affect my performance evaluation	
	IS6	I neglect the information security aspects of the job that I'm obligated to perform	
	IS7	I fail to perform essential information security duties	

The survey used 7-point Likert scale (ranging from 1-Strongly Disagree to 7-Strongly Agree) to measure all the items.

APPENDIX B: MEASUREMENT ITEMS FOR EMPLOYEE COMPETENCE STUDY

Construct	Code	Instrument	Source
Purposeful Heedful Interaction	HI1	I help to clarify the idea of another group member so that we all understand her/his idea about information security.	Karahanna et al. (2006)
	HI2	I rephrase what a group member says so that I can check my understanding of his/her idea about information security.	
	HI3	I ask a group member to elaborate on his/her idea so that I can make sure I understand what he/she is saying about information security.	
	HI4	I carefully explain a concept to a group member who does not understand the concept on information security.	
	HI5	I carefully contribute relevant examples in my group related to information security	
	HI6	I try to think about how I can connect my ideas to ideas offered by other group members on information security.	
Tacit Knowledge	TK1	I learned the value of information security through discussions with organizational members.	Cavusgil et al. (2003)
	TK2	I seek ideas and expertise from senior colleagues to improve my work in information security.	
	TK3	I seek feedback on hard-to-find knowledge or unwritten knowledge from colleagues about information security.	
	TK4	There are a lot of constructive informal discussions with other colleagues regarding information security.	
	TK5	I was mentored by senior colleagues about information security as a way to encourage employees to learn from each other.	
Explicit Knowledge	EK1	I gain knowledge about information security work from reports, official documents, and self-explanatory software.	Dabestani et al. (2014)
	EK2	I learn about information security from well-documented manuals, methodologies and models.	
	EK3	I learn about management techniques related to information security from written knowledge provided by my organization.	

	EK4	I usually utilize the reports and documents shared by others regarding information security.	
Employee Competence	CO1	I take action to stay informed about developments directly related to information security.	Bassellier & Benbasat (2004)
	CO2	I participate in activities that are directly related to information security.	
	CO3	I am concerned about the overall information security performance of my organization.	
	CO4	My work has an impact on the information security performance of the organization.	
	CO5	If I have an information security question or problem I cannot solve alone, I'm quite confident about finding the right person to contact in my organization.	
	CO6	If I have an information security question or problem I cannot solve alone, I'm quite confident about finding the right contacts outside my organization (consultants, vendors).	
	CO7	If I have an information security question or problem I cannot solve alone, I'm quite confident about finding other relevant sources of information including Internet sites, trade journals, and conferences.	
Information security job performanc e	IS1	I adequately complete duties assigned in information security	William & Anderson (1991)
	IS2	I fulfill my responsibilities specified in job description related to information security	
	IS3	I perform tasks that are expected from me in information security	
	IS4	I meet information security requirements of the job	
	IS5	I engage in information security activities that will directly affect my performance evaluation	
	IS6	I neglect the information security aspects of the job that I'm obligated to perform	
	IS7	I fail to perform essential information security duties	

The survey used 7-point Likert scale (ranging from 1-Strongly Disagree to 7-Strongly Agree) to measure all the items.

.

APPENDIX C: ITEM LOADINGS AND CROSS-LOADINGS FOR THRIVING AT WORK STUDY

	Hope	Optimism	Resilience	Self-efficacy	Task focus	Heedful interaction	Thriving at work	IS job performance
PCH1	**0.855**	0.61	0.786	0.645	0.508	0.659	0.613	0.512
PCH2	**0.852**	0.667	0.79	0.811	0.722	0.772	0.874	0.555
PCH3	**0.825**	0.685	0.714	0.658	0.528	0.616	0.611	0.371
PCH4	**0.875**	0.664	0.807	0.724	0.639	0.714	0.795	0.597
PCH5	**0.923**	0.634	0.789	0.803	0.764	0.818	0.803	0.519
PCH6	**0.772**	0.578	0.711	0.533	0.433	0.535	0.62	0.632
PCO1	0.685	**0.915**	0.699	0.7	0.48	0.662	0.721	0.351
PCO2	0.691	**0.942**	0.706	0.692	0.459	0.696	0.696	0.35
PCO3	0.727	**0.94**	0.705	0.722	0.458	0.634	0.69	0.293
PCO4	0.673	**0.897**	0.668	0.667	0.463	0.562	0.668	0.276
PCR1	0.844	0.641	**0.872**	0.657	0.452	0.596	0.653	0.699
PCR2	0.798	0.644	**0.902**	0.723	0.487	0.694	0.697	0.526
PCR3	0.746	0.647	**0.87**	0.619	0.403	0.614	0.656	0.411
PCR4	0.753	0.694	**0.848**	0.66	0.572	0.719	0.738	0.44
PCSE1	0.771	0.71	0.738	**0.91**	0.635	0.806	0.76	0.377
PCSE2	0.765	0.69	0.724	**0.912**	0.628	0.792	0.815	0.456
PCSE3	0.767	0.683	0.735	**0.871**	0.559	0.641	0.7	0.401
PCSE4	0.734	0.709	0.625	**0.924**	0.609	0.683	0.767	0.421
PCSE5	0.639	0.571	0.581	**0.863**	0.536	0.491	0.683	0.452
TASK1	0.669	0.56	0.518	0.594	**0.899**	0.57	0.701	0.42
TASK2	0.566	0.344	0.416	0.516	**0.907**	0.568	0.664	0.327
TASK3	0.69	0.488	0.566	0.634	**0.932**	0.673	0.782	0.552
TASK4	0.665	0.436	0.496	0.674	**0.916**	0.631	0.751	0.45
HEED1	0.758	0.629	0.676	0.707	0.638	**0.937**	0.751	0.449
HEED2	0.551	0.522	0.467	0.517	0.482	**0.824**	0.625	0.214
HEED3	0.643	0.602	0.657	0.68	0.559	**0.908**	0.729	0.332
HEED4	0.725	0.586	0.67	0.618	0.556	**0.834**	0.615	0.35
HEED5	0.827	0.688	0.756	0.725	0.618	**0.907**	0.795	0.507
HEED6	0.751	0.604	0.708	0.765	0.654	**0.837**	0.818	0.464
THRIVE1	0.758	0.677	0.693	0.725	0.785	0.739	**0.936**	0.516
THRIVE10	0.809	0.675	0.753	0.747	0.654	0.736	**0.892**	0.67
THRIVE2	0.796	0.739	0.711	0.729	0.808	0.729	**0.913**	0.516
THRIVE3	0.746	0.687	0.712	0.744	0.755	0.757	**0.922**	0.496
THRIVE4	0.697	0.63	0.656	0.694	0.664	0.658	**0.89**	0.537
THRIVE6	0.761	0.616	0.7	0.727	0.634	0.713	**0.846**	0.604

THRIVE8	0.754	0.774	0.697	0.803	0.716	0.782	**0.89**	0.442
THRIVE9	0.746	0.57	0.686	0.783	0.662	0.816	**0.849**	0.507
PERFORM1	0.57	0.268	0.487	0.402	0.54	0.363	0.526	**0.833**
PERFORM2	0.568	0.314	0.567	0.418	0.441	0.43	0.556	**0.911**
PERFORM3	0.552	0.35	0.534	0.412	0.351	0.429	0.481	**0.87**
PERFORM4	0.47	0.205	0.497	0.317	0.244	0.358	0.42	**0.843**
PERFORM5	0.372	0.26	0.355	0.361	0.364	0.235	0.473	**0.634**

Second-order construct ‘psychological capital’ not shown in the table as it is measures by first-order constructs.

APPENDIX D: ITEM LOADINGS AND CROSS-LOADINGS FOR EMPLOYEE

COMPETENCE STUDY

	Purposeful heedful interactions (PHI)	Tacit knowledge (TCK)	Explicit knowledge (EXK)	Competence (COMP)	Information security job performance (PERF)
PHI1	**0.876**	0.732	0.665	0.627	0.636
PHI2	**0.901**	0.730	0.759	0.618	0.620
PHI3	**0.900**	0.774	0.708	0.659	0.653
PHI4	**0.914**	0.763	0.740	0.583	0.579
PHI5	**0.921**	0.808	0.802	0.655	0.659
PHI6	**0.906**	0.734	0.754	0.550	0.568
TCK1	0.775	**0.914**	0.828	0.666	0.685
TCK2	0.760	**0.922**	0.782	0.681	0.710
TCK3	0.701	**0.890**	0.737	0.511	0.539
TCK4	0.771	**0.896**	0.831	0.577	0.602
TCK5	0.779	**0.899**	0.863	0.601	0.581
EXK1	0.767	0.849	**0.942**	0.628	0.623
EXK2	0.732	0.824	**0.934**	0.570	0.609
EXK3	0.776	0.831	**0.942**	0.626	0.608
EXK4	0.754	0.809	**0.884**	0.555	0.531
COMP1	0.585	0.572	0.533	**0.928**	0.683
COMP2	0.645	0.616	0.580	**0.934**	0.713
COMP3	0.640	0.663	0.650	**0.890**	0.688
PERF1	0.599	0.616	0.549	0.702	**0.890**
PERF2	0.631	0.614	0.607	0.673	**0.884**
PERF3	0.563	0.595	0.531	0.676	**0.897**
PERF4	0.628	0.648	0.579	0.708	**0.917**
PERF5	0.567	0.578	0.549	0.572	**0.784**
PERF6	0.602	0.576	0.526	0.613	**0.836**
PERF7	0.556	0.558	0.536	0.625	**0.831**