TECHNOLOGY THREAT AVOIDANCE FACTORS AS PREDICTORS OF RISKY CYBERSECURITY BEHAVIOR WITHIN THE ENTERPRISE

A dissertation

Presented to

The College of Graduate and Professional Studies

College of Technology

Indiana State University

Terre Haute, Indiana

In Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy

---

by

Andrew R. Gillam

May 2019

Keywords: technology management, human resource development and cybersecurity, human factors and cybersecurity, technology threat avoidance theory, risky cybersecurity behavior

VITA

Andrew R. Gillam

EDUCATION

2019	Indiana State University, Doctor of Philosophy in Technology Management
1996	Texas State University, Master of Science in Computer Science
1985	Kansas State University, Bachelor of Science in Computer Science

PUBLICATIONS

Gillam, A.R. (in press). Cybersecurity and human resource development implications for the enterprise. *Cyber Security: A Peer-Reviewed Journal*

Gillam, A.R., Gillam, S.W., McDaniel, P.H. (in press). Increasing hospital patient throughput: A gamification case study. *Management in Healthcare*.

Gillam, A. (2017). Application of decision support techniques from manufacturing in managing employee attrition. *Journal of Applied Management and Entrepreneurship, 22*(2), 67-79. doi:10.9774/GLEAF.3709.2017.ap.00006

Gillam, S. W., Gillam, A. R., Casler, T. L., & Cook, K. (2017). Increasing patient recall of nurse leader rounding. *Applied Nursing Research, 38*, 163-168. doi:10.1016/j.apnr.2017.10.013

Gillam, S. W., Gillam, A.R., Casler, T., Curcio, K (2016). Education for medications and side effects: A two part mechanism for improving the patient experience. *Applied Nursing Research. 36*(2), 72-78. doi*:* 10.1016/j.apnr.2015.11.017

CONFERENCE PRESENTATIONS

Gillam, A.R., Waite, A.M. The Current State of Trust in Virtual Teams: A Literature Review. 2019 Association of Human Resource Development Conference in the Americas, Louisville, KY

MANUSCRIPTS UNDER REVIEW

Gillam, A.R., Waite, A.M. Exploring the Current State of Trust in Virtual Teams: An Integrative Literature Review

PROFESSIONAL EXPERIENCE

2013 – 2017	Founder, Infant Guard LLC
2011 - 2013	Senior Director of Global Retail Software Services, Infogain Corporation
2005 – 2011	Consulting Services Manager, Oracle USA, Inc.
2002 – 2005	Director of Product Development, 360Commerce Inc.
1999 – 2002	Director of Consulting Services, AppliedTheory Corporation
1996 – 1999	Project Manager, Cornerstone Retail Solutions
1994 – 1996	Project Manager, Wayne Division, Dresser Industries, Inc.
1989 – 1994	Software Developer, IBM Advanced Workstation Division

COMMITTEE MEMBERS

Committee Chair: W. Tad Foster, Ed.D.

Professor, Department of Human Resource Development and Performance Technologies

Indiana State University

Committee Member: Vincent W. Childress, Ph.D.

Professor, Department of Graphic Design Technology

North Carolina Agricultural and Technical State University

Committee Member: Carroll M. Graham, Ed.D.

Associate Professor, Department of Human Resource Development and Performance Technologies

Indiana State University

ABSTRACT

Recent research of information technology (IT) end-user cybersecurity-related risky behaviors has focused on items such as IT user decision-making, impulsiveness, and internet use as predictors of human cyber vulnerability. Theories which guide user human behavioral intent, such as protection motivation theory (PMT, introduced by Rogers, 1975) and technology threat avoidance theory (TTAT, introduced by Liang and Xue, 2009) have not been widely investigated as antecedents of risky cybersecurity behavior (RScB). This dissertation describes exploratory research that analyzed and evaluated PMT/TTAT factors as predictors of RScB by enterprise IT users. This work uniquely contributes to the literature by investigating associations between accepted behavioral motivation models and RScB. Findings are intended to provide human resource development (HRD) practitioners and researchers innovative techniques to identify factors which may compel enterprise IT users to avoid risky cybersecurity behaviors in the workplace. Findings, based on survey responses by 184 working professionals in the United States, were largely consistent with previous TTAT-focused works. New insights arose regarding the predictive impact of perceived cost as a predictor of RScB ($p = .003$) with small-to-medium effect sizes. Predictability was further leveraged using discriminant analysis to predict RScB category membership derived from k-means clustering. Significant outcomes were noted with practical utility. An overarching goal of this study was to more fully inform the HRD community of scholar-practitioners of the urgent need to design, deliver, implement, and evaluate initiatives that could be utilized to diminish inappropriate and costly cybersecurity behaviors in various workplace environments.

PREFACE

Our information-intensive society presents inexorably increasing need for talented individuals to combine their abilities and scale mountainous challenges. As information technology empowers us to climb higher peaks, we encounter new pitfalls, some incidental, some malicious. I hope this work shares knowledge that benefits the hard-working souls who bridge those pitfalls in an increasingly competitive global landscape.

My interests in technology, cybersecurity and human performance unfolded from disparate experiences as a member of the U.S. Army Military Police Corps and myriad roles in professional software development. Those disjointed domains revealed an invariant need to work with others who were focused yet adaptable, and willing to invest trust in each other despite frequently anxiety-laden circumstances.

This work is tightly coupled with 21st century information technology. However, most of the insights it captures were fueled by my experiences as a husband, father, soldier, athlete, engineer, and professional leader. The gift of lifelong learning that buttressed this research could not have taken root without that tapestry of experience,

Deepest thanks to my wife, Dr. Sally Gillam, for her wisdom, insight and support during this journey. I could not have considered doctoral study worthwhile or possible had she not blazed her own trail despite opposition by countless others.

Sincere gratitude to W. Tad Foster, Ed.D. who chaired my program of study and research committees; he balanced flexibility and constraint with remarkable aplomb as I tested boundaries

between information technology and human behavior. Additional thanks to Vincent Childress, Ph.D. of North Carolina A&T State University for his stable presence, adaptability, and unwavering support throughout my course of study. My gratitude to Carroll M. Graham, Ed.D., who admirably demonstrated the epitome of flexibility and support for his colleagues and learners at Indiana State University when life circumstances altered their best-laid plans. My deep appreciation to Alina Waite, Ph.D. of Indiana State University, who demonstrated patience and diplomacy in considerable amounts as my writing skills took shape.

Thanks to my professional colleagues of the past many decades; their presence allowed a tree of knowledge to bear fruit through countless lessons; my greatest motivation and admiration arose from my experiences partnering with people who somehow moved the proverbial needle when history and intuition implied that our objectives were not achievable. Similar thanks to my long-standing friends and departed colleagues of the U.S. Army 3d Infantry Division and the 3d Military Police Company; their insights, actions, and guidance exemplified adaptive reasoning in circumstances that were frequently unclear.

Finally, thanks to Kansas State University, and the people of the great state of Kansas for extending the hand of opportunity to a young undergrad when possibilities seemed few and far between.

Andrew R. Gillam
Austin, Texas
February 1, 2019

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Technology is a human-based phenomenon. Its impacts exceed its core purpose of aiding human problem solving and increasing our ability to perform work -- it influences our basic way of thinking. This assertion is evident when one considers supposedly innate human behaviors that are strongly influenced by human-created artifacts; clocks and maps are two examples (Carr, 2011). The proliferation of information-oriented technology (IT) has created similar societal dependencies on IT products and services (Fan, Liu, Wang, & Wang, 2017). This dependency presents opportunities for cyber attackers compelled by commercial, military, or economic factors to illicitly access and/or steal electronic information. Attackers can be driven by a variety of interests. Those interests generally originate from one of four general areas, although some cybersecurity (CySec) threats can encompass multiple objectives. Intrusion scenarios described by Gross (2015) include:

- Cyber crime -- conventional crime committed by individual actors;
- cyber espionage, which may include government-on-government activity as per historical norms; however, recent years have seen pervasive instances of industrial and economic activity;
- cyber warfare, which focuses primarily on military activity where computer operations aim to infiltrate a system and collect, export, destroy, change, or

encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated system. These activities may be technically similar to some cyber crimes but are distinguished by magnitude or severity of impact; and

- cyber terrorism -- "an intersection between cyber crime and warfare" (p. 133). A key element of terrorism is its enactment by non-state entities, which distinguishes it from acts of war.

CySec threats are increasingly prevalent in contemporary society (Ben-Asher & Gonzalez, 2015). The problem domain is dynamic, as threats and their targeted environments are complex and constantly changing (Huang, 2015). CySec breach-related activity has increased over time since the 1990's. The first widespread email virus, Happy99, appeared in early 1999 (Ben-Asher & Gonzalez, 2015). By 2012, more than a half million email-based cyber attacks were intercepted daily in the Symantec cloud environment (Sawyer et al., 2015). The frequency of email-based cyber attacks has increased further since then, doubling between 2014 and 2016 (Sawyer & Hancock, 2018).

Successful CySec breaches have gained notoriety in recent years. Better known incidents include events at:

- Target, the U.S. retailer, where in 2013 70 million customers suffered loss of financial data (Plachkinova & Maurer, 2018);
- Yahoo.com, where a series of breaches that began in 2013 saw personally identifying information compromised for 3 billion user accounts (Shepardson, 2017; Stanciu & Tinca, 2017),

- the financial services firm Equifax, where a 2017 data breach resulted in the compromise of consumer financial data for 143 million users (Federal Trade Commission website, n.d.), and
- Marriott International, which in late 2018 reported a breach of data and payment information from its Starwood reservations system for up to 500 million of its customers (Perlroth, Tsang, & Satariano, 2018).

Human Factors in CySec

The CySec problem domain is extensive; it encompasses both technology and human-based factors. Humans play a critical role – a 2014 IBM Global Technology Services CySec report attributes more than 70% of successful CySec breaches to human action (Carlton & Levy, 2015; Parsons et al., 2017). Although in-house experts are necessary for effective CySec, they are insufficient to ensure its effectiveness (Beyer & Brummel, 2015). Human activity in CySec varies by incident type and individual characteristics – three general human role types are associated with CySec problems: a) CySec specialists, b) malicious individuals or parties (i.e., hackers) and c) IT end-users. (Beyer & Brummel, 2015; Cavelty, 2014). End-users are crucial for sound CySec, as IT systems are vulnerable to threats caused by end-user behavior; human behavior significantly affects the frequency and severity of CySec intrusions, and human decisions determine whether cyber intrusion attempts succeed or fail (Aldabbas & Teufel, 2016; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Sawyer et al., 2015). Beyer and Brummel (2015) note vulnerabilities frequently arise from circumstances involving IT end-users who lack certain knowledge or skills. Attitudes and behavior also impact risk of cyber intrusion (McCormac et al., 2017).

CySec-related behavioral concerns apply to organizations in government, business, and educational sectors (Rawal, Liang, Loukili, & Duan, 2016). Unintentional CySec compromises can originate from a) inadvertent mistakes and/or b) inaction by responsible individuals. User negligence and lack of related knowledge are associated with both categories of compromise (Cebula, Popeck, & Young, 2014). Insights and/or validation of CySec-related end-user expertise is necessary to understand related risks (Stanciu & Tinca, 2017; Trim & Upton, 2016). An understanding of end-user behavior is also needed to comprehend risks of compromising IT resources (Coventry, Briggs, Blythe, & Tran, 2014).

Until recently, few items of CySec-related literature investigated IT end-user behaviors and vulnerabilities. However, over the past decade, research has investigated human factors in CySec in greater numbers. This assertion was substantiated by a search for relevant scholarly journal articles via the Serial Solutions Summon^{TM} service. Counts were taken of relevant items published by year between 1996 and 2018. Items were identified via use of subject keywords *cyber*, *security* and *human*, combined with the keywords a) *behavior*, or b) *decision*. Table 1 shows the yearly counts. Relevant publication increased significantly after 2006: ($U=2.00$, $p < 0.001$). Despite greater research interest in CySec and human factors over the past decade, a comparison of human factors-focused works against the larger CySec domain revealed that fewer than 3.5 percent of more than 4100 CySec articles published between 1996 and 2018 investigated human factors.

Table 1.

Scholarly Human-Focused CySec Publication Counts by Year

Year	Count of related works	Year	Count of related works	Year	Count of related works
1996	0	2004	2	2012	12
1997	1	2005	4	2013	8
1998	1	2006	6	2014	14
1999	1	2007	7	2015	7
2000	2	2008	6	2016	12
2001	2	2009	13	2017	13
2002	3	2010	8	2018	14
2003	3	2011	4		

IT End-User Behavior

Until recently, most CySec literature items that investigated end-user behavior, attitudes, beliefs, experiences, backgrounds, or other cultural/demographic factors addressed specific scenarios such as email phishing, social media use, or network access. CySec IT end-user-focused research domains appear to have expanded in recent years -- several articles published

since 2015 examine the role of decision-making factors in wider contexts. Relevant works are summarized in Appendix A.

Decision-making factors frequently associated with CySec derive from two related areas: a) protection motivation theory (PMT), introduced by Rogers (1975), and b) technology threat avoidance theory (TTAT), a technology-focused adaptation of PMT, introduced by Liang and Xue (2009).

PMT description. Originally introduced by Rogers (1975), PMT defines predictive elements of individual decision-making regarding actions intended to preclude "noxious" events from occurring (Rogers, 1975, p. 96). PMT includes three core components:

- noxiousness (i.e., severity),
- probability of occurrence, and
- the efficacy of a protective response.

The PMT holds that protection motivation arises from individual realization that some event of a certain severity and likelihood exists, and that a coping response also exists which can effectively prevent the event from occurring. A decision to enact a protective response derives from the problem severity, its probability of occurring, and whether or not the protective response is likely to affect an outcome. Figure 1 shows the conceptual structure of PMT factors.

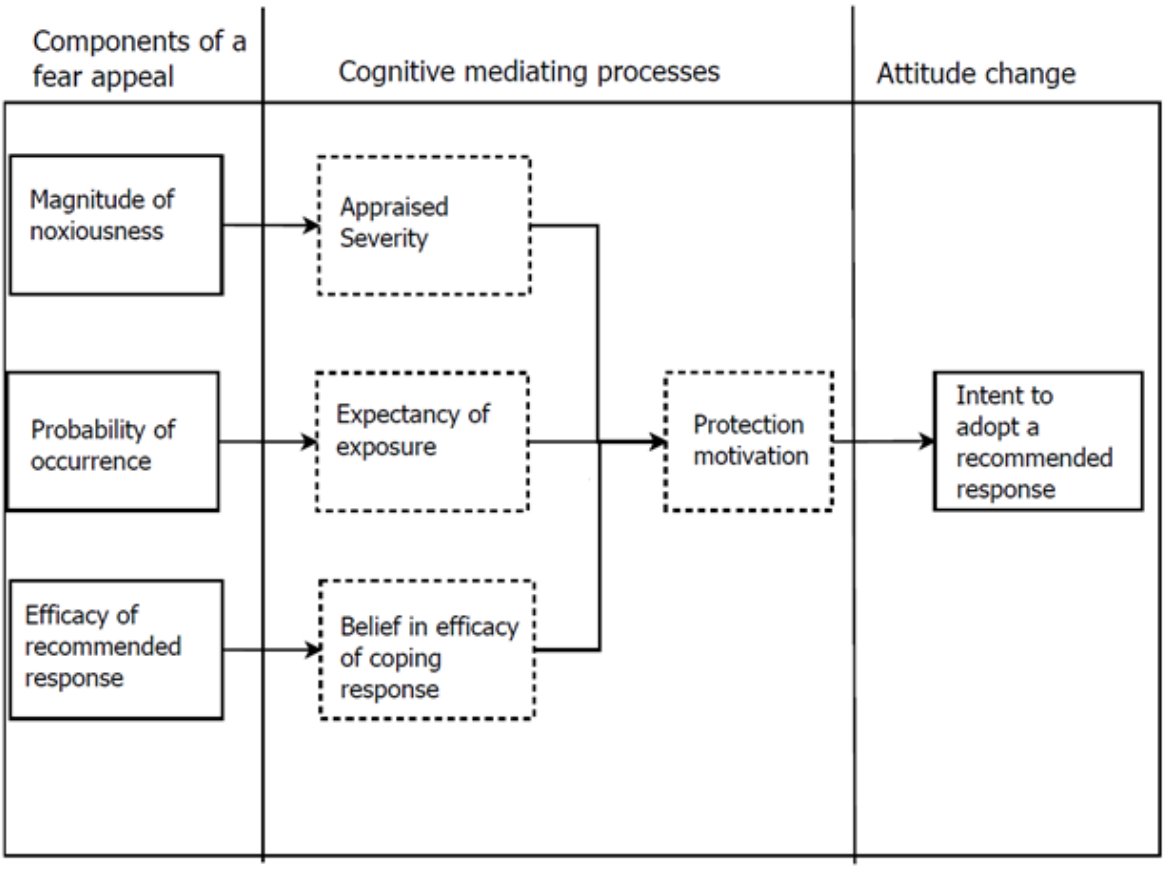


Figure 1. Conceptual schema of basic PMT factors (Rogers, 1975, p. 99)

TTAT description. In 2009, Liang and Xue (2009) extended the PMT by adding and refining multiple factors, and expanding/renaming the attitude change PMT outcome area to accommodate different *coping* behaviors. Noxiousness and probability PMT factors were combined into a new aggregate TTAT factor, *perceived threat*. The efficacy PMT factor was also further refined as an aggregate factor named *perceived avoidability*, comprised of three sub-factors: a) perceived effectiveness, b) perceived cost, and c) self-efficacy of a coping response. Self-efficacy reflects the confidence in one's own ability to apply an avoidance behavior (e.g., someone needing to self-administer an injection of a highly effective medication to fight an illness may not be able to perform the activity). Finally, TTAT coping behaviors are further

refined to differentiate between emotion-focused coping (exercised in instances where actors cannot or will not administer an avoidance behavior), and overt action (i.e., TTAT avoidance coping) to avoid, mitigate, or nullify a threat. Appendix B shows the TTAT instrument from Liang and Xue (2010). Figure 2 depicts its general conceptual model. Several typographical errors noted in the original work were intentionally replicated in Appendix B.

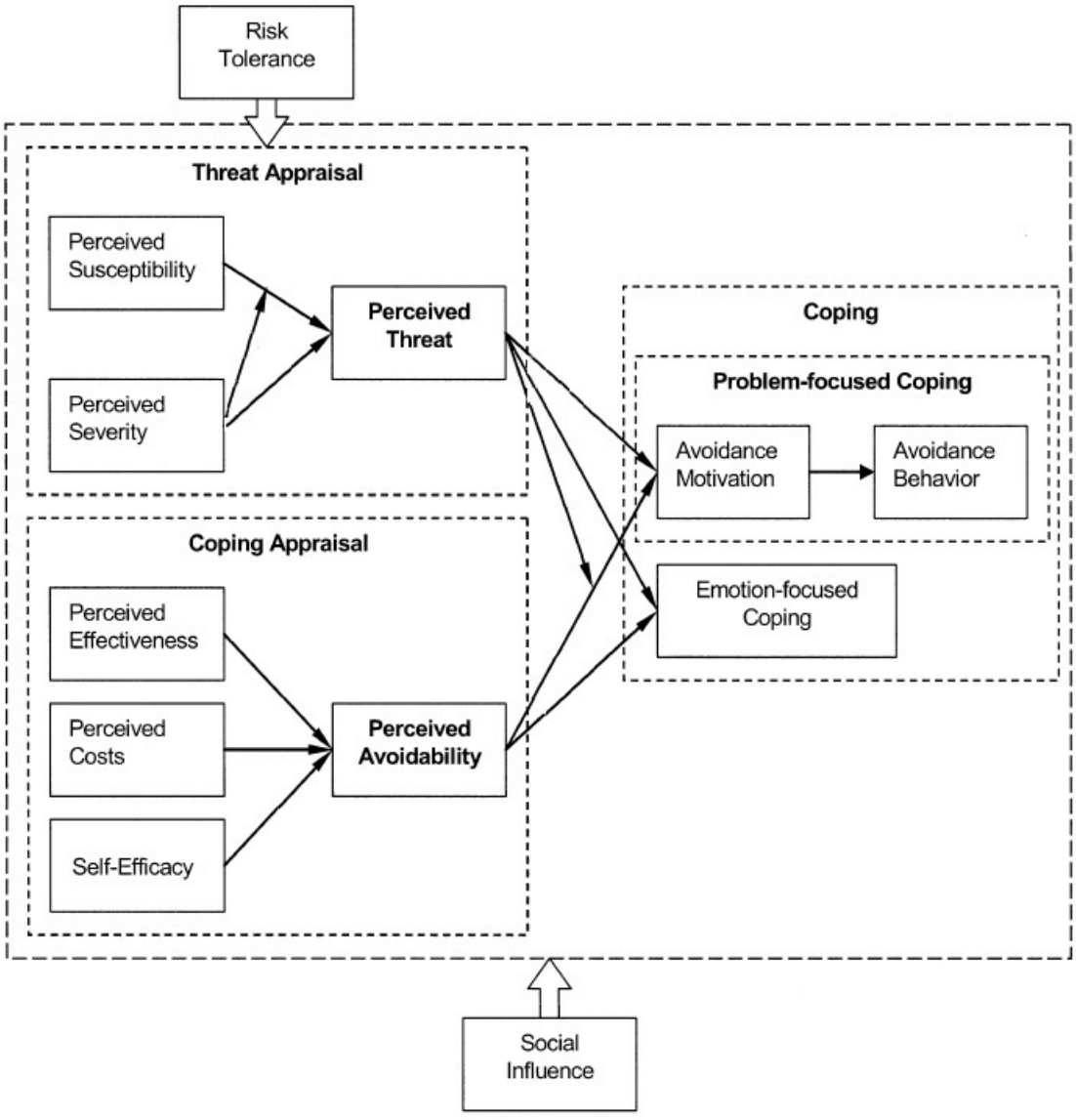


Figure 2. Conceptual schema of TTAT factors (adapted from Liang & Xue, 2009, p. 79)

Theoretical Framework

The study intent is to investigate CySec decision-making factors which affect risk-based decision making by IT end-users. The research is motivated by HRD-related interests. Consequently, the study must be supported by theoretical linkages spanning the disciplines of HRD, CySec, and protection motivation/technology threat avoidance. The concept of technology-based risk must also be associated with these disciplines to fully ground this study.

The HRD discipline has no all-encompassing, centralized theory; Swanson and Holton (2009) outline it as a construct of multiple supporting theories, the primary ones are

- psychological theory, which governs human behavior pertaining to productivity, change, culture, and other nuances;
- systems theory, which governs purpose, components and integration of operational items into a functional whole; and
- economic theory, which describes concepts and entities that drive and sustain organizational existence.

Swanson and Holton (2009) state that independently, the three supporting theories are not adequate for understanding HRD or for garnering reliable results while studying it. They propose an integrative approach to combine "its contributing and useful psychological, economic, and systems theories into a core HRD theory and model for practice" (Kindle loc. 1399). At minimum, a theoretical framework for this research must address elements from all three HRD supporting theoretical areas.

Several decades have passed since the term *cybersecurity* emerged during the 1980's. However, the term still has no widely accepted definition (Stevens, 2018). Similarly, no encompassing theory yet exists to govern the CySec realm; the discipline is currently described

by two dominant perspectives. The first sees CySec as a collection of IT problems which require fixing, while the second considers CySec a collection of issues pertaining to social interaction between humans and IT. Those perspectives do not overlap (Cavelty, 2018). The United States Army similarly characterizes CySec as a mix of underlying hardware/infrastructure, communication nodes, and a social layer of human and cognitive elements (Dawson & Thomson, 2018; TRADOC, 2010). The study addresses these social elements of CySec, and is therefore applicable to HRD research and practice.

The pervasiveness of CySec threats in work environments and the role of human behavior as a determinant of cyber-attack success or failure presents an intuitive case for HRD involvement in CySec activity. General human resources-related implications of IT staffing trends also support this supposition: Information access becomes more important over time to non-IT specialists who must access data to fulfill their job responsibilities. Proliferation of application frameworks to support this need are inexorably pushing greater levels of IT-related responsibility to end-users (Agrawal, Agrawal, Seshadri, & Taylor, 2017). Finally, organization information security (infosec) policies and practices must also be considered, as mandatory infosec compliance measures demonstrate small levels of impact on organization behavior (noted in Da Veiga, 2016 and Hanus, 2014). Environmental considerations to influence organizational behavior are aligned most strongly in the HRD realm.

The theoretical framework builds atop these considerations. Conceptual overlaps between key areas of supporting HRD theory and the problem domain are identified and linked to further depict CySec as an HRD-relevant concern.

Psychological theory and related links between study elements. Multiple areas of psychological theory support the HRD discipline (Swanson & Holton, 2009). *Behavioral*

psychology is based on the premise that observable behaviors derive from circumstantial responses based on the capacity and experience of the individual. *Cognitive psychology* posits that behaviors are objective-oriented, and that humans organize their lives to follow some purpose. Social psychology, oriented on individual interactions with other individuals and groups is also depicted as relevant to HRD by Swanson and Holton (2009). Behavioral psychology is mentioned by Sherman et al. (2018) as one of several vital CySec-supporting disciplines. Multiple recent works cite psychology-based determinants of CySec behavior; among them are Acquisti et al. (2017), Coventry, Briggs, Blythe and Tran (2014), Dawson and Thomson (2018), and Vishwanath, Harrison and Ng (2016). TTAT overtly supports psychological considerations; in the original theoretical work by Liang and Xue (2009), the authors highlight the influence of health-related psychology as an elemental component of TTAT.

Attempts to associate CySec expertise with HRD calls for reconciliation between different styles of risk-taking behavior and incorporates concepts rooted in psychological theory. HRD includes risk-taking and innovation as vital activities in learning organizations (Berdrow & Evers, 2014; Swart, et al., 2005). Such behavior differs from undesired risk-taking. Desired and undesired risk-taking behaviors are described by approach-avoidance theory, a psychological sub-theory, introduced by Atkinson (1957). Risk-taking behavior is frequently considered favorable when individuals or groups show willingness to incur certain risks of loss to approach a set of conditions (i.e., an end state) which is more desirable than the current state. They do this by demonstrating *approach behavior*. The counterpart of approach behavior is *avoidance behavior*, which is demonstrated when individuals maintain the current state when risks are excessive because potential gains do not exceed the consequences associated with a less desirable end state. Despite their similarity, the behaviors are governed by different thought and

reasoning processes which originate in different regions of the human brain (Liang & Xue, 2009; Sutton & Davidson, 1997). Undesirable risk-taking occurs when:

- *approach behavior* is demonstrated in the face of excessive risks, or
- *avoidance behavior* is warranted but not exercised.

Psychological theory pervades the HRD and CySec domains and the TTAT CySec sub-domain, via frequent intersections in behavioral psychology. This aspect of underlying theory is overtly present in HRD; it also manifests clearly in CySec when considered in its social manifestation described by Cavelty (2018), and is definitively part of TTAT and risk-oriented decision-making. The psychological theoretical area intersects strongly among the related disciplines and consequently constitutes a second group of theoretical links to frame this work.

Systems theory and related links between study elements. The relevance of systems theory to HRD derives from need to understand and study how components of organizational and processing systems organize, perform, and deliver work products. Jacobs (2014) observes "system theory has contributed to the understanding of HRD as much or more than any other foundational theory or body of knowledge" (p. 21). Ruona (2009) is less charitable, and states systems theory has not yet fully taken hold as a part of the foundational base of HRD. The disparity is highlighted in related characterizations by Thomas (2017), who characterizes systems theory as insufficient for examining interactions between humans and systems because a pure systems approach considers humans as procedural objects and not as unpredictable living organisms. System stability and security are noted as relevant aspects of systems theory by Ritzman and Kahle-Piasecki, (2016), who share insights from a pure systems perspective:

> Systems theory allows for a comprehensive view of potential security gaps by examining the subsystems that make up the organization and how they function within the

> organization; it is important to note that a change in one subsystem undoubtedly affects other subsystems within the organization. (p.18)

Ruona (2009) bridges the systems/security gap beyond Thomas (2017) via cybernetics, a sub-area of systems theory which examines communication, feedback, and control inside systems and also between systems and their environments. Cybernetic theory a) comprises the foundation for use of feedback loops in systems to monitor and improve performance and b) is relevant to human behavior, as humans are part of the systems environment. Human/system cybernetic boundaries also present a conceptual link with the social perspective shared by Cavelty (2018) which describes CySec as a set of issues related to social interaction between humans and IT.

Cybernetics are explicitly coupled with TTAT -- Liang and Xue (2009) describe threat avoidance as a cybernetic concept which incorporates a positive feedback loop intended to increase the distance between the current user state and a noxious end state. Psychological theory is implicitly shared in this description via concepts intrinsic to approach-avoidance behavior, described earlier in this section. General systems and cybernetics theories, augmented by psychological theory comprise the second set of common connections that permeate the problem areas of HRD, CySec, TTAT, and IT end-user risky behavior.

Economic theory and related links between study elements. Economic theory envelops HRD-relevant *human capital theory* (Swanson & Holton, 2009). Human capital theory holds that when organizations incur the cost of training and educating members of a workforce, such outlays comprise capital expenditures by the employer (Becker, 1993). The magnitude of such investments are guided by an economic concept entitled *scarce resource theory* (Swanson & Holton, 2009). Scarce resource theory addresses allocation of finite enterprise resources to

derive the greatest possible benefit from each expenditure. From an HRD perspective, greatest benefit derives from activities which yield the greatest, most impactful changes in organization performance (Swanson & Holton, 2009). Similar concerns apply to CySec, which suffers from problematic levels of investment in many organizations -- CySec investments are not incrementally associated with new revenue, and are not readily quantifiable in terms of cost avoidance or immediacy of need (Gordon, Loeb, Lucyshyn, & Zhao, 2018). TTAT overtly supports considerations of scarce resourcing – the theory includes explicit cost considerations. Several works find CySec cost magnitude negatively associated with threat avoidance behaviors: Liang and Xue (2010), Samhan (2017), and Tsai et al. (2017). Finally, one must consider general economies of scale for addressing enterprise-wide needs. Centralized HRD-managed training programs can also provide commonality and organization across the enterprise with consistent program design and execution (Bergeron & Fornero, 2018). Considered holistically, economic theory weaves together aspects of HRD, CySec, and TTAT to partially integrate the theoretical framework, and support additional argument for CySec expertise development as an HRD-related concern.

Summarizing the theoretical links. The HRD and CySec disciplines are not self-contained theoretical bodies. Therefore, a theoretical framework to support HRD-fueled research of CySec, TTAT and IT end-user risky behavior must reconcile elements across several supporting theoretical areas. The HRD and CySec disciplines were examined in light of key HRD contributing theories to unearth shared interdisciplinary links. The combined set of links from psychology, systems, and economic theory form a collective framework to support a) conceptual applicability of this research as an HRD-motivated activity and b) evaluation of

TTAT factors as antecedents of risky CySec behavior by IT end-users. The intersection of contributing theories and coupling of the HRD and CySec domains are depicted in Figure 3.

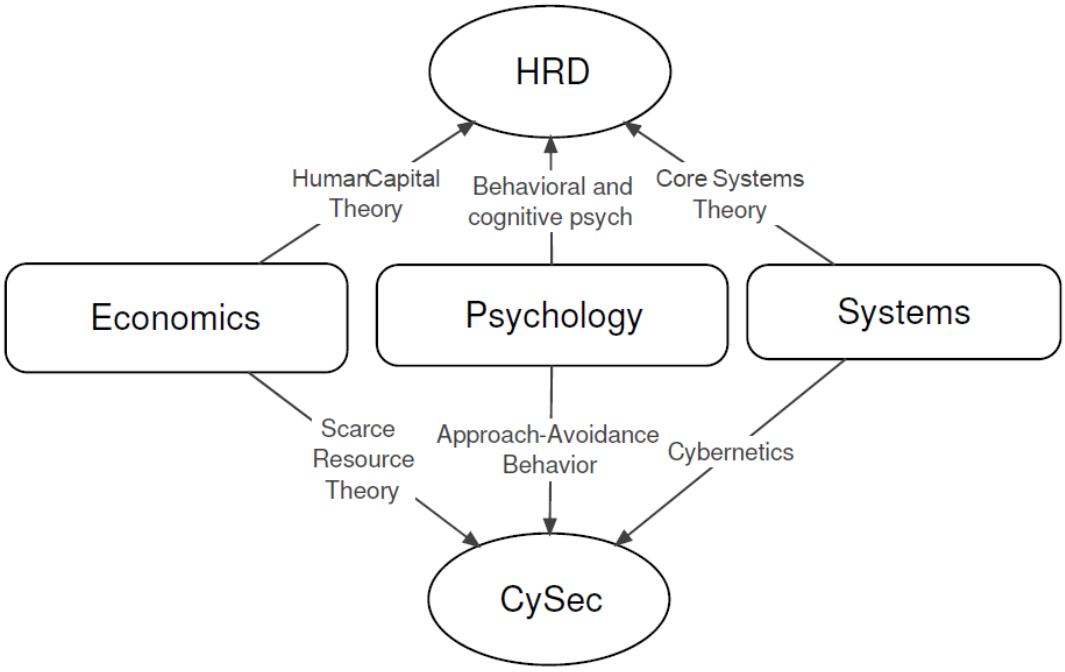


Figure 3. Interdisciplinary theoretical model -- HRD and CySec

Statement of the Problem

Risky CySec behavior (RScB) occurs when IT end-users do not exercise avoidant behavior in circumstances where it is warranted. This poses notable risk to enterprises and organizations. End-user expertise and capable decision-making are critical to manage RScB, as ultimately, success or failure of cyber intrusion attempts hinge on the actions of end-users (Beyer & Brummel, 2015). Factors which motivate protective behavior in IT environments are vital influences in CySec end-user decision-making. Published research investigates the role and impact of human protective motivation and threat avoidance factors regarding technology acceptance, CySec incident rates, and preventive behaviors. Further exploration of the role and

impact of PMT/TTAT factors as predictors of risky CySec behaviors is needed to grow relevant HRD knowledge, and better inform the HRD community of the urgent need for initiatives to diminish inappropriate and costly CySec behaviors in the workplace. However, it is difficult to predict RScB in work environments due to limited research addressing CySec practices regarding risk; historically, that capability has not been addressed as part of HRD-sponsored training and development.

Statement of the Purpose

The explorative one-shot quantitative study explores associations between a) motivational/decision-making factors of TTAT and b) IT end-user self-reporting of RScB by adults who use or have used organization IT assets to perform their work on a regular basis. Previously published TTAT-oriented works focus on dependent variables (DVs) associated with protective (i.e., non-harmful) CySec workplace behavior. In contrast, the research seeks to extend the HRD CySec-focused body of knowledge by examining associations between TTAT factors and risky (i.e., potentially harmful) CySec behavior. The specific purpose of the study is to identify and analyze relationships between TTAT factors and RScB in the workplace.

Several research questions explored the impact of technology threat avoidance factors on IT end-user RScB, the latter represented by variable values obtained from the RScB instrument by Hadlington (2017). The study questions are:

- To what extent do significant associations exist between TTAT factor values and RScB?
- To what extent can RScB instrument measures be categorized for descriptive classifications of RScB (e.g., to incorporate levels such as *low*, *medium* or *high*)?

- Which TTAT factors are the strongest and weakest predictors of RScB?
- To what extent do associations between TTAT factor values and RScB appear consistent with previously published associations between TTAT factor values and measurements of protective (i.e., non-harmful) behavior?
- To what extent do significant associations between TTAT factors on RScB demonstrate HRD business-level utility (i.e., differences in terms of statistical effect sizes)?

Statement of the Need

The research need derives from HRD concerns regarding adverse impacts on organization performance which originate from risky workforce behavior. Literature to date describes research which explores associations between TTAT factors and a variety of IT-related DVs including technology acceptance, frequency of adverse CySec incidents, and demonstration of protective CySec behaviors. The current state of the supporting literature is summarized in Figure 4.

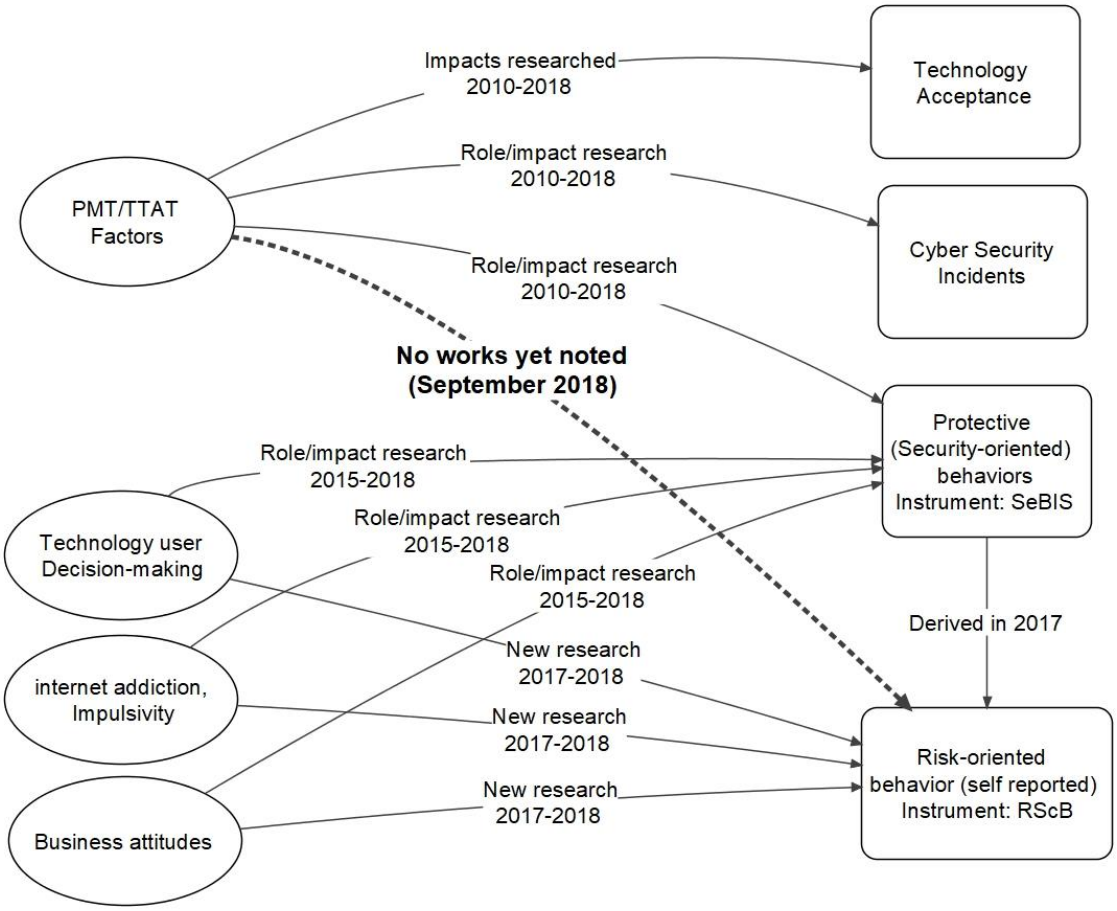


Figure 4. PMT/TTAT literature foci, mid-late 2018

Multiple researchers have investigated associations between TTAT factors and avoidance behaviors originally described by Atkinson (1957). Avoidance behaviors described by their works were typically comprised of activity to protect IT assets from breaches. The body of knowledge currently lacks research which investigates the role and impact of TTAT factors on undesirable risk-taking (i.e., failures to demonstrate avoidance behavior while performing work). The body of knowledge must expand to fully address the range of behavior described by approach-avoidance theory, and more fully inform the HRD community of CySec workplace behavior that adversely impacts organization performance.

Statement of the Assumptions

Several underlying assumptions shaped and governed the research domain. Those assumptions were:

1. Hierarchical regression analyses of the RScB DV (RScB) by Aivazpour and Rao (2018), and Hadlington (2017) sufficiently characterize the RScB instrument score as an interval-based DV suitable for analysis via least squares regression techniques.
2. Previous study of the RScB DV by Aivazpour and Rao (2018), Hadlington (2017), and Hadlington and Murphy (2018) establishes sufficient RScB content validity to support use of the RScB instrument in this study (content validity was established via conferral with law enforcement and digital forensic specialists).
3. Previous study by Aivazpour and Rao (2018), Hadlington (2017), and Hadlington and Murphy (2017) establishes sufficient RScB predictive validity for the RScB to reflect risky cybersecurity behavior by IT end-users (demonstrated via significant associations between RScB and media multi-taskers, individuals with high motor impulsivity, and participants who demonstrated internet-addictive behavior).
4. The TTAT instrument by Liang and Xue (2010) provides a reliable and valid instrument for studying self-reported aspects of individual IT end-user protective motivation in CySec environments as per findings by Chen and Li (2017), Herath et al. (2014), Samhan (2017), Talebi (2018), and Tsai et al. (2016).
5. Respondent anonymity mitigates risk of participant response bias.

Statement of the Limitations

This study incorporated several limitations. Those are listed as follows:

- Convenience sampling was used; potential participants were contacted primarily via email and social media, and effects of snowballing.
- The research did not categorize findings by regional, racial, socioeconomic, or cultural demographic attributes.
- Administration of the questionnaire was limited to online delivery with no paper-based counterpart.
- The DV was based on self-reported IT end-user behavior and not subjected to observation/verification.
- The DV was based on an aggregate scalar RScB instrument value; sub-factors were not formalized or analyzed aside from actions taken to ensure that adequate levels of internal consistency were met to support the study.
- Multiple participant recruitment samples were targeted for the study. However, the instrument does not provide means to unambiguously determine a population of origin for individual participants.
- Social factors related to the work environment may effect work performance which may include demonstration of risk-taking behavior by IT end-users; Hawthorne effect (introduced by Mayo, 1933) and Pygmalion effect (originally discussed by Rosenthal and Jacobson, 1968) are examples – neither were targeted for measurement or evaluation by this research.
- Due to greater levels of CySec protection in formal organizations which can dedicate more IT assets to protective infrastructure than can individuals, IT end-

users may be compelled to exercise risky behaviors they would not exercise otherwise (Hadlington, 2017). This study used no safeguards to preclude this from occurring or to quantify its impact.

Statement of the Delimitations

Qualified study participants were adults (age 18 and older) in the United States either currently or previously employed by companies with a U.S. presence, who are (were) required to use employer-owned IT assets when fulfilling their work assignments. Targeted participants were not delimited by industry or work specialization. Study participants required some means of accessing the study instrument online. Both personal and employer-owned assets were considered acceptable for accessing the instrument.

Significance of the Study

To date, no published CySec studies have examined the predictive strength of technology threat avoidance-based independent variables (IVs) using RScB as a DV. This research uniquely contributes to the literature by revealing the role and impact of PMT/TTAT on the prevalence of RScB reported by U.S. adults with employment experience who use or have used organization-owned IT assets to accomplish their work.

Operational Definitions

Attentional impulsivity. A form of impulsive behavior which adversely affects someone's ability to focus on the task at hand (Whiteside & Lynam, 2001).

Construct validity. Ascertainment a research instrument measures the constructs it was designed to measure, usually provided by some form of factor analysis (Matsumoto & Hwang, 2013).

Cybersecurity (CySec). The information systems and human-based concerns which encompass the safeguarding and authorized use of electronic information assets and supporting infrastructure owned by organizations and individuals.

Cyber threat. A potential action or circumstance that can be used against IT assets by exploiting one or more cyber vulnerabilities (Sherman et al., 2018).

Cyber vulnerability. A shortcoming or weakness that could lead to IT assets being compromised or damaged (Sherman et al., 2018).

Generation (Gen) Y. Individuals born between the years of 1977 and 1995 (Hobart & Sendeck, 2014).

Human resource development. "A process of developing and unleashing expertise for the purpose of improving individual, team, work process, and organizational system performance" (Swanson & Holton, 2009, Kindle loc. 181).

Malware. Malicious software logic placed on compromised IT platforms. Includes all types of intrusive mechanisms including viruses, worms and other destructive or intrusive software programs (Broucek & Turner, 2013)

Media multi-tasking (MMT). The simultaneous use of two or more types of media or a persistent alternation between media types such as watching TV, text messaging, web surfing, e-mailing, talking via phone, etc.) (Hadlington & Murphy, 2018).

Motor impulsivity. A form of impulsive behavior where the individual takes action on the spur of the moment and/or exhibits restlessness while choosing an action (Holmes et al., 2009; Whiteside & Lynam, 2001)

Phishing. Use of email for cyber attacks, primarily to deliver malicious code (malware) or obtain information (Sawyer, et al, 2015)

Risky CySec behavior (RScB). IT end-user conduct which reflects low levels or absence of avoidance behavior defined by Atkinson (1957) and further described by Liang and Xue (2009).

Social engineering. Manipulation of individuals to motivate them to share information about organizations or assets they would not normally share, while not raising their suspicion. This includes manipulation via online methods and by voice (i.e., "vishing") (Mitnick & Simon, 2011; Yeboah-Boateng & Amanor, 2014)

Virus. A self-propagating malware item which propagates due to software flaws exploited by actions of IT end-users. May also include logic payloads to cause damage or perform work on compromised systems (Bauer, Van Eeten, Chattopadhyay, & Wu, 2008)

Worm. A self-replicating malware item which contains logic to identify and travel over connections to other systems to become more pervasive. May also include logic payloads to damage or perform processing on compromised systems (Bauer, et al., 2008).

Statement of the Method

This exploratory correlational research investigates associations between a) individual attitudes and intentions to avoid technology threats and b) self-reported RScB in the workplace. Measurements were collected via an instrument comprised of combined mechanisms by Liang

and Xue (2010), and Hadlington (2017); the instrument also incorporated refinements by Samhan (2017), and Tsai et al. (2017). Associations were investigated using ordinary least squares regression to determine the strength of any associations, compare RScB outcomes with studies of protective (non-harmful) behavior, and determine the degree of business-level utility inherent in the findings. Finally, levels of RScB were explored via k-means clustering to establish descriptive categories of RScB in the workplace.

CHAPTER 2

REVIEW OF THE LITERATURE

A review of literature for this study began with works that strive to outline the general CySec domain. The domain is not well-defined, as the field is considered to be in its infancy. Moreover, it is expanding faster than research can keep pace with (Dawson & Thomson, 2018). The rate of expansion has motivated several recent holistic research efforts to understand the general CySec domain and its boundaries. Holistic studies frequently incorporate the well-known Delphi method, originally championed by Olaf Helmer of Rand Corporation in 1963 and 1967. The Delphi study by Carlton and Levy (2015) identifies threat types across the general CySec expanse and analyzes them in terms of rank/order. A group of subject matter experts from law enforcement and private industry supported the research. Figure 5 shows the resulting rank/ordered threat types across nine areas. Findings fueled subsequent development of a CySec skills assessment instrument described by Carlton (2016).

Variable	Components	Description	Range	Weight
SK_1	$T_{1_1} + T_{1_2} + T_{1_3} + T_{1_4}$	Preventing the leaking of confidential digital information to unauthorized individuals	0 – 40	.136
SK_2	$T_{2_1} + T_{2_2} + T_{2_3} + T_{2_4}$	Preventing malware via non-secure Websites	0 – 40	.132
SK_3	$T_{3_1} + T_{3_2} + T_{3_3} + T_{3_4}$	Preventing personally identifiable information (PII) theft via access to non-secure networks	0 – 40	.127
SK_4	$T_{4_1} + T_{4_2} + T_{4_3} + T_{4_4}$	Preventing PII theft via e-mail phishing	0 – 40	.112
SK_5	$T_{5_1} + T_{5_2} + T_{5_3} + T_{5_4}$	Preventing malware via e-mail	0 – 40	.109
SK_6	$T_{6_1} + T_{6_2} + T_{6_3} + T_{6_4}$	Preventing credit card information theft by purchasing from non-secured Websites	0 – 40	.100
SK_7	$T_{7_1} + T_{7_2} + T_{7_3} + T_{7_4}$	Preventing information system compromise via USB or storage drive/device exploitations	0 – 40	.097
SK_8	$T_{8_1} + T_{8_2} + T_{8_3} + T_{8_4}$	Preventing unauthorized information system access via password exploitations	0 – 40	.095
SK_9	$T_{9_1} + T_{9_2} + T_{9_3} + T_{9_4}$	Preventing PII theft via social networks	0 – 40	.092
CSI	$\left(\frac{5}{2}\right)\sum_{i=1}^{9}[(SK_i) \cdot w_i]$	Coefficient * (Sum of all 9 skills * respective weights)	0 – 100	

Figure 5. Rank/ordered CySec threats (from Carlton, Levy, Ramim, & Terrell, 2016, p. 5)

A general best practices/human factors-oriented work by Coventry, Briggs, Blythe, and Tran (2014) shares insights regarding general IT end-user behaviors known to mitigate risk of cyber intrusion, irrespective of threat types. It also lists hindrances to adoption of end-user best practices:

- IT end-users are routinely told that substantial risks are associated with online activity,
- IT end-users do not directly experience negative outcomes related to risks they are told about; if they do experience negative outcomes, the outcomes cannot be related back to a specific behavior the end-user had the power to change; and
- CySec experts unintentionally communicate to IT end-users that they can do a few things to self-protect, but experts frequently do not agree on what those things are.

The article shares a three-factor framework of personal, social, and environmental factors to influence development and evaluation of CySec interventions. Coventry, Briggs, Blythe, and Tran (2014) also point out the need to ensure a) interventions are targeted for specific

organizational objectives, and b) CySec factors are revisited over time to adopt interventions as the CySec domain shifts.

Iterative Delphi studies by Sherman et al. (2017) address the expansive nature of the CySec domain, but do so regarding knowledge, skills and behaviors for CySec analysts. They illustrate CySec boundaries using six example scenarios. The scenarios range from protecting package delivery by drones, to protecting against social engineering activity. Another CySec analyst-targeted work, Parekh et al. (2018), use the Delphi technique to analyze education and training needs. The needs expanse includes aspects of general decision making (e.g., prioritization, ethical behavior, and privacy) as well as CySec-specific training regarding intrusion detection and protection. Dawson and Thomson (2018) also anticipate future CySec analysts to be systemic thinkers, team players, motivated continual learners, strong communicators, and civic-minded individuals who possess a mix of technical and social skill.

Classifying the Threats

The inexact nature of the CySec domain is demonstrated by the absence of a widely accepted taxonomy for classifying intrusion attempts. IT end-user-targeted threats, referred to as *semantic user attacks* by Heartfield and Loukas (2015) defy classification despite the end-user-targeted nature of relevant intrusion techniques. Countermeasures similarly defy classification, which can complicate efforts to unify related knowledge and manage end-user interventions. Heartfield and Loukas (2015) share a taxonomy to provide structure for the domain. However, a widely used threat classification scheme has yet to take root. The inexact, frequently changing CySec footprint further implies HRD relevance as the problem space encompasses larger proportions of enterprise activity over time.

Information Security

The strong alignment of CySec with IT has motivated the presence of a related policy artifact in many organizations. The artifact is strongly rooted in the IT realm: the *information security (infosec) policy*. An infosec policy a) guides employees who process information and b) establishes a baseline for ethical decision-making when employees use information. The policy also influences employee interaction with information assets and guides compliance with legislative, regulatory and contractual requirements (Da Veiga, 2016). Ritzman and Kahle-Piasecki (2016) observe that up to one third of organizations do not have infosec policies, despite their characterization as indispensable artifacts: "Development and implementation of a comprehensive information security policy is the first and perhaps the most important step toward preparing an organization against assaults from both internal and external security threats" (p. 18).

In organizations where infosec policies are institutionalized, not all employees will have been exposed to or trained about it at any given time. This occurs for a variety of reasons. Employees who have read infosec policies may have a shared understanding of the organization's common values to protect information. De Veiga (2016) describes findings of a survey administered to employees of a large international corporation in four iterations between 2006 and 2013 that resulted in nearly 8000 responses: a) fewer employees who read the infosec policy shared passwords (85.1% versus 89.8 %), b) employees who read the policy protected data offsite (54.8%) to a greater degree than those who had not read the policy (45.3%), and c) more employees who read the policy exercised care talking about confidential information in public (74.2%) than those who had not read the policy (69.6%). Although the differences are arguably notable and likely significant; significance can occur merely due to large sample sizes

(Lin, Lucas, & Shmueli, 2013). Business-level utility in statistical measures is reflected by calculations of effect sizes (ES), classified as small, medium or large in basic models shared by Cohen (1992). No ES metrics are shared by De Veiga (2016) to reflect operational impact of employees who read the infosec policy.

The dissertation by Hanus (2014) explores impacts of the infosec policy in a Texas municipal organization. Structural equation modeling (SEM) measured the impact of several variables as predictors of a) infosec awareness, and b) intended infosec policy compliance. Employee attitudes towards the infosec policy appeared to be the strongest predictor of intent to comply with the policy; the presence of enticements and sanctions did not demonstrate significant impact on intention to comply with the policy, nor did the employees overall level of security awareness. Neither Hanus (2014) nor Da Veiga (2016) observe medium to large effect size impacts on actual or intended employee CySec behavior. HRD implications may derive from both works if considered in light of Choi and Ruona (2011) – formal directives did not demonstrate medium or greater effects on a) individual intention to comply with the policy in the case of Hanus (2014) or b) actual compliance behaviors described by Da Veiga (2016). This consideration is consistent with the 2011 work, which states coercive/power strategies for initiating behavior change are less effective than strategies based on combinations of empirical awareness and normative behavior.

IT End-Users

IT end-user characteristics are widely associated with susceptibility to cyber intrusion. Those characteristics include attitudes, beliefs, experiences, professional backgrounds, and other cultural/demographic factors which affect IT end-user online behavior differently than they

affect behavior in face-to-face or personal settings. Cyber-enabled dissociative anonymity may motivate IT end-users to be more likely to divulge personal information to strangers than they would otherwise (Yeboah-Boateng & Amanor, 2014).

User knowledge, skill, ability, and behavior (KSAB) are key to many CySec domain studies (Barlette, Gundolf,& Jaouen, 2015; Coventry, Briggs, Blythe, & Tran, 2014; Yeboah-Boateng & Amanor, 2014). Relevant works are intrinsic to the CySec domain, yet are often not recognized; Astakhova (2015) observes end-users are "greatly underestimated in the practice of information security" (pp. 635-636). Other works by Beyer and Brummel (2015) and Cebula et al. (2014) characterize human actions as key factors in CySec. Groups are frequently studied to uncover and understand differences in CySec behavior. Observations of several such studies relate to gender, age, interests, and other such factors. Recent studies are described below.

Gender. Gender-based findings are mixed across a wide expanse of studies. No significant differences arose regarding gender when studied in light of CySec-related behaviors by several works:

- adoption of CySec safeguard measures studied by Samhan in 2017 and van Schaik, also in 2017, or those who used CySec software for home computers, studied by Claar and Johnson in 2012;
- email phishing recognition activity by Sawyer and Hancock (2018),
- victims of online fraud studied by Van Wilsem (2013),
- gender-based covariance in the ANOVA-based analysis of cyber risk awareness by Coventry, Jeske, and Briggs (2014), and
- the PMT-focused dissertation by Talebi (2018).

Most studies which noted significant differences between males and females regarding CySec behaviors found females exhibited greater cyber vulnerability. These research items included Fagan, Albayram, Khan, and Buck (2017), who noted males used password management software more frequently than females. Several studies of email phishing behavior noted greater phishing vulnerability in females than males:

- Hanus (2014) noted males were less likely to open phishing emails;
- Goel, Williams, and Dincelli (2017) noted males were less likely than females to open phishing emails, but neither gender was more likely to activate embedded phishing links inside an email;
- Gratian, Bandi, Cukier, Dykstra, and Ginther (2018) found females reported less effective password generation than males;
- Sawyer et al. (2015), cite multiple works where females were more likely to open phishing links than males, and were also more likely to share personal information via phishing links;
- Sheng et al. (2010) noted more females clicked phishing links than males, where the proportion of females who provided personal information after clicking the link was even greater than for the original clicking behavior; however, after a set of training interventions, no significant differences were noted between genders;

Only one study of the reviewed items noted significantly lower levels of CySec vulnerability by females: the PMT-focused study by Tsai et al. (2016). However, gender represented the weakest correlation with the DV (protective intent) among the 11 significant IVs ($r = 0.07$; $p < .05$, $n = 988$).

Age. Subject age poses additional considerations in CySec study. Coventry, Briggs, Blythe and Tran (2014) note a problematic consistency of cyber vulnerability-focused end-user studies -- many occur in university environments with student participants who are younger than the population mean. Most of the articles reviewed for this research show low levels of association between age and CySec activity. Most items showed no significant relationships between age and their respective DV when age was included as an IV. Most notable among these works is Liang and Xue (2010), the original TTAT study, which found no significant associations between participant age as a control variable and avoidance motivation or behavior. Conversely, the PMT study by Samhan (2017) noted age positively associated with protective behavior. Reviewed works which share significant age-related findings are:

- Sheng, Holbrook, Kumaraguru, Cranor, and Downs (2010) find younger individuals more likely to follow phishing links in emails, and
- The Netherlands-based study of online fraud by Van Wilsem (2011).

The Dutch study of online victimization in a 6200 person sample found approximately 2.5 percent of individuals lost money online from undelivered purchases. The percentage was higher among individuals less than 35 years of age (4 percent), and lower among individuals 55 and older (0.5 percent). Impulsive behavior was the greatest predictor of online victimization noted by that study; that attribute was not significantly associated with age or gender. Adoption of CySec protective measures may be affected by age as well; in 2012, Claar and Johnson noted that older users of home computers perceived greater difficulty using CySec software than did other age groups.

Age, work patterns, and CySec. Age-related work patterns are explored by Leuprecht, Skillicorn, and Tait (2016) regarding work and online use behaviors by Gen Y age cohort

members. Work patterns are contrasted with earlier age cohorts and IT models; earlier models adhered to barricade-based protections and physical levels of security whereas the constantly connected mindsets of younger workers blur distinctions between work and non-working activity. Work productivity is not limited to set time intervals or geographic locations, which presents a quandary -- individuals are as likely to perform personal online contact at the workplace as they are to perform work in public (unsecure) venues. Substitution of privately owned devices for employer-provided ones is widespread as well, as:

- Gen Y members are prolific early adopters of technology, preferring instead to acquire new personal equipment immediately upon market release and leverage it for work in any convenient setting; and
- increasing prevalence of employer support for bring your own device (BYOD) to work policies which support employees' use of personally-owned equipment to do their jobs (Dang-Pham & Pittayachawan, 2015).

Security protocols are consequently subverted in these circumstances. Members of younger age groups also prefer broadcast channels over one-to-one or one-to-many transmissions such as email; exchanges are in near real time, and cover larger social circles than other age group cohorts. Users self-determine what is transmitted, which also circumvents gatekeeping mechanisms that may be in place.

Special interest groups. Online activity poses greater challenges for individuals with physical impairments than non-impaired individuals; difficulties arise from accessibility issues and security concerns. Individuals with visual impairments were participants in a study by Inan, Namin, Pogrund, and Jones in 2016. Hindrances arose from a combined fear of cyber-threats, exposure of sensitive information, and limited accessibility of the internet and its features. A

majority of 20 participants, self-reported a variety of online activities when personally interviewed:

- 80% used email,
- 70% browsed for entertainment,
- 70% used online file transfers,
- 65% performed educational activity,
- 85% shopped online, 80% banked online, and 85% made online payments.

Participants reported three primary problem areas with online activity: a) automatic web page refreshes, b) images with missing alternate text descriptions, and c) difficult/complex web forms. Areas of highest CySec concerns for 70 percent of the sample were stealing of private information. Similarly, 70 percent were concerned regarding unauthorized access to financial information, and 65 percent were concerned about personal information being made public. The area of lowest concern was of computing devices becoming infected by malware (35 percent). Participants' knowledge and skills had significant negative correlations with level of cybersecurity concern and frequency of internet activities. Conversely, frequency of internet issues/problems was found to have a positive, significant correlation with the frequency of internet activities and social media involvement.

Knowledge and skills-based groups. Cyber vulnerability to email phishing of university students in the U.S was examined by Goel et al. (2017) using knowledge and skill-based groupings. Individuals with higher levels of education and those studying in science, technology, engineering, or math (STEM) related fields appear significantly less susceptible to phishing traffic than learners in other areas. Business majors were more likely than humanities majors to open phishing emails, but the groups did not differ in the proportion of members who activated

embedded phishing links. HRD implications are noted in that work – training may best be formulated to address highly contextualized messages which infer risk of loss from not responding. For the participant sample in Goel et al. (2017), phishing emails that warned students of de-registration in coursework were the most effective at baiting users to follow embedded links.

Computer configurations derived from interest groups of users comprised four study categories by Ovelgönne, Dumitraş, Prakash, Subrahmanian, and Wang (2017): gamers, professionals, software developers, and others. Those four classes were augmented by an overall fifth category which incorporated all subjects. CySec risk was characterized using software which analyzed installed programs and utilities on participant computers, as well as history of malware attacks detected by the Symantec CySec product suite. Executable images were sub-classified as high prevalence, low prevalence, uniqueness, signed/unsigned, and downloaded. A final IV, travel history, rounded out the IV set. The group with the highest number of executable images on machines was also the most frequently attacked – software developers. Non-development systems also exhibited higher attack frequencies when higher numbers of executables were installed, but not to the same degree as software development systems. It is important to note that attack frequencies do not equate to infection rates, although the two concepts are related. Ovelgönne et al. (2017) declined to observe whether software developers were better equipped to fend off attacks due to greater domain expertise, or whether said expertise establishes a false sense of security.

Social media users comprised participants for the study by Saridakis, Benson, Ezingeard, and Tennakoon (2016), who analyzed online victimization in light of user activity and perception

of personal information security on social networking services (SNS). Services were sub-divided into three classifications: General focus (Facebook, Google+, etc), narrow focus (e.g., World of Warcraft, Second Life, MySpace), and knowledge exchange (e.g., Twitter, LinkedIn, Blogger and Flickr). The study found negative associations between general SNS use and victimization, and positive associations between knowledge exchange services and victimization. For knowledge exchange SNS users, higher levels of victimization did not occur for frequent users of SNS or users who perceived low levels of risk in using SNS. Individuals with higher perceptions of computer efficacy were not associated with lower levels of victimization, either. Two significant IVs were noted: Individuals who perceived high levels of control over their personal information were victimized less frequently, and individuals who claimed a high propensity for risk-taking saw higher degrees of victimization. Related take-aways were:

1. social networking usage affects online victimization, but the sign, significance and magnitude of the effect depend on the network type;
2. cybercrime can be mitigated by increasing service security controls on social media sites, and by improving skills of end-users to better control the process of personal information disclosure, and
3. awareness of risky user behavior on social media plays a significant role in reducing cyber victimization.

The findings by Saridakis et al. (2016), contrast with those by Van Wilsem (2011) which note significant positive associations between higher levels of SNS use and online victimization; forum participants at the age of 20 were more than 4 times as likely as non-forum participants to experience online victimization as were 20-year-old forum non-members. An accompanying

regression analysis showed more frequent forum use by individuals with lower levels of self-control. Composite user profile comparisons are shown in Figure 6.

Respondent profile	Predicted probability of victimization (per cent)
Age 20 years, academic education, active online shopper, active forum participant, low self-control	43.1
Age 20 years, academic education, active online shopper, non-participant in forums, high self-control	9.9
Age 20 years, low education, active online shopper, non-participant in forums, low self-control	10.1
Age 60 years, academic education, non-shopper, active forum participant, high self-control	3.8
Age 60 years, low education, active online shopper, non-participant in forums, low self-control	4.8
Age 60 years, low education, non-shopper, non-participant in forums, high self-control	0.6

Figure 6. Predicted likelihood of user victimization (from Van Wilsem, 2013, p. 175)

Protection Motivation

Many CySec studies investigate associations between IT end-user KSABs in regards to CySec-related risk avoidance. Factors associated with PMT are frequently adopted as variables in CySec studies. Prior to adoption for technology-related study, PMT was widely used in the study of psychology and health-related fields. Claar and Johnson (2012) observe PMT derives from a predecessor developed during the 1950's in the US: the *health belief model* (HBM), which was originally developed to investigate failure of a tuberculosis prevention program sponsored by the U.S. Public Health Service. Rosenstock (1974) describes a major influence by Lewin (1951), and discounts the decision-making impact of historical perspective in protective behavior -- HBM concept development embraced factors reflecting the immediate environment as primary determinants of health-related decisions. This focus on environmental influences

motivated HBM adoption of its original four factors: susceptibility, severity, benefits and barriers.

Creation of the PMT by Rogers (1975) is also driven by health-related concern. However, further investigation conflicts with Claar and Johnson (2012): Rogers (1975) does not cite Rosenstock's work as a basis for PMT; the original 1975 PMT work instead focuses on realignment of fear-based appeals as cognitive influences of motivation, as "One is not affected by even the direst events when they are not perceived or understood" (p. 98). These cognitive elements comprise what Rogers labeled as cognitive mediating processes. They comprise the middle section of Figure 1. Rogers' re-characterization of fear as a cognitive element is central to PMT's distinction from earlier fear appeals-based literature.

Rosenstock, Strecher, and Becker (1988) are credited for adding efficacy considerations to the HBM in the 1980's (Claar & Johnson, 2012). However, PMT incorporated the concept of efficacy nearly a decade before the HBM refinement as part of its baseline (although the later work by Rosenstock et al. does not cite Rogers' 1975 paper). Differences between models (which appear closely related if one ignores supporting references), are described by Jansen and van Schaik (2017) such that "HBM consists of a set of variables that have an effect on behaviour, while PMT arranges its predictor variables in cognitive processes that individuals apply to evaluate threats and coping measures."

Other PMT-associated theories. Some CySec works consider Ajzen's 1991 theory of planned behavior (TPB), based on the theory of reasoned action (TRA), introduced by Fishbein and Ajzen in 1975. Both present factors associated with general behavioral intent, and are considered potentially applicable to the CySec domain as the *reasoned action approach* (RAA), which is built from elements of both theories.

Omissive behavior. The 2008 study by Workman, Bommer, and Straub investigates differences between PMT factors and omissive CySec behavior (i.e., failure to take action to mitigate CySec threats; the equivalent of RScB, although Workman does not use that term). Omissive behaviors are further subdivided into subjective (i.e., questionnaire-based) and objective (i.e., determined via artifact inspection) components. The IVs also incorporate a locus of control factor derived from social cognitive theory by Bandura (1977). The DV basis used by Workman et al. (2008) differs from many subsequent works via the researchers' decision to use DVs based on omissive behavior, which coincides with measurement of undesirable risk-taking, (i.e., lack of avoidant behavior) used for this study (albeit via a user-reported behavior, not an objective measurement).

The omissive behavior study by Workman et al. engaged 588 employees of a large U.S. IT firm. Least squares analysis was used to analyze outcomes, depicted in Figure 7. All PMT factors showed negative associations with omissive behavior, as expected. Associations appeared generally stronger between IVs and subjective DVs than between IVs and objective DVs. The locus of control factor (extent to which motivation to act is internally or externally driven, derived from Bandura, 1977), failed to exhibit significant associations with the objective behavior-based outcome. Multiple PMT works appear to characterize coping activity as a PMT factor, although coping behaviors per se are not intrinsically part of PMT; in PMT, the term *coping* is only used regarding one's level of believed efficacy in taking of an action to contend with a threat. Specific aspects of various coping responses appear following Liang and Xue's 2009 expansion of PMT into TTAT. The inconsistency is noted here instead of in discussions of additional works to preclude repetitive passages when lines appear blurred between PMT and TTAT.

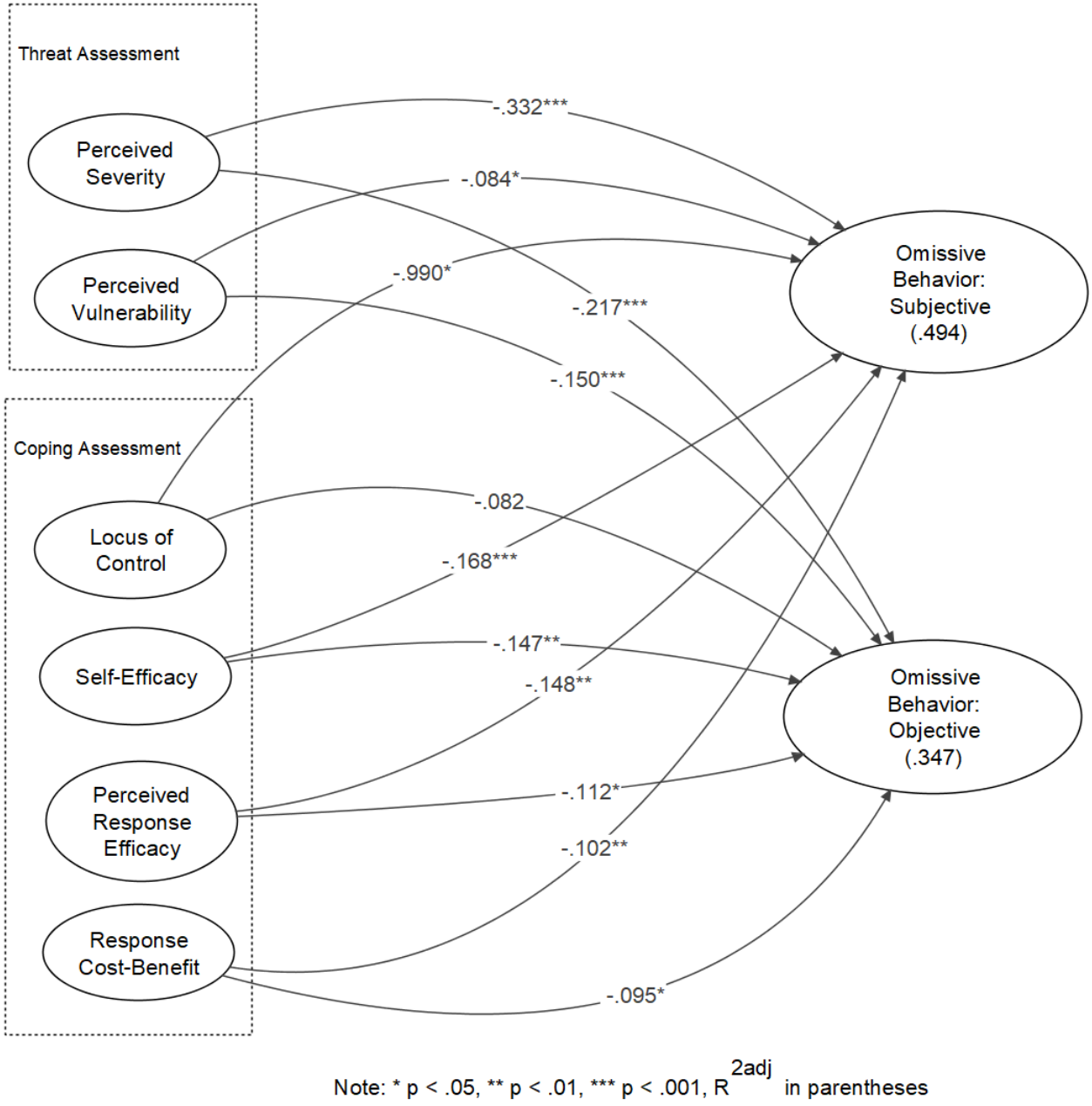


Figure 7. PMT threat assessment measures from Workman et al. (2008, p. 2811)

PMT-based research post-2010. Researchers continued to explore the effects of PMT factors in the CySec realm following introduction of TTAT in 2009-2010. Email authentication service adoption comprised a dichotomous DV in the 2014 study by Herath et al. that developed

and used a model based on multiple theories: PMT, TTAT and the *technology acceptance method* (TAM) introduced by Fred Davis in 1989 (TAM asserts an influence of attitude as a significant factor in technology acceptance). The researchers intended to derive a predictability model for organizational adoption of email authentication security services. Such behavior was anticipated to mitigate risk of CySec threats that use email as an attack vector. External coping mechanisms (i.e., attitudes from the TAM) were identified as having the greatest impact in the partial least squares model, followed by threat appraisal (i.e., risk). The factor of lowest impact was self-efficacy (actually a TTAT factor), which demonstrated a negative association with the DV. Another 2014 work adhered more tightly to PMT considerations, albeit as a literature review augmented by a Delphi exercise. Social and behavioral implications were investigated by Coventry, Briggs, Blythe, and Tran to better understand:

- behaviors needed for people to reduce cyber vulnerability,
- why do people not behave securely online,
- what behavioral theory tells society about how to effectively influence behavior,
- the role of communication campaigns in changing behavior, and
- how interventions can be designed to motivate appropriate CySec behavior.

Outcomes concluded that communications campaigns can help get messages out to fuel rational CySec behavior. However, additional activity must also include a) community programs, b) policy and law changes, c) available produces and services to support targeted behavior, d) tailored messages for specific audiences, and e) role models and champions who exhibit the desired (normative) behaviors.

Characteristics of chief executives (n=177) of small and medium-size enterprises (SMEs) are examined by Barlette et al. (2015) regarding infosec enterprise planning. PMT is adopted as a

basis for the model described by Barlette et al. as having two sub-components, an: a) threat appraisal and b) coping appraisal. Multiple regression is used to determine significant predictors of the DV which is composed of two dichotomous variables: a) intention and b) plan to introduce security measures in the near or medium future. Coping appraisal comprised the strongest predictive factor. Sub-elements were overall response efficacy (0.292, self-efficacy (0.189), and response cost (0.187). Threat appraisal, manifested by vulnerability concerns comprised the other significant factor (0.232).

PMT factors were augmented with a new construct by Boehmer, LaRose, Rifon, Alhabash, and Cotten (2015) -- *personal responsibility*. Two studies of college students (n =565 and n=206) explored determinants of protective behavior. The new variable explored additional variance beyond the core PMT factors. Two activities are described by the work: First, a multiple regression analysis relates PR to protective behaviors and addresses the effects of two previously noted variables from Barlette et al. (2015): TA and CA. Four independent variables produced a significant regression model to predict online safety behavior: *Software protection coping efficacy, software protection response efficacy, personal responsibility norm*, and *third party responsibility norm*. A subsequent intervention was devised to gauge the likelihood of taking protective CySec actions in light of *coping self-efficacy* and *safety involvement* variables. A 2x2x2 ANOVA was used (the intervention was the 3rd factor) to determine likelihood of taking action. Participants who perceived online safety to be their personal responsibility were significantly more likely to take protective measures when opportunities arose. Threat susceptibility and severity had no impact on the likelihood of participants taking protective measures against perceived threats.

A later work by Tsai et al. (2016) also explored personal responsibility as a protective motivational factor. A cross-sectional survey (N = 988) of Amazon Mechanical Turk (MTurk) users was conducted to examine how classical and new PMT factors predicted security intentions. The new factors included: prior experiences, subjective norms, habit strength, and perceived security support). The researchers noted a 15 percent increase in model explanatory power resulting from the added factors. Two of the added factors exhibited the strongest correlation with the DV: habit strength (end-user's habitual propensity to perform protective actions) and personal responsibility; moreover, those two new factors manifested stronger correlations with the DV than with each other.

Characteristics of three predictive models of protective behavior are analyzed and compared by Jansen and van Schaik (2017): RAA, PMT, and a combined model. Five sub-behaviors were used to characterize the DV, precautionary online behavior of 1200 online banking users in The Netherlands:

(1) keeping security codes secret,

(2) ensuring debit card are not shared,

(3) properly securing devices used for online banking,

(4) regularly checking bank account activity, and

(5) reporting security incidents directly to the financial institution.

Analysis compared the models using least squares path modelling. In a pure PMT model, response efficacy yielded the greatest weighting on precautionary behavior (0.49, which nearly tripled the weighting of perceived severity). User self-efficacy was significant as well, but of notably lower impact: 0.30. The RAA model found-user self-efficacy weighting close to that of the PMT model (0.27), with attitude having the greatest impact (0.36), followed by self-efficacy

(0.27). Locus of control, an element of social cognitive theory, carried the third highest weighting at 0.25. Weightings of a combined PMT/RAA model changed outcomes -- response efficacy had the heaviest weighting (neither the PMT or RAA model saw response efficacy weighted in the top three predictors), followed by attitude and self-efficacy. Outcomes infer operational utility with medium effect sizes. The article advocates ongoing study to compare RAA and PMT, and influence development of more predictive models for precautionary banking behavior.

Another hybrid model is described by White, Ekin, & Visinescu (2017): a combination of PMT and HBM factors as predictors of CySec incidents by users of home computers in the U.S. (n=945). Outcomes associated user awareness of the CySec problem domain associated with increases in CySec incidents. This outcome was not attributed to vulnerability as much to reporting based on increased user ability to recognize CySec incidents and report them, a phenomenon earlier reported by White (2015). Self-efficacy was determined to have the highest weighting of the least squares analysis factors in the 2017 work. However, outcomes are not shared regarding effect sizes; operational utility of the findings remains to be determined.

Technology Threat Avoidance

Chapter 1 of this study describes the initial extensions and refinements applied to PMT by Liang and Xue (2009) to formulate the TTAT. Multiple subsequent works further establish TTAT validity and expand the framework further to explore remaining unexplained variances in CySec threat avoidance. This section investigates findings and implications of recent TTAT-focused studies.

Hewitt, Dolezel, and McLeod surveyed 335 U.S. students in healthcare-related courses of study in 2017 to explore perceptions of healthcare learners regarding CySec threats, the effectiveness and cost of protective measures, self-efficacy, vulnerability, threat severity, and individual motivation/actual actions taken to secure their mobile devices. Findings were limited to descriptive statistics, but nevertheless fueled researcher concern – learners did not feel individually susceptible to CySec threats despite their perceptions of threat severity. Moreover, protective behaviors were largely understood by participants, but adoption behaviors were mixed --cost and barrier (an HBM concept) considerations were identified as the greatest hindrances to adoption.

Samhan (2017) explored TTAT factors in an operational healthcare context. Structural equation modelling produced models similar to those shared in Figures 7 and 8 by Workman et al. (2008) and Chen and Li (2017), accounting for 37 percent of variance in avoidance behavior. Consistent with other works, the control variables of participant age and education level were both found to significantly co-vary with threat avoidance behavior. Samhan noted effect sizes of significant interaction effects between factors in the small-to-medium range (susceptibility × severity and perceived threat × safeguard effectiveness), but not between IVs and the DV.

As IT end-users embrace greater mobility and cloud-based computing, concerns about data security and data privacy grow more significant (Broucek & Turner, 2013). Virtually all contemporary computers and mobile devices access back end systems hosted distributed computing environments (Burov, 2016). Studies that examine behaviors of IT end-users on mobile platforms warrant consideration, as CySec behaviors may differ between mobile platforms and relatively non-mobile workstations: Yeboah-Boateng and Amanor (2014) note a significantly greater phishing vulnerability for male users than female users on mobile

computing platforms (smart phones). This is opposite of differences noted by Sawyer et al. (2015) in general online environments.

In 2016, Das and Khan explored prospective differences among sub-platforms of 465 mobile device users (Android, iOS, and Blackberry systems) in the Middle East. Significant differences were noted between TTAT-based factors augmented with a trust variable where several protective actions comprised a behavioral DV (device locking, software updating, use of anti-virus, sensitive data encryption, avoidance of sensitive data on the device, and feature review before application installation). Differences were noted between all three platforms regarding perception of vulnerability (Android users felt most vulnerable and iOS users least vulnerable) and the security behavior DV: behavior rank/order by platform echoed vulnerability findings. Despite significant outcomes, intuitive inspection of findings did not appear to reveal notable effect sizes, and none are given in the work.

In 2017 Alsaleh, Alomar, and Alarifi executed a TTAT-based qualitative study of 30 smartphone users in Saudi Arabia who were over the age of 16 and who had six months or more of experience using their devices. Regarding impact of susceptibility and impact of CySec vulnerability, the researchers noted “the impact of perceived convenience of smartphone features and applications on smartphone users' actual behaviors might sometimes be higher than that of other predictors of behavior such as the perceived severity and perceived susceptibility of IT threats” (p. 15). Negative associations were also noted between the perceived cost of protective behavior (in terms of money, time and cognitive load) and the actual practice of protective behaviors. Lastly, device users were not observed to practice protective behavior based on their awareness of privacy concerns regarding mobile technology.

Chin, Etudo and Harris (2017) studied business student use of mobile devices in the U.S. regarding attitudes, behaviors, and security practices. Two groups were studied using convenience sampling techniques, grouped by a) those who received a mobile security training intervention (n = 187), and b) those who did not (n = 160). Protective behaviors were defined as an aggregate of three sub-behaviors types across a variety of ten activities. The sub-behaviors were:

1. avoidant activity to elude cyber threats,
2. use of add-on protective device features, and
3. use of built-in protective device features.

The training intervention consisted of video courseware addressing mobile security, social networking, password protection and data protection. Recipients were tested on relevant knowledge following the training delivery, although the article does not share testing outcomes. Outcomes did not adhere to hypothesized expectations: individuals who received the training intervention were more likely to eschew avoidant activity rather than embrace it, counter to hypothesized expectations. In addition, no differences were noted between groups regarding use of add-on protective features or built-in protective features. Abstractly, these findings align with the observations of Leuprecht et al. (2016) regarding avant garde-like behaviors of younger IT end-users. Findings echoed overall take-aways discussed by Hewitt et al. (2017) in young users of mobile devices. Chin et al. noted apparent apathy among college age students regarding their use of mobile technology; ongoing questions emanate from the study outcomes, among them are the possibility of undiscovered confounding factors, and the single shot nature of the training regimen; the latter contrasts with the iterative approach described by Bowen, Devarajan, & Stolfo (2012) which was used to alleviate vulnerability to email phishing-based threats.

Chen and Li proposed a TTAT-based research model in 2017 to explore motivating factors for end-user adoption of protective software on mobile devices. The researchers augmented the technology threat avoidance model, with a new variable termed *privacy security awareness*, and measured its impact on basic TTAT factors. A new factor was also added to the TTAT factors: *anticipated regret*. Figure 8 shows the resultant model and its least squares analysis results.

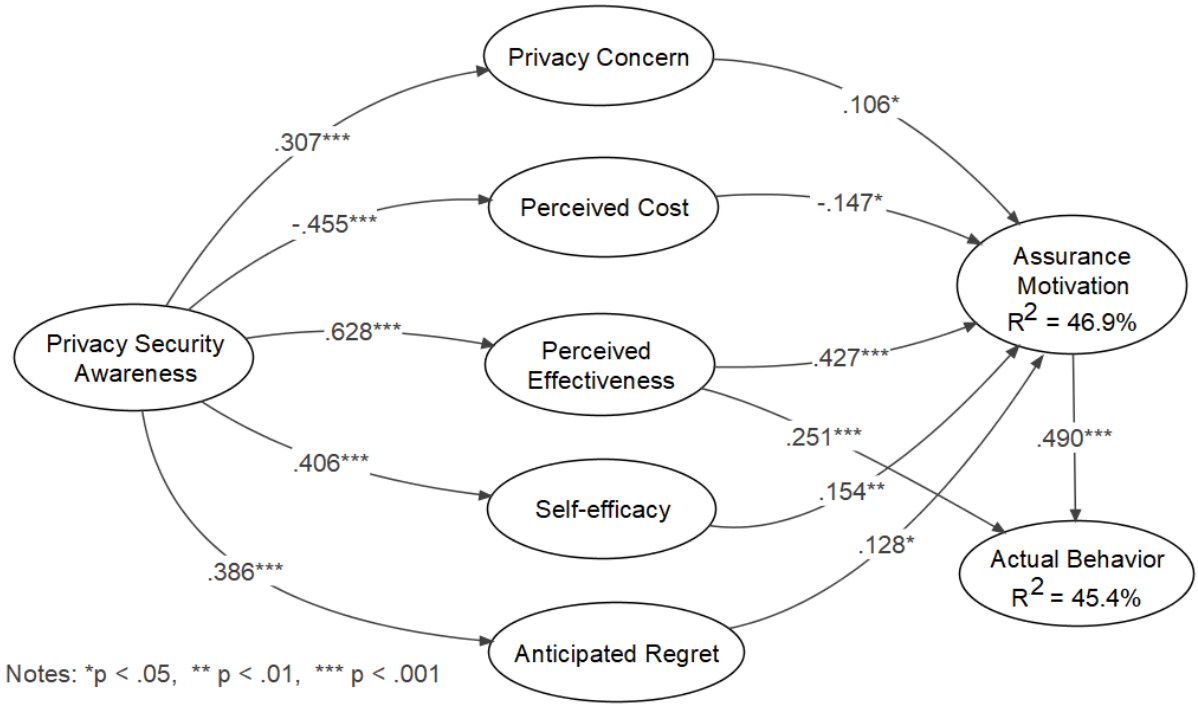


Figure 8. Augmented TTAT model and least squares weightings (Chen and Li, 2017, p. 338)

The overall explained variance differs notably from the objective measurement of omissive CySec behavior variances from the 2008 model by Workman et al. (34.7% -- see Figure 7). Differences may arise from two notable possibilities: a) actual behaviors in Chen and Li's 2017 work were self-reported, which may show greater similarity with Workman's subjective measurement than with the objective determination from the same work, and/or b) inherent

variances that differ between omissive behaviors investigated by Workman and its conceptual converse: the protective behaviors explored by Chen and Li. The latter possibility coincides with need for this research (exploring influences of TTAT factors on RScB).

Humans, CySec, and Risk

The 2008 study of PMT factors and omissive CySec behavior by Workman comprises a conceptual milestone for this research – no other works were noted that study associations between protective behavior (i.e., PMT factors) and known RScBs. Similarly, no works are yet noted that study associations between RScB and technology threat avoidance factors (see Figure 4) although the omissive behavior study by Workman et al. (2008) addresses concepts similar to TTAT and RScB. This paucity of similarly-focused literature may exist in part because literature items associated with RScB are also relatively new to the CySec landscape – more than 70% of the works in this category were written in 2017 or later.

Human aspects of information security. In 2013 a group of Australian CySec researchers introduced a new human factors research instrument: the *human aspects of information security questionnaire* (HAIS-Q). This inaugural HAIS-Q work was authored in pursuit of two objectives: 1) to conceptually develop and validate a CySec risk-based instrument for workplace behavior, and 2) examine the relationship between knowledge of policy and procedures, and attitudes towards policy, procedures and behavior when using organization IT assets. Applicability of the HAIS-Q towards this research derives from a) the work (HRD)-focused charter for HAIS-Q development, b) its characterization of the Infosec domain as a set of IT end-user activities (i.e., focus areas), and c) its ability to capture self-reported measurement of infosec risk-taking by IT end-users in the workplace.

In the first HAIS-Q focused literature work, Parsons et al. (2014) collected HAIS-Q results from 500 employed Australian citizens who used computers to perform their work. This initial study indicated that knowledge of policy and procedures more strongly affected individual policy and procedure-focused attitudes than they did actual CySec behavior in the workplace. This finding appears consistent with infosec-related observations by Hanus (2014) and Da Veiga (2016); both works noted medium to small effect sizes on the influence of infosec on actual behavior. Both implied infosec policy knowledge may not impact responsible CySec behavior to large degrees. This is because infosec policy-related attitude explained more of the variance in responsible infosec behavior than knowledge did. Parsons et al. (2013) explore implications of using self-reported CySec behavior as a study basis. The Australian team notes findings by Workman (2007) where self-reported behavior strongly correlated with objective behavioral measurements of responsible CySec practices regarding social engineering ($r = 0.89$, $p < .001$). Workman (2007) warns against wanton substitution of objective measures with subjective values, however -- 20% of the variance between subjective and objective measures in that work was unexplained. Parsons et al. (2013) list several considerations for collection of reliable self-reporting behavior measures, asserting participant bias will occur when any of four conditions are in effect:

1) if participants are violating the subject policy,

2) if participants are reporting on a highly sensitive construct,

3) if participants are predisposed to give socially desirable responses, or

4) if participants believe that responding truthfully could lead to punishment.

HAIS-Q refinement continued post-2013; the instrument itself was eventually shared in 2017, which was a prolific year for the Australian research cohort; four studies were published

that year relating to the HAIS-Q. McCormac, Calic, Butavicius, Parsons, Zwaans, and Pattinson shared findings regarding HAIS-Q test/retest reliability and internal consistency that year. The instrument was administered to 197 participants in two iterations. Earlier administrations of the instrument appeared susceptible to over-claiming by participants who might be inclined to answer in a socially acceptable manner (the 3rd item in the above list from Parsons et al., 2013). Three over-claiming items were included in the instrument. Those items included a knowledge question, an attitude question and a behavior-related question to identify participants who responded in a socially desirable manner. Analysis of the over-claiming items revealed test-retest reliability below Cronbach's α cutoff value of .70 (Cronbach, 1951); the alpha value was .66 for each item. Moreover, the internal consistency score between the three items also failed to meet the .70 cutoff (α = .55). Authors surmised this may have been due to the small number of over-claiming questions. Further refinement was deemed necessary for the HAIS-Q to solidify self-reported measurement of CySec behaviors.

A HAIS-Q hierarchical regression study was undertaken in 2017 by McCormac, Zwaans, Parsons, Calic, Butavicius, and Pattinson. The study intent was to examine relationships between individual infosec awareness and individual characteristics and attributes, including age, gender, personality and risk-taking propensity in 505 Australian participants (286 female, 219 male). The personality assessment used the widely accepted Big Five personality assessment scale, which measures neuroticism, extraversion, openness, agreeableness and conscientiousness -- Big Five factors were deemed applicable as predictors of infosec workplace compliance by Shropshire, Warkentin, Johnston, and Schmidt in 2006. Risk-taking was evaluated using the Risk Averseness scale, which measures inclinations to take risks in decision-making (Pan & Zinkhan, 2006). Participant age and gender were validated as significant control variables, and several elements

were found significantly associated with infosec awareness. Of greatest note for this study was an affiliation between risk taking propensity and infosec security awareness. However, this was not directly applied to the immediate study; the association was significant, but notably smaller than associations between the conscientiousness and agreeableness IVs and the infosec awareness DV.

Further HAIS-Q validation studies are described by Parsons et al. (2017). The article also shares the HAIS-Q instrument content. The two studies described by Parsons et al. (2017) included a) an administration to university undergraduate students (n = 122), which also involved an email phishing experiment, and b) a subsequent administration to working Australians as a general infosec awareness measure (n = 505). The first study noted participants who scored higher on the HAIS-Q were less susceptible to phishing emails. The second validated reliability and validity measures of the HAIS-Q as a measurement of infosec awareness, which also incorporated a factor analysis of 21 candidate factors (all confirmed). The 63 questions of the instrument cover an expanse of seven IT end-user activities (each of the focus areas is comprised of three factors). The over-claiming activity described in McCormac et al. (2017) appears to be robustly addressed in the structure of the 2017 instrument shared by Parsons et al.: questions pertaining to knowledge, attitude, and behavior are present in all seven focus areas, and internal consistency measurement values for focus areas exceeded the Cronbach reliability cutoff value of .70; values ranged from .75 to .82. The factor analyses and other activities described by Parsons et al. (2017) allow the authors to purport the validity of the HAIS-Q as a robust measure of infosec awareness based on user self-reporting.

The seven HAIS-Q focus areas are:

- password management,

- email use,
- internet use,
- social media use,
- mobile devices,
- information handling, and
- incident reporting.

A subsequent study by Pattinson, Butavicius, Parsons, McCormac, and Calic (2017) used a subset of the HAIS-Q to compare infosec awareness between employees of an Australian bank (n =198) and the general workforce (n=500). Infosec awareness levels as measured by the HAIS-Q were approximately 20 percent higher for bank employees, a significant difference; bank employees routinely received infosec training. However, repetitive administrations of the training did not indicate higher levels of infosec awareness for bank employees. The study further underlined the applicability of the HAIS-Q instrument to measure the effectiveness of training programs designed to increase employee infosec awareness. However, risk-taking behaviors were not addressed in the work, as the risk assessment HAIS-Q items (i.e., 21 questions across the seven focus areas pertaining to behavior) were not used for this study.

Intended security behaviors. Egelman and Peer (2015) note that despite an availability of instruments to evaluate infosec and protective behaviors in CySec arenas, few tools exist to evaluate general IT end-user security behaviors. The authors introduce and perform early validation of the *security intentions behavior scale* (SeBIS) to fill the need. The SeBIS is a 16-question CySec attitude-measurement instrument with four sub-scales that measure a) attitudes towards choosing passwords, b) device securement (i.e., locking devices using passwords, PINs, etc.), c) keeping software up-to-date, and d) proactive awareness of web content (i.e., noticing

and addressing environmental CySec cues). All questions are based on a five-level Likert scale ranging from never=1 to always=5. Instrument questions are shown in Figure 9. The article describes exploratory factor analysis (EFA) where axis rotation validated the four factors of the model. Data were furnished by surveying 354 crowd-sourced participants. To establish general content validity for the SeBIS model, instrument outcomes were compared with previously

Device Securement
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.
I use a password/passcode to unlock my laptop or tablet.
I manually lock my computer screen when I step away from it.
I use a PIN or passcode to unlock my mobile phone.
Password Generation
I do not change my passwords, unless I have to.^{r}
I use different passwords for different accounts that I have.
When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.
I do not include special characters in my password if it's not required.^{r}
Proactive Awareness
When someone sends me a link, I open it without first verifying where it goes.^{r}
I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.^{r}
I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).^{r}
When browsing websites, I mouseover links to see where they go, before clicking them.
If I discover a security problem, I continue what I was doing because I assume someone else will fix it.^{r}
Updating
When I'm prompted about a software update, I install it right away.
I try to make sure that the programs I use are up-to-date.
I verify that my anti-virus software has been regularly updating itself.

Figure 9. SeBIS instrument detail (Egelman and Peer, 2015, p. 2879)

published instruments via Pearson product-moment correlation. Password choosing, software updates, and proactive awareness behaviors showed highly significant correlations with the Domain-Specific Risk-Taking Scale (DoSpeRT), introduced by Blais and Weber in 2006 to assess risk-taking behaviors in five dimensions: 1) ethical, 2) financial, 3) health/safety, 4) recreational, and 5) social. However, despite high significance ($p < .001$), correlation values were low -- all significant relationships were accompanied by r-values less than 0.23. Similar outcomes applied to decision-making styles in the password choosing, software updates, and proactive awareness behaviors of the SeBIS when correlated with the general decision-making

style (GDMS) instrument values from Scott and Bruce (1995): all significant correlation values were such that $|r| < 0.25$. (The GDMS measures decision-making in light of rational, avoidant, dependent, intuitive and spontaneous factors). The low levels of correlation for both analyses weakly validate the SeBIS in regards to risk-taking and general decision-making.

A subsequent SeBIS research study by Egelman, Harbach, and Peer (2016) applied the SeBIS instrument to crowd-sourced participants in the U.S. to analyze instrument outcomes in light of CySec-related behavior. Table 2 summarizes specific activities and analysis outcomes. Effect sizes for significant differences using methods from Cohen (1992) showed operational utility in results via medium-to-large effect sizes for SeBIS instrument outcomes between subjects who demonstrated a CySec behavior specified for each SeBIS subscale and those who did not. The task associated with the SeBIS awareness subscale activity may not be a fully

Table 2.

SeBIS analysis of common CySec-related behaviors

SeBIS subscale	Analysis activity	Findings
Awareness	Use of a web browser URL status bar to identify a phishing website based on characteristics of the URL	3.1% of n=718 correctly identified the phishing website. (SeBIS M = 4.31 vs. 3.68, $t = 5.22$, $p < .0005$), large effect size

SeBIS subscale	Analysis activity	Findings
Passwords	Creation of passwords not easily cracked using a password cracking utility; password re-use	Crackable: SeBIS M = 3.21, uncrackable: SeBIS M = 3.56 (t = 3:47, p < 0.001), medium effect size. Subjects reporting password reuse also scored significantly lower on SeBIS: 2.94 vs. 3.46 (t = 6.94, p < .0005), medium-large effect size
Software updates	Prompt updating of software when updates are available	Users who installed updates within 3 weeks scored significantly higher than users who did not (24% of n=281, SeBIS M = 3.52 vs. 3.02, t = 4.11, p < .0001), medium effect size
Device securement	Employment of secured lock screens on smart phones	Users of secure unlock methods scored significantly higher than slide-to-unlock users (50.7% of n=71, W=169, p < .0005), large effect size

valid determinant of proactive awareness: only 3.1 percent of participants correctly identified a phishing website based on the attributes of URLs displayed in their web browser tool bar. More recent studies of human recognition of spoofed or phishing websites by Williams and Li (2018) and Kelley, Amon, and Bertenthal (2018) note higher levels of phishing URL detection across wide ranges of users – combinations of novice and experienced browser users exhibited more

than ten times the detection rate of Egelman et al. (2016). However, later studies also incorporate some degree of cognitive activity which includes inspection of web content that prompts for access credentials. Despite the inexact comparison, the contrast implies need for future evaluation of the SeBIS proactive awareness subscale to consider behavioral determinants with more balanced outcomes.

Risky CySec behavior. Recent studies have begun to investigate the impact of IT end-user attitudes and activities as predictors of risky CySec behavior. An early version of the RScB instrument by Hadlington (2017) was used by Hadlington and Murphy (2018) to measure associations between self-reported cognitive failure, media multi-tasking, and RScB. (Note: Direct exchanges with Lee Hadlington confirmed that the work described in 2018 by Hadlington and Murphy preceded the activity reported by Hadlington, 2017, despite the eventual year of publication of each item). MMT was considered as a possible antecedent of RScB due to earlier work by Murphy, McLauchlan, and Lee (2017**)** that investigated inhibitory response control and levels of MMT use by individuals. Hadlington and Murphy noted similar associations in their work. A one-way ANOVA post hoc analysis noted heavy media multi-taskers were associated with higher levels of self-reported CySec risky behavior -- RScB instrument scores were significantly higher for heavier multi-taskers than for light and medium multi-taskers ($n = 144$, $p <= .004$). The work does not report effect sizes for the differences. Some characteristics are shared for the early RScB instrument which included 11 factors; all answered using a 6-level Likert scale (0=never, 5=always). Items were found internally reliable (Cronbach's $\alpha = 0.73$). Content validity derived from a) partial derivation of risk-based elements from the SeBIS and b) consultation with law enforcement and digital forensic specialists.

RScB works following Hadlington and Murphy use a later version of the instrument, shown in Table 3. Hadlington (2017) evaluated RScB measures for use as a DV using IVs from three other instrument scales measuring: a) attitude towards cybercrime and CySec in business, b) impulsivity, and c) internet addiction. Hierarchical regression was used to perform the analysis on a sample of 538 participants in the U.K. Results showed

- internet addiction was a significant predictor of RScB,
- positive attitude towards CySec in business was negatively related to RScB, and
- both attentional and motor impulsivity significantly predicted RScB; non-planning was a significant negative predictor.

The significant findings did not appear to constitute large effect sizes for the CySec attitudinal and internet addiction behaviors – the aggregate effect of both instruments explained a total of 16% of the variance in RScB. Impulsivity explained an additional 9% of the RScB variance.

Table 3.

The RScB instrument (Hadlington, 2017, p. 7)

Item #	Item
1	Sharing passwords with friends and colleagues.
2	Using or creating passwords that are not very complicated (e.g. family name and date of birth).
3	Using the same password for multiple websites.

Item #	Item
4	Using online storage systems to exchange and keep personal or sensitive information.
5	Entering payment information on websites that have no clear security information/certification.
6	Using free-to-access public Wi-Fi.
7	Relying on a trusted friend or colleague to advise you on aspects of online-security.
8	Downloading free anti-virus software from an unknown source.
9	Disabling the anti-virus on my work computer so that I can download information from websites.
10	Bringing in my own USB to work in order to transfer data onto it.
11*	Checking that software for your smartphone/tablet/laptop/PC is up-to-date.
12	Downloading digital media (music, films, games) from unlicensed sources.
13	Sharing my current location on social media.
14	Accepting friend requests on social media because you recognise [*sic*] the photo.
15	Clicking on links contained in unsolicited emails from an unknown source.

Item #	Item
16	Sending personal information to strangers over the Internet.
17	Clicking on links contained in an email from a trusted friend or work colleague.
18*	Checking for updates to any anti-virus software you have installed.
19	Down loading data and material from websites on my work computer without checking its authenticity.
20	Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop).

* Indicates reverse scored items

The RScB implementation used by Hadlington (2017) exhibited higher internal consistency than its predecessor ($\alpha = 0.823$ for the later version). Descriptive statistics also appear to characterize an approximately normal distribution of data values for the later version ($M = 27.72$, $SD = 14.81$, $n = 515$). Mean RScB values did not appear to vary widely from the mean reported by Hadlington and Murphy using the previous version: ($M = 26.37$, $SD = 6.11$, $n = 144$), however, the first work sample exhibited a notably smaller standard deviation. It is unclear how the difference in SD values affected RScB distribution normality in the two studies. This research activity called for examination of sample normality to validate the appropriateness of using parametric methods to analyze the findings.

Hadlington considers the study limitations associated with self-reporting of CySec behavior, and reinforces concerns derived from contrasts between Workman (2008) and Chen

and Li (2017). Activity for this study strived to maximize the four conditions described by Parsons et al. (2013) to minimize response bias. Hadlington also poses a possible confounding attribute concerning RScB in work environments. Formal organizations generally have more IT assets dedicated to CySec support than do individuals who may be more apt to accept greater CySec risk at work: "As the individual believes they are more protected in the workplace they may be inclined to take more risks, circumvent accepted protocols and engage in poorer information security behaviours" (p. 13). The limitation was included for this research, as the study design does not address potential confounding effects arising from greater participant confidence in protective IT assets at work.

A replication study of Hadlington (2017) was undertaken by Aivazpour and Rao in San Antonio, Texas in 2018; the same instruments were applied to a sample of 245 crowd-sourced participants in the United States. The U.S. study findings largely paralleled those from the U.K.; no major differences emerged. However, the impulsivity measure explained a greater proportion of RScB variance in the U.S. study, more than 40%. In comparison, the original study saw less than 10% of the DV variance explained by the impulsivity measure.

RScB validity. In their conclusion, Aivazpour and Rao (2018) render a parting criticism of RScB validity; the researchers share intent to focus future study on refining the RScB measure, and characterize its current disposition as follows:

> Currently the risky cybersecurity behaviors scale appears to be a relevant, but random, collection of behaviors which introduce risk in disparate ways. For instance, using the same password for multiple accounts, and, disabling anti-virus software are both risky behaviors. However, they are not likely to be the result of the same causal variables, nor

> is it likely that they can be combated using the same techniques. We believe that the construct risky cybersecurity behaviors needs to root in theory. (p. 8).

A notable opportunity exists for researchers to reinforce RScB construct validity -- Factor analyses may discern underlying constructs of the RScB as the CySec discipline becomes more formally defined. The EFA applied to the RScB predecessor SeBIS by Egelman and Peer (2015) may serve as an example. However, Aivazpour and Rao (2018) appear almost brazenly dismissive, as several avenues do support arguments for RScB instrument validity. *Content* validity considers instrument coverage of the theoretical dimensions or content areas (Warner, 2008). The theoretical basis of CySec remains in flux with no all-encompassing theory; in this case, content validity can still be determined "by having expert judges decide whether the content coverage is complete" (Warner, 2008, p. 864). This was accomplished via baseline development of the instrument, which incorporated consultation with law enforcement and digital forensic specialists (Hadlington & Murphy, 2018). The RScB embodies *predictive* validity, which is established when instrument scores can predict group membership. This was the case for heavy media multi-taskers described by Hadlington and Murphy (2018). Similarly for Aivazpour and Rao (2018), who noted high correlation values between RScB and individuals exhibiting high levels of motor impulsivity ($r = 0.65$, $p < .01$), and individuals demonstrating internet-addictive behavior ($r = 0.61$, $p < .01$); the work also captured strong negative correlations between RScB and individuals with positive attitudes towards CySec in business ($r=-.70$, $p<.01$). Table 5 summarizes these considerations. Finally, this dissertation partially roots the RScB in theory via its operational definition despite complications posed by the multi-disciplinary nature of the CySec domain.

CHAPTER 3

METHODOLOGY

This one-shot quantitative study explored associations between a) motivational/decision-making factors of TTAT and b) IT end-user self-reporting of risky CySec workplace behavior by adults in the workplace (i.e., RScB). The following research questions motivate the study:

- To what extent do significant associations exist between TTAT factor values and RScB?
- To what extent can RScB instrument measures be categorized for descriptive classifications of RScB (e.g., to incorporate levels such as *low, medium* or *high*)?
- Which TTAT factors are the strongest and weakest predictors of RScB?
- To what extent do associations between TTAT factor values and RScB appear consistent with previously published associations between TTAT factor values and measurements of protective (i.e., non-harmful) behavior?
- To what extent do significant associations between TTAT factors on RScB demonstrate HRD business-level utility (i.e., differences in terms of statistical effect sizes)?

Population and Sample

The study criteria required all participants to be 18 years of age or older in the United States, with experience using IT assets in a professional capacity. Data were collected from participants via anonymous online questionnaires with secured access. Three participant samples were planned: 1) employees in a healthcare setting (a 328-bed acute care hospital in Austin, Texas); 2) non-industry-specific participants recruited via the Amazon mechanical turk (MTurk) framework, and 3) convenience sample participants contacted via snowball techniques.

The snowball convenience sampling technique consists of participant recruitment by word of mouth. The technique has utility in difficult-to-reach populations, and is described by Atkinson and Flint (2001). The study does not target populations generally considered difficult to reach, but the technique may have yielded larger participant counts than might have otherwise occurred. Any consequent increase in participants were deemed beneficial for the research findings. A common password was used by all participants.

The MTurk framework is leveraged by several referenced works; relevant works are by Aivazpour and Rao, 2018; Egelman and Peer, 2015; Egelman, et al., 2016; Mamonov and Benbunan-Fich, 2018, and Tsai et al., 2016. Specific foci of these works can be found in Appendix A. Use of the MTurk framework was later precluded for this research; ISU IRB requirements for exempt status require participant anonymity. This predicated that not only were responses to be non-traceable to respondents, but that identities of respondents remain unknown altogether. In contrast, MTurk participant compensation practices call for issuance of unique identifiers to participants upon survey completion. The identifiers are used to validate survey completion and manage compensation approval. This incompatibility led to preclusion of MTurk as a recruitment mechanism prior to the beginning of recruitment.

The sample target population of healthcare professionals consisted of 800 nursing professionals and patient care technicians at a single acute care facility in Texas. No more than 100 individuals were anticipated to participate from that population. Recruitment occurred via an email to nursing managers which requested their participation and snowball recruiting, subject to individual judgement. The text of that email appears in Appendix F. Content of the non-industry-specific recruitment email to support general snowballing activity appears in Appendix G. Both emails originated from the author's academic email account, hosted at Indiana State University. The questionnaire implementation included all informed consent criteria specified for internet research participants by the Indiana State University Institutional Review Board (2014, pp. 43-44). Appendix H shares the Institutional Review Board letter of exempt status notification for the study.

Generalizability. Generalization of findings derived from a sample to applicability to an overall population calls for two levels of reasoning (Bracht & Glass, 1968):

> 1) from the sample to the experimentally accessible population, and (2) from the accessible population to the target population. The first jump, a matter of inferential statistics, usually presents no problem if the experimenter has selected his sample randomly from the accessible population (p. 440).

For this study, such generalizability can only be precluded and not inferred, because convenience sampling was used. Consequently, this study does not embody external validity. Proportions of age and education levels were compared between the sample and the general US population to reach this conclusion.

It is important to note that lack of preclusion does not automatically infer generalizability, as the study instrument did not include variables that reflect regional, racial, socioeconomic, or

cultural demographic attributes. Moreover, the use of snowball recruitment may introduce additional complications within samples by involving individuals who work in the same area, groups of people with similar social, professional, or political interests, or individuals with special knowledge or skills who are compelled to contribute to the research.

Instrumentation

A Likert-style questionnaire of 68 study-specific questions was used to collect data for the study. Of the questions, 13 were general/demographic, and 20 related to the RScB DV. One of the RScB questions was asked predicated on an answer to its precedecessor. Of the 35 remaining questions, 31 related to the TTAT factors and four were input validation trap questions.

Questions which solicit input for TTAT factor values are derived from published works as shown in Table 4. The instrument and theoretical body have been subjected to numerous studies and validation activities described in the literature review section.

Table 4.

Derivation of instrument questions -- technology threat avoidance factors (IVs)

Factor	Source of Instrument Questions
Perceived Susceptibility	Tsai et al. (2016)
Perceived Severity	Tsai et al. (2016)
Perceived Threat	Liang & Xue (2010)

Factor	Source of Instrument Questions
Perceived Effectiveness	Tsai et al. (2016)
Perceived Cost	Liang & Xue (2010)
Self-Efficacy	Samhan (2017)
Avoidance Motivation	Liang & Xue (2010)
Avoidance Behavior	Liang & Xue (2010)

Questions derived from the RScB instrument by Hadlington (2017) were used to provide DV values. The RScB instrument was selected as it

- is relevant to CySec and HRD bodies of knowledge,
- has undergone iterative refinement through multiple peer-reviewed, published studies,
- illustrates RScB independently of infosec (unlike the HAIS-Q),
- exhibits content and predictive validity (see Table 5), and
- exhibits internal consistency with Cronbach α values of 0.823 from Hadlington (2017) and 0.73 from Hadlington and Murphy (2018).

Table 5.

RScB instrument validity summary

Supported validity type	Supported by	Comments
Content validity	Subject matter expert involvement in baseline development	Hadlington and Murphy (2018)
Predictive validity (all measures were collected as part of hierarchical regression analyses described by the cited items)	• Heavy media multi-tasking group membership $F(1,141) = 7.71$, $p = 0.001$ • Group members with high levels of motor impulsivity ($r = 0.65$, $p < .01$), $n = 245$ • Group members demonstrating internet-addictive behaviors ($r = 0.61$, $p < .01$) $n = 245$ • Group members with positive CySec attitudes in business ($r = -0.70$, $p < .01$) $n = 245$	• Hadlington and Murphy (2018) • Aivazpour and Rao (2018) • Aivazpour and Rao (2018) • Aivazpour and Rao (2018)

Sample validation via trap questions. Several trap questions augmented the questionnaire and were interspersed throughout its delivery. Their purpose was to identify participants who swept through the instrument without reflection. An incorrect answer to any trap question caused exclusion of a participant's input. The trap questions were:

1. Barack Obama was the first American president. Please select *strongly disagree*.
2. The United States of America consists of 10 states. Please select *strongly disagree*.

3. I am happy with receiving a very large bill from the IRS. Please select *strongly disagree*.
4. For quality assurance purposes please select *strongly agree*.

Trap questions 1-3 were used by Talebi (2018, p. 91). Trap question number 4 was retrieved from Guin, Baker, Mechling, & Ruyle (2012).

Other considerations regarding source instruments. The study instrument included several questions to collect demographic information to validate participation criteria and for potential use as control variables: In the event study variable values varied based on gender, age, education, or industry employment-related attributes, demographic data were planned for use as control variables to allow partial analysis of independent variables (PMT/TTAT factor values) on the RScB-based DV.

One question collected information regarding the size of the employer, based on employee headcount. This consideration was not noted in any of the cited works. However, the explorative nature of this research poses an opportunity to note associations between RScB levels and enterprise size. Business size categories were consistent with classes used by the US Bureau of Labor Statistics website (2018).

The research instrument is shown in Appendix E. One question appeared in both the TTAT and RScB source instruments: Question number 18 from Table 3 coincided with the second TTAT avoidance behavior question in Appendix B: both questions asked participants to describe their behavior in updating anti-virus software. The question was removed from the DV (RScB-based) questions in the combined instrument. One refinement was added to the study instrument to shed greater light on answers pertaining to use of public WiFi networks (relevant to question 6 of the RScB instrument in Table 3). Although free-to-use public WiFi network

access is an RScB attribute, VPN use is considered a self-protective behavior (Maimon, Becker, Patil, & Katz, 2017). For this study, self-reporting of VPN-related self-protective behavior was considered an acknowledgement of risk and a counterbalance to the pitfalls inherent with accessing free-to-use public WiFi. The DV portion of the study instrument encompassed a total of 19 items (plus the conditional VPN counterbalance question) for the DV, with an aggregate score range of 0–114. Finally, several typographical errors were noted in the original TTAT instrument in Appendix B. Those errors were corrected in the combined instrument.

Data Collection

Data were collected via online questionnaire hosted on the Qualtrics platform. Recruitment messaging occurred via email (individual contacts and listserv mailing lists) and social media (FaceBook and LinkedIn) postings. Data collection occurred over an 11-day period. Total participants numbered 294. A notable proportion of responses were excluded according to the dispositions shown in Table 6. The remaining entries (n = 184) were deemed valid and retained for further study.

Table 6.

Summary of excluded responses

Disposition	# of responses
Participants who used privately owned hardware as their primary work platform	46
Incomplete responses	11
Invalid responses to trap question(s)	53
Total number of exclusions	110

Design and Data Analysis

Analysis used ordinary least squares regression to evaluate TTAT factors as predictors of the DV (i.e., the RScB composite score) values. Effect sizes were determined where appropriate using techniques from Cohen (1992), Ferguson (2009), Kim (2017), and Warner (2008). Calculations were performed using IBM SPSS Statistics version 23. Figure 10 shares the conceptual model for the planned analysis.

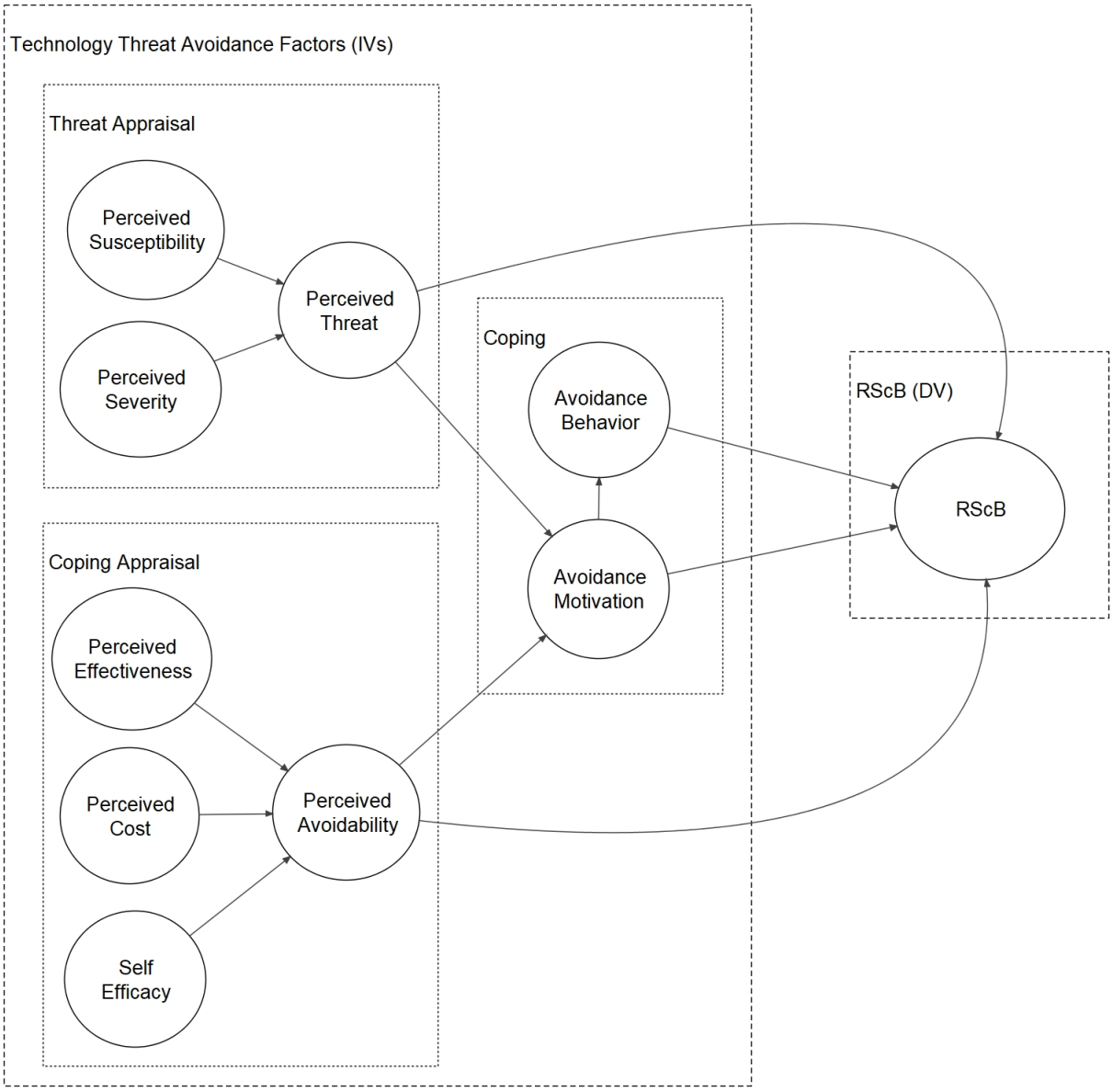


Figure 10. Conceptual model for analysis

The human behavior orientation of the study questions imply a Type I Error setting of $\alpha = .05$ for this research. Accordingly, a type II error setting $\beta = .20$ (statistical power of .80) accompanies the alpha. A sample size of at least 107 was needed to detect medium effect sizes (ES) in linear regression analysis, per Cohen (1992).

Analysis technique. Ordinary least squares regression (LSR) was selected to allow exploration of underlying relationships between TTAT factor values and the RScB DV. The technique appears widely accepted in social CySec research; LSR outcomes are shared by numerous works including Chen and Li (2017), Herath et al. (2014), Workman et al. (2008), Jansen and van Schaik (2017), and White, Ekin, and Visinescu (2017).

LSR has been identified as appropriate for explorative work in scenarios where the predictors are strongly correlated. Such collinearity frequently arises in social science research (Sawatsky, Clyde, and Meek, 2015); Some collinearity of findings was anticipated in this study due to the arrangements of factors and sub-factors intrinsic to the TTAT model (see Figure 10). Use of LSR appeared preferable to a competing technique, principal component progression (PCR), as use of PCR might have eliminated some predictors of RScB which may assert a large influence on the analysis model even if the eliminated components appear to exert a minor influence on the DV (Sawatsky et al., 2015). Use of LSR also appeared suitable for the study of values which were anticipated to comply with the underlying assumptions of LSR: predictor variables are continuous with continuous response variables (Sawatsky et al., 2015). Sawatsky et al. (2015) also describe data pre-processing to mitigate impact of collinear IVs -- values should be centered and scaled (i.e., converted to z-score equivalents by dividing the difference between each raw value and the variable mean by the value of the standard deviation) before analysis to ensure all variables have equal opportunity to impact the model.

Candidate confoundings. Age, gender, years of work experience, and formal levels of education were identified as possible confounding control variables in the event their values exhibited significant relationships with the RScB DV. Methods used to determine associations (parametric versus nonparametric methods) were determined after examining characteristics for

each variable (distribution and variable type). Distribution normality judgement used techniques from Ghasemi and Zahediasl (2012) and Kim (2013).

SPSS covariate classifications were planned during LSR to isolate factor effects from those of candidate control variables (age, gender, years of work experience, and formal levels of education) for any of the four variables confirmed as confounding factors. Three of the four variables (age, gender, education level) were noted as covariates of CySec-related attitudes and behaviors in the review of the literature. Years of work experience were included due to its intuitive association with the problem domain; no studies were reviewed which analyze and identify it as a non-covariate of targeted outcomes.

Descriptive categories of RScB. K-means cluster analysis was planned to use aggregate values of the RScB DV, ostensibly to classify IT end-user behaviors using common terms such as low, medium, and high. Descriptive terms were to be derived from the cluster analysis findings. The number of clusters was to be determined using the method introduced in 1974 by Caliński and Harabasz, which calls for maximizing the function shown in Figure 11 using test values for K.

$$CH(K) = \frac{\frac{B(K)}{(K-1)}}{\frac{W(K)}{N-K}}$$

Figure 11. Caliński-Harabasz index formula (from Reddy & Bhanukiran, 2014, p. 91)

In Figure 11,

- N represents the number of data points,
- B(K) is the between cluster sum of squares,

- W(K) is the within cluster sum of squares, and
- K is the number of clusters.

For the research, test values for K ranged from 2 thru 5. The range of candidate values for K was chosen in accordance with a desire for theoretical power and convenience in labeling RScB levels; theoretical power and convenience are higher when categories are fewer in number (Bryson & Phillips, 1975).

Study Timeline

A study schedule was developed to ensure requirements were addressed and study progress adhered to available time frames. Several milestones were planned to mark progress of the research. The timeline structure, activities and milestone dates are shown in Appendix C.

CHAPTER 4

RESULTS

Description of the Sample

After data were inspected to identify and remove invalid responses, retained records were examined to discern demographic insights and determine statistical techniques for further analysis. Pertinent variables are summarized in Table 7.

Table 7.

Sample demographics

Variable	Category	Frequency	Percentage
Gender	Female	105	57.10%
	Male	79	42.90%
Age	18-19 years	1	0.50%
	20-29 years	4	2.20%
	30-39 years	46	25.00%
	40-49 years	41	22.30%
	50-59 years	51	27.70%
	60-69 years	33	17.90%
	70-79 years	6	3.30%

Variable	Category	Frequency	Percentage
	80-89 years	2	1.10%
Level of Education	Less than high school	-	-
	High school graduate	1	0.50%
	Some college	13	7.10%
	2 year degree	8	4.30%
	4 year degree	46	25.00%
	Graduate or professional degree	63	34.20%
	Doctorate	53	28.80%
Enterprise size (# of employees)	1-4 employees	7	3.80%
	5-9 employees	4	2.20%
	10-19 employees	4	2.20%
	20-49 employees	4	2.20%
	50-99 employees	8	4.30%
	100-249 employees	10	5.40%
	250-499 employees	14	7.60%
	500-999 employees	19	10.30%
	1,000 or more employees	114	62%
Years of experience in industry	0-4 years	15	8.20%
	5-9 years	28	15.20%
	10-14 years	27	14.70%

Variable	Category	Frequency	Percentage
	15-19 years	21	11.40%
	20-24 years	27	14.70%
	25-29 years	27	14.70%
	30-34 years	15	8.20%
	35-39 years	13	7.10%
	40-44 years	10	5.40%
	45-49 years	1	0.50%
Industry	Technology products/services	24	13.00%
	Automotive	3	1.60%
	Healthcare	48	26.10%
	Legal	3	1.60%
	Hospitality	1	0.50%
	Retail	0	0%
	Education	69	37.50%
	Government	7	3.80%
	Military/Defense	1	0.50%
	Financial	7	3.80%
	Other	21	11.40%

Demographic variables. Interval-based age data used 10-year groupings. Age data were normally distributed ($M = 4.47$, $SD = 1.28$, $Z_{skew} = .89$, $Z_{kurtosis} = 1.14$, $n = 184$). Gender mix did not significantly differ between the sample and overall population ($\chi^2(1) = 2.89$, $p = .089$). Years

of work experience was not compared against national figures, as Department of Labor reports were limited to employee tenure at current place of employment and did not report industry-wide experience.

RScB variables. RScB aggregate values ranged from 2 to 62 (n = 184). Descriptive statistics conformed to a generally normal distribution: The mean value of 25.8 was accompanied by a standard deviation (SD) of 11.93. The distribution embodied a slight skew to the right, as the mean value exceeded the median value by 0.8.

CySec Behavior Outside of Work

Five questions were asked of participants regarding general online safety behavior away from work. Responses are depicted in Table 8.

Table 8.

General online precautions by participants when away from work

Precautionary activity	Yes (%)	No (%)	I don't know (%)
Do you use virus protection software on computers or mobile devices you own?	151 (83%)	21 (11.6%)	10 (5.5%)
Do you use internet firewall software on computers or mobile devices you own?	130 (71.4%)	31 (17%)	21 (11.5%)
Do you use virtual private networking (VPN) software on computers or mobile devices you own?	76 (41.8%)	83 (45.6%)	23 (12.6%)

Precautionary activity	Yes (%)	No (%)	I don't know (%)
Do you use encryption software to protect personal information on computers or mobile devices you own?	56 (30.8%)	94 (51.7%)	32 (17.6%)
Do you routinely remove web browsing information from computers or mobile devices you own?	105 (57.7%)	74 (40.7%)	3 (1.7%)

More than 89 percent of males reported use of virus protection, versus 76 percent of females. Proportions of users were compared between individuals who answered yes and those who answered other than yes to the antivirus use question. The difference was significant, and manifested a low-medium ES, evaluated as per Kim (2017): $\chi^2(1, N=184) = 5.74$, $p = .017$; Cramer's $V = .177$.

The mean age of virus protection software users also differed according to use. Significant differences were noted despite the use of ten-year age groupings (e.g., a mean age value of 2.x for some group would indicate a mean age of twenty-something, and so on). Anti-virus users ($M = 4.6$, $SD = 1.282$ $N = 151$) were significantly older than non-users ($M = 4.1$, $SD = 1.09$, $N = 21$). Both were older than individuals who did not know if they used virus protection software or not ($M = 3.3$, $SD = .823$, $N = 10$): $F(2, 179) = 6.17$, $p = .003$. The age group differences exhibited a small-to-moderate ES, determined using the ANOVA-specific technique by Cohen (1992). No gender or age differences were noted regarding browser cache/history flushing or the use of firewall, VPN, or encryption software.

Lastly, the outside-of-work behaviors were checked for relationships between behaviors. Chi squared tests of association revealed two significant relationships. Both exhibited large ES as per Kim (2017):

- Individuals who used virus protection software were more likely to use firewall protection software: $\chi^2(4,N=182) = 58.01$, $p < .001$ (Cramer's V = .383), and
- individuals who used virtual private networking software were more likely to use encryption software to protect their data: $\chi^2(4,N=182) = 68.25$, $p < .001$ (Cramer's V = .433).

Given the significant associations between age/gender and use of virus protection, evaluation of virus protection use on RScB was warranted. VPN use was also noted for further analysis of RScB impact due to strong association of VPN software use with virus protection. No plans were established other than to note relationships between outside-of-work behaviors and RScB if any were subsequently noted; neither variable was originally planned for study and both were identified by exploratory nature of the research.

RScB Component Validation

The 19 RScB question response values were checked for internal consistency via use of Cronbach's α. The initial value ($\alpha = .679$) failed to meet the .70 cutoff value specified by Cronbach (1951), and was notably lower than the α=.823 consistency measure noted by Hadlington (2017). Refinement was needed to obtain a DV with an acceptable level of internal consistency before the further analysis could take place.

Principal component analysis (PCA) was used to identify RScB items that weakly loaded onto RScB underlying factors. Any weakly aligned internal variables noted from the PCA were removed from the RScB aggregate calculation.

RScB Principal Component Analysis. The 19 RScB variables were submitted to a PCA using eigenvalue-based extraction and varimax rotation. Eigenvalue-based extraction was used, as scree plots and parallel analysis indicated use of a 2-factor extraction. However, those two factors explained about 27% of the variance in the model in the sum of squares loadings. In contrast, an eigenvalue-based extraction of seven factors explained almost 60% of the variance. The seven-factor extraction was used to better support decision-making.

Total loading of each RScB variable on the seven factors was calculated as the dot product of the component variable loadings and the corresponding percentage of variance explained by each component. Three variables (RScB7 – collegial advice, RScB8 – free virus protection downloads, and RScB11 – device updating) produced dot product values less than .06 and were excluded. The revised 16-item RScB instrument showed improved internal consistency (α = .707) RScB totals used for subsequent analysis excluded these variables. Henceforth, RScB values discussed by this research refer to the revised (16-item) construct with a potential score range of 0 – 96.

Adjusted RScB values distribution. Adjusted RScB DV values from the sample ranged from 0 to 56, exhibited a mean value of 21.1, a median value of 20.5, and were accompanied by a standard deviation of 11.46 (n = 184). RScB skewness and kurtosis statistics were examined as per Ghasemi and Zahediasl (2012) and Kim (2013) to assess distribution normality. RScB skewness and kurtosis values were divided by their respective standard error values to reveal corresponding z-scores. The mean and median values closely coincided. However, the Z_{skew} of

3.12 exceeded the upper limit of 2.58 from Kim (2013). The histogram was inspected against a superimposed normal curve (see Figure 12). Despite the Z_{skew} statistic value, adjusted RScB values appeared to largely conform to a Gaussian distribution. Determination called for reconciliation via Warner (2008, p.152): "In general, empirical distribution shapes are considered problematic only when they differ dramatically from normal." In the case of RScB values, no dramatic differences were noted between the shape of the histogram and the normal curve, so RScB values were deemed normally distributed.

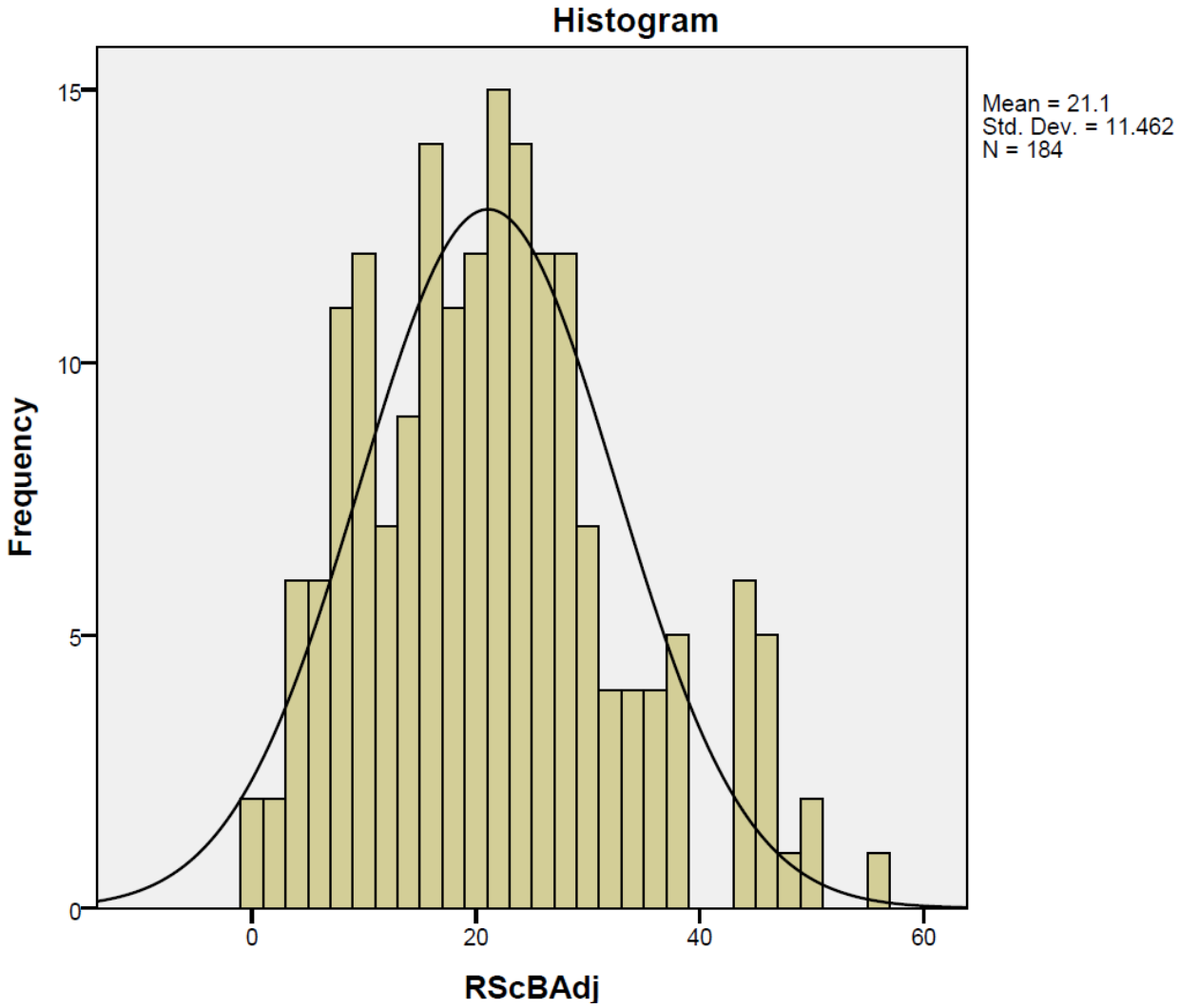


Figure 12. Distribution of adjusted RScB values

RScB Descriptive Categories

Planned activity called for four cases of k-means cluster analysis to investigate the optimal number of RScB descriptive categories (i.e., cluster counts). Candidate counts ranged from two to five. Cluster centers were initialized using the approach described by MacQueen (1967): random values were automatically selected at the outset of each instance. Final cluster centers were determined after all cluster assignments were complete. The RScB cluster assignments were then used to derive the Caliński-Harabasz index value for each cluster. Formula findings are shown in Table 9, which also shows cluster centroid values and the number of cluster elements for each instance.

Table 9.

Caliński-Harabasz index values and case counts -- K-means cluster analysis

K	CH(K)	Centroid 1 (# cases)	Centroid 2 (# cases)	Centroid 3 (# cases)	Centroid 4 (# cases)	Centroid 5 (# cases)
2	311.4	15 (121)	34 (63)	-	-	-
3	498.8	10 (69)	24 (87)	41 (28)	-	-
4	**606.19**	**8 (55)**	**20 (69)**	**30 (45)**	**46 (15)**	**-**
5	547.5	7 (42)	16 (50)	26 (67)	40 (21)	51 (4)

The greatest index value occurred in the case where K=4. The terms *averse* and *seeking* were applied to the upper and lower sub-ranges, consistent with the widely cited risk behavior piece by Weber, Blais, and Betz (2002). Terms were further expanded to describe a four-level scale. Clusters were examined further to determine lower and upper bounds of each descriptive sub-range (i.e., *RScB category*).

The entire range of RScB variable values was sub-divided into RScB categories according to cluster membership. In instances where clusters did not directly adjoin (i.e., members were separated by gaps), RScB category boundaries were determined using the formula:

$$\text{boundary} = \max(\text{cluster}[i]) + \frac{\min(\text{cluster}[i+1] - \max(\text{cluster}[i])}{2}$$

The range of each RScB category was derived from the sample data and is shown by Table 10.

Table 10.

Descriptive RScB categories

Descriptive RSCB category	Lower Bound	Upper Bound	Participant count	Percentage of participants
Strongly averse	0	14	55	29.9%
Averse	15	25	69	37.5%
Seeking	26	40	45	24.5%
Strongly seeking	41	56	15	8.2%

Validation of the category mapping. No formal tests were applied to validate the results of the k-means clustering. However, comparison of the Table 10 bounds between the *seeking* and *strongly seeking* RScB values coincided with the notable gap between values in the Figure 12 histogram. This informally confirmed that the categorization activity captured high level characteristics of the RScB data.

RScB Confounding Factors

Characteristics of candidate confounding variables (age, gender, years of work experience, and education level) determined the statistical techniques needed to evaluate their effects on the DV. Table 11 lists the technique used to analyze each IV.

Table 11.

Tests of association for candidate confounding factors

IV	IV Type/ distribution	DV	DV Type/ distribution	Test of association
Age	Interval/Normal	RScB	Interval/Normal	Pearson linear correlation
Gender	Dichotomous/ Uniform	RScB	Interval/Normal	Independent samples T-test
Work experience (years)	Interval/Poisson[a]	RScB	Interval/Normal	One-way ANOVA

IV	IV Type/ distribution	DV	DV Type/ distribution	Test of association
Education level	Ordinal/ undetermined (not normal, Poisson, uniform, or exponential)[a]	RScB	Interval/Normal	One-way ANOVA

[a]Determined using Kolmogorov-Smirnov tests augmented by visual inspection

Initial evaluation of candidate confounding variables. Tests of association listed in Table 11 determined a significant negative association between age and RScB ($r = -.120$, $p = .043$, $n = 184$). No other significant associations were noted between RScB and the remaining candidate confoundings.

Confounding variables re-visited. Associations were re-examined between candidate confounding factors (gender, experience, and education level) and RScB after introduction of the descriptive RScB category using the same tests from Table 11 to investigate the possibility that empirical effects might accompany the increased theoretical power of categorization described by Bryson and Phillips (1975). No additional significant associations were noted.

Behaviors away from work and RScB levels. Two outside-of-work CySec behaviors were also evaluated as predictors of RScB risk category level using discriminant analysis: a) use of virus protection and b) use of firewall protection. Neither behavior exhibited significant predictive impact on the categorical/ordinal DV. No further examination occurred regarding outside-of-work behaviors.

Summary of confounding factors. Age was the only confirmed confounding variable. Its effect on the DV demonstrated a small/medium level of effect, determined as per Cohen (1992).

RScB levels by Vertical Industry

Participant employment industries were captured for descriptive purposes. Research questions did not target industry-specific differences in RScB levels. Nevertheless, significant differences were noted in mean RScB levels when grouped by industry: $F(9,174) = 3.07$, $p = .002$. A Levene test showed variances were homogeneous across groups. RScB mean values by industry, sorted in descending order, are included in Table 12 for posterity.

Table 12.

RScB mean values by industry

Industry	RScB Mean	N	RScB SD
Automotive	32.67	3	16.50
Other	25.29	21	11.25
Financial	24.29	7	14.20
Education	23.67	69	9.84
Legal	21.00	3	5.29

Industry	RScB Mean	N	RScB SD
Technology products/services	18.71	24	11.91
Healthcare	17.79	48	11.68
Military/Defense	15.00	1	
Government	9.57	7	4.96
Hospitality	2.00	1	

Technology Threat Avoidance Factor Validation

Several steps were used to evaluate the TTAT factors prior to formal analysis. TTAT response values were first checked for internal consistency. All eight variable sets (i.e., components) exhibited acceptable levels of internal consistency (Cronbach's $\alpha > .70$). However, further validation seemed prudent, as factor questions originated from multiple sources (see Table 4). An incremental step was taken to ensure components (i.e., question variables) of the synthesized hybrid instrument not only exhibited internal consistency, but also loaded strongly onto their intended factors.

TTAT principal component validation. PCA was performed on the TTAT response variables to evaluate TTAT factor loading. Of the 31 TTAT response variables, 26 exhibited loading weights of .6 or greater onto their primary factors (see Figure 13). The avoidance motivation and avoidance behavior questions strongly loaded onto the same factor, as did

perceived cost. Cost questions reflected negative loading weights which appeared consistent with earlier TTAT studies, cost having an expected negative association with avoidance motivation and avoidance behavior. This did not raise immediate concern, aside from avoidance motivation question number 2 (which captured predicted use of protective CySec measures if they are available -- responses for that question loaded more strongly onto *perceived effects* than they did the intended factor).

Two factors exhibited notably more aberrant loadings than the remaining factors. Four items (*perceived severity* questions 2 and 3, and *perceived threat* questions 4 and 5) loaded less strongly onto their primary factor than unidentified 7th and 8th factors, respectively. Those four items were:

- Perceived severity Q2 from Tsai et al. (2016): malware causing a work computer to run more slowly,
- perceived severity Q3 from Tsai et al. (2016): malware causing a work computer to crash from time to time,
- perceived threat Q4 from Liang and Xue (2010): level of dread regarding a malware-infected work computer, and
- perceived threat Q5 from Liang and Xue (2010): level of risk associated with using a work computer that contains malware.

Rotated Component Matrix[a]

	Component							
	1	2	3	4	5	6	7	8
Perceived Susc Q1	.016	**.861**	-.078	-.031	-.013	.166	-.022	-.025
Perceived Susc Q2	-.047	**.872**	-.059	-.082	.048	.179	-.112	-.063
Perceived Susc Q3	-.180	**.799**	-.085	-.048	.019	.080	.063	-.156
Perceived Susc Q4	-.036	**.918**	-.027	-.030	.006	.133	-.006	-.064
Perceived Sev Q1	-.030	.005	-.138	**.715**	.059	-.047	.194	.149
Perceived Sev Q2	.079	-.028	-.021	.344	.044	-.037	.788	.249
Perceived Sev Q3	.081	-.040	-.168	.373	.051	.033	.823	.033
Perceived Sev Q4	-.043	-.098	-.001	**.663**	.035	.167	.240	-.013
Perceived Sev Q5	-.020	-.057	-.080	**.695**	-.009	.004	.282	-.018
Perceived Sev Q6	.090	.003	-.022	**.800**	.078	-.054	-.098	.181
Perceived Sev Q7	.013	-.037	-.029	**.767**	-.006	.063	.031	.081
Perceived Threat Q1	-.071	.127	.021	.036	.179	**.879**	-.013	.044
Perceived Threat Q2	-.113	.160	-.011	.071	.036	**.916**	.091	.053
Perceived Threat Q3	-.002	.326	-.039	.016	.091	**.819**	-.078	.079
Perceived Threat Q4	.047	-.180	-.093	.270	.081	.177	.247	.710
Perceived Threat Q5	-.011	-.180	.123	.206	.288	.041	.050	.745
Perceived Effect Q1	.119	-.026	.055	.084	**.758**	.110	.023	.074
Perceived Effect Q2	-.016	-.013	.028	.006	**.808**	.158	.140	-.016
Perceived Effect Q3	.056	.082	.063	-.010	**.791**	.052	.022	.210
Perceived Cost Q1	**-.693**	.207	-.328	.044	.219	.071	-.045	-.100
Perceived Cost Q2	**-.767**	.034	-.204	-.068	.023	.106	.055	.043
Perceived Cost Q3	**-.721**	.176	-.236	.047	.141	-.092	.048	-.244
Self-Efficacy Q1	.271	.056	**.838**	-.130	.015	-.034	.054	.143
Self-Efficacy Q2	.215	-.046	**.889**	-.089	-.016	-.054	.010	.070
Self-Efficacy Q3	.127	-.146	**.853**	-.093	.070	.038	-.112	-.057
Self-Efficacy Q4	.079	-.106	**.876**	.021	.086	.018	-.125	-.094
Avoidance Motiv Q1	**.653**	-.027	-.072	.021	.563	.008	-.014	-.019
Avoidance Motiv Q2	.414	.050	-.001	.064	.644	-.044	-.166	.063
Avoidance Motiv Q3	**.768**	.028	-.017	.155	.375	-.014	.037	-.150
Avoidance Behav Q1	**.798**	.009	.158	-.060	.219	-.036	.127	-.003
Avoidance Behav Q2	**.809**	-.014	.079	-.048	.217	-.088	.087	-.009

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 7 iterations.

Figure 13. Confirmatory TTAT component loading (initial)

Efforts to reconcile similarities/ differences between the four questions were not productive -- the items did not appear to differ markedly from other questions within their respective factors. Internal consistency measures of the TTAT factors reinforced this reasoning.

To avoid the need to introduce and formalize a new TTAT factor to embrace the four items in question, an additional CFA with varimax rotation was performed. The additional CFA excluded the four variables bulleted above. The exclusions forced loadings cleanly onto eight factors (including the previously mis-loaded avoidance motivation question number 2). The resultant load matrix is shown in Figure 14. The revised, more highly partitioned model strengthened prospects for subsequent analysis findings, as:

- inconsistent loading for the perceived severity and perceived threat factor components no longer occurred,
- the perceived cost components loaded cleanly onto a separate factor, and
- the avoidance motivation and avoidance behavior factor components also loaded strongly onto separate factors.

Internal consistency values were re-calculated for all sets of factor variables and are reflected in Table 13.

Rotated Component Matrix[a]

	Component							
	1	2	3	4	5	6	7	8
Perceived Susc Q1	-.067	**.857**	-.034	.170	.037	-.028	.048	.031
Perceived Susc Q2	-.045	**.878**	-.104	.180	.069	.010	-.058	.093
Perceived Susc Q3	-.098	**.810**	-.048	.071	.166	.027	-.045	-.080
Perceived Susc Q4	-.034	**.923**	-.030	.129	.031	.028	.004	-.033
Perceived Sev Q1	-.162	-.001	**.759**	-.049	-.053	.138	-.055	-.058
Perceived Sev Q4	.010	-.092	**.697**	.155	.120	-.030	.039	.043
Perceived Sev Q5	-.096	-.046	**.735**	-.002	-.057	-.042	-.188	.140
Perceived Sev Q6	-.001	-.013	**.773**	-.037	-.039	.051	.027	.113
Perceived Sev Q7	-.039	-.051	**.766**	.070	.035	.048	.178	-.170
Perceived Threat Q1	.034	.116	.034	**.889**	.097	.140	-.025	.066
Perceived Threat Q2	-.023	.152	.091	**.922**	.057	.063	-.046	-.081
Perceived Threat Q3	-.040	.324	.007	**.821**	-.026	.108	-.016	.009
Perceived Effect Q1	.049	-.024	.090	.103	-.060	**.761**	.038	.261
Perceived Effect Q2	.001	.002	.035	.136	.026	**.839**	-.007	.166
Perceived Effect Q3	.055	.059	.030	.057	.044	**.859**	.193	.069
Perceived Cost Q1	-.280	.182	.022	.101	**.805**	.079	-.177	-.051
Perceived Cost Q2	-.168	-.004	-.043	.142	**.775**	-.042	-.233	-.225
Perceived Cost Q3	-.199	.167	.024	-.076	**.815**	-.012	-.210	-.072
Self-Efficacy Q1	**.842**	.031	-.095	-.016	-.222	.035	.169	.013
Self-Efficacy Q2	**.889**	-.056	-.065	-.051	-.208	.017	.108	-.027
Self-Efficacy Q3	**.858**	-.130	-.126	.029	-.148	.033	-.052	.102
Self-Efficacy Q4	**.889**	-.092	-.013	.008	-.027	.036	.057	.029
Avoidance Motiv Q1	-.010	-.039	.007	.019	-.258	.334	.350	**.717**
Avoidance Motiv Q2	.088	.027	.023	-.012	-.049	.349	.126	**.811**
Avoidance Motiv Q3	.049	.020	.134	-.009	-.261	.112	.553	**.656**
Avoidance Behav Q1	.189	-.020	-.022	-.028	-.316	.129	**.834**	.226
Avoidance Behav Q2	.112	-.038	-.019	-.083	-.334	.120	**.808**	.259

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 8 iterations.

Figure 14. Confirmatory TTAT component loading (revised)

Table 13.

Internal consistency of TTAT factors

TTAT Factor	Number of variables	Cronbach's α
Perceived Susceptibility	4	.91
Perceived Severity	5	.78
Perceived Threat	3	.90
Perceived Effectiveness	3	.82
Perceived Cost	3	.85
Self-Efficacy	4	.91
Avoidance Motivation	3	.85
Avoidance Behavior	2	.93

TTAT factor validation. The TTAT core theory incorporates one latent factor (LF) within each appraisal domain (see Figures 2 and 9): *perceived threat* resides in the threat appraisal domain and *perceived avoidability* resides within the coping appraisal domain. The perceived threat latent factor was comprised of an independent set of question responses. No instrument question responses directly populated the perceived avoidability factor. The planned

research called for perceived avoidability to be constructed from the weighted means of the three coping appraisal IVs: a) perceived effectiveness, b) perceived cost, and c) self-efficacy.

Threat appraisal factor evaluation. Correlational analysis was performed between the threat appraisal independent factors (IFs) and the perceived threat LF in the conceptual model. Correlation values are shown in Table 14.

Table 14.

Threat appraisal factor correlation values

		Perceived Susceptibility	Perceived Severity	Perceived Threat
Perceived Susceptibility	Pearson correlation	1		
	Sig. (2-tailed)			
	N	184		
Perceived Severity	Pearson correlation	-.088	1	
	Sig. (2-tailed)	.233		
	N	184	184	
Perceived Threat	Pearson correlation	.374**	.066	1
	Sig. (2-tailed)	.000	.376	
	N	184	184	184

** Correlation significant at the 0.01 level (2-tailed)

Correlation analysis revealed a) no significant correlation between the IFs and b) a weak association between the perceived susceptibility IF and the perceived threat LF. Cognitively and as per TTAT, the IFs appeared related and strongly poised to load to a common factor, but correlational findings indicated otherwise. A cursory run of CFA took place using varimax rotation to force the two IFs onto a single factor to evaluate the factor loading. The CFA showed the IFs explained 54% of the LF variance.

Coping appraisal factor evaluation. The correlation and CFA activities were repeated for the coping appraisal IFs. Regression outcomes are shown in Table 15.

Table 15.

Coping appraisal factor correlation values

		Perceived Effectiveness	Perceived Cost	Self-Efficacy	Perceived Avoidance
Perceived Effectiveness	Pearson correlation	1			
	Sig. (2-tailed)				
	N	183			
Perceived Cost	Pearson correlation	-.055	1		
	Sig. (2-tailed)	.463			
	N	183	184		
Self-efficacy	Pearson correlation	.073	-.428**	1	
	Sig. (2-tailed)	.348	.000		
	N	169	170	170	
Perceived Avoidance	Pearson correlation	.439**	-.225**	.909**	1
	Sig. (2-tailed)	.000	.003	.000	
	N	169	169	169	169

** Correlation significant at the 0.01 level (2-tailed)

Correlation findings for coping appraisal appeared more promising than for threat appraisal, as all three IFs were significantly associated with the LF. However, none of the associations were strong ($r > .6$) and the perceived cost was inversely related to the other IFs. To further evaluate possible weaknesses, the cost variable was re-depicted as 'negative cost' with its sign reversed, and CFA with varimax rotation was used again to force the three IFs onto a single factor. Weakness was again confirmed: a cumulative variance of 48.1% occurred from the factor loading. The loss of more than half of the information from the IFs again motivated consideration of excluding the relevant LF (perceived avoidance) from the regression model.

TTAT factor refinement. Weak loadings of the threat and coping appraisal IFs onto their LFs (perceived threat and perceived avoidance, respectively) fueled reflection regarding the structure of the regression model. The work by Liang and Xue (2010) helped reconcile insights.

The 2010 work shared no concerns coincided with the consistency issues noted in the local data. However, Liang and Xue discussed nuances of mediated relationships between variables and matters of researcher preference for mediated versus direct relationships in research models. Empirical concerns ultimately outweighed design nuances in the local case for both the coping and avoidance appraisal domains – the perceived threat and perceived avoidance LFs were removed. This change partially mirrors considerations by Young et al. (2016), who excluded the coping appraisal LF. Young et al. (2016) also failed to note significant relationships between the threat appraisal IFs and the perceived threat LF. However, the model was left unperturbed in that research, which was a replication study of the original work by Liang and Xue (2010).

Later research by Jansen and Van Schaik (2017) excluded use of both the perceived threat and perceived avoidance LFs in studies of precautionary online behavior. Identical refinements were used in the local study after the correlational and CFA findings were noted. Figure 15 shows the revised conceptual model.

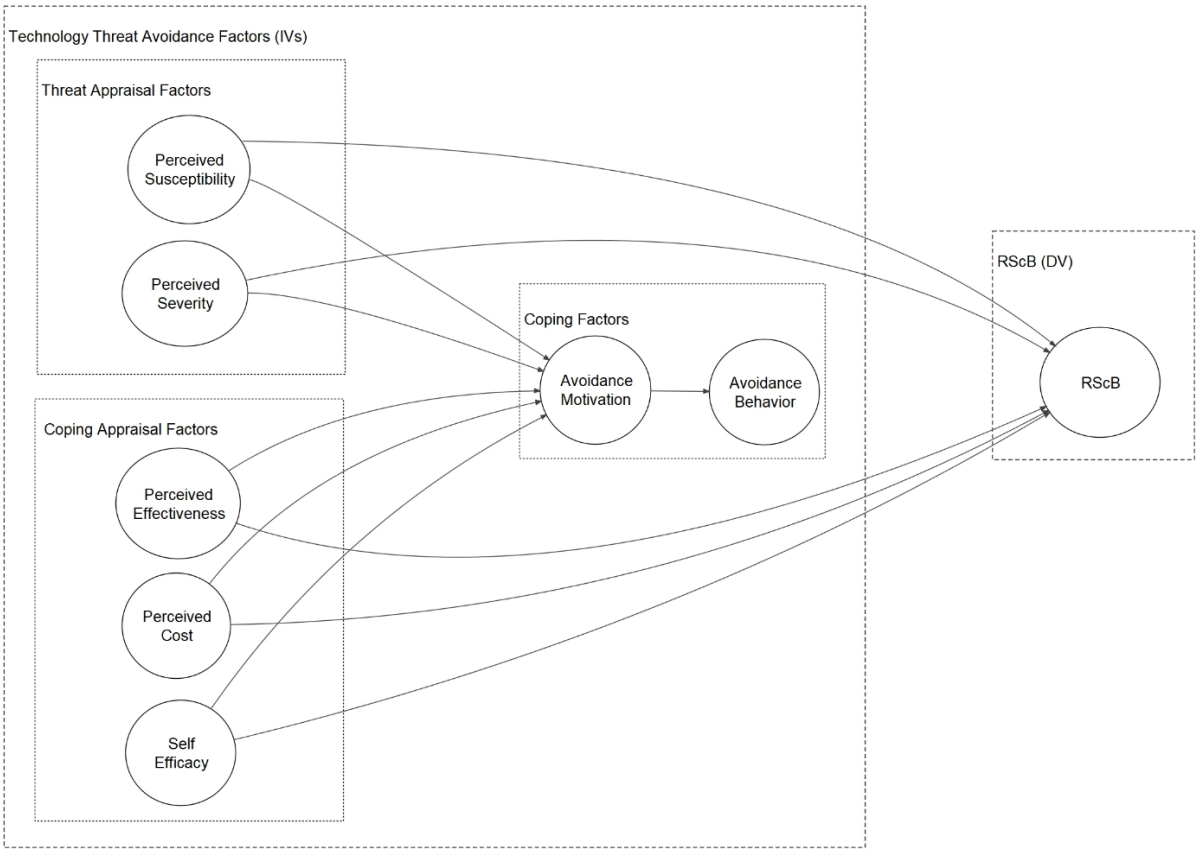


Figure 15. Conceptual model after correlational and factor analyses

Regression Findings: TTAT versus RScB

Regression analysis was applied to the IVs and DVs to determine which variables were significantly predictive. Three separate regression analyses were used: 1) between TTAT IVs and avoidance motivation, 2) between avoidance motivation and avoidance behavior, and 3) between TTAT IVs and RScB. Conservative methods were used to determine the impact of the IVs on the DV:

- All calculations were performed using two steps to isolate the IV impacts from age-related impacts,
- all explained variances were determined using the adjusted variances, and

- all coefficient values were standardized.

To maximize findings, missing values were excluded on a pair-wise basis to fully utilize participant responses -- response tuples were retained if isolated values were missing. However, individual responses were excluded from specific calculations if those responses did not contain a value for a calculation variable. This was in contrast to the list-wise deletion, which completely excludes participant responses where any values are missing.

All IVs consisted of standardized values (i.e., variable Z-scores) and were processed using the enter method. Bonferroni correction was applied to the statistical alpha to determine a revised significance indicator: (.05/3) = .017. All three regression models were significant with p-values ≤ .001. Constant terms were included in the regression calculations, which produced a standardized coefficient close to zero for the constant term in each of the three models (p = 1.0). Outcomes of the combined models are shared in Figure 16 and are presented using the structure of the research conceptual model.

Impact of independent variables on avoidance motivation. The first phase of examining the three-phase model called for examining relationships between the TTAT IVs and avoidance motivation. Related findings are shared in Table 16, Table 17, and Table 18.

Table 16.

Avoidance motivation DV SPSS regression command

SPSS Command
REGRESSION /MISSING PAIRWISE /STATISTICS COEFF OUTS R ANOVA CHANGE /CRITERIA=PIN(.05) POUT(.10) /NOORIGIN /DEPENDENT ZFctrAvoidMot /METHOD=ENTER ZageGrpNum /METHOD=ENTER ZFctrPrcvdSusc ZfctrPrcvdSev ZfctrPrcvdEffctv ZFctrPrcvdCost ZFctrSelfEffic.

Table 17.

Avoidance motivation DV regression model summary

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate	Change Statistics				
					R^2 Change	F Change	df1	df2	Sig. F Change
1	.148[a]	.022	.016	.99198	.022	3.726	1	167	.055
2	.641[b]	.411	.389	.78180	.389	21.374	5	162	.000

a. Predictors: (Constant), z-score of age group
b. Predictors: (Constant), z-score of age group, z-score of perceived cost, z-score of perceived severity, z-score of perceived effectiveness, z-score of perceived susceptibility, z-score of self-efficacy

Table 18.

Avoidance motivation DV regression coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig
		B	Std. Error	Beta		
1	(Constant)	1.342E-15	.076		.000	1.000
	Z-score of Age Group	.148	.077	.148	1.930	.055
2	(Constant)	2.229E-16	.060		.000	1.000
	Z-score of Age Group	.048	.063	.048	.768	.444
	Z-score of Perceived Susceptibility	.061	.063	.061	.963	.337
	Z-score of Perceived Severity	.052	.062	.052	.839	.403
	Z-score of Perceived Effectiveness	.462	.062	.462	7.451	.000
	Z-score of Perceived Cost	-.427	.069	-.427	-6.156	.000
	Z-score of self-efficacy	-.046	.069	-.046	-.669	.504

Dependent variable: z-score of avoidance motivation

Impact of avoidance motivation on avoidance behavior. The second phase of the three-phase model examined relationships between the avoidance motivation and avoidance behavior. Related findings are shared in Table 19, Table 20, and Table 21.

Table 19.

Avoidance behavior DV SPSS regression command

SPSS Command
REGRESSION /MISSING PAIRWISE /STATISTICS COEFF OUTS R ANOVA CHANGE /CRITERIA=PIN(.05) POUT(.10) /NOORIGIN /DEPENDENT ZFctrAvoidBeh /METHOD=ENTER ZageGrpNum /METHOD=ENTER ZFctrAvoidMot.

Table 20.

Avoidance behavior DV regression model summary

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate	Change Statistics				
					R^2 Change	F Change	df1	df2	Sig. F Change
1	.193[a]	.037	.032	.98397	.037	6.978	1	181	.009
2	.613[b]	.375	.368	.79479	.338	97.422	1	180	.000

a. Predictors: (Constant), z-score of age group
b. Predictors: (Constant), z-score of age group, z-score of perceived cost, z-score of perceived severity, z-score of perceived effectiveness, z-score of perceived susceptibility, z-score of self-efficacy

Table 21.

Avoidance behavior DV regression coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig
		B	Std. Error	Beta		
1	(Constant)	-5.805E-17	.073		.000	1.000
	Z-score of Age Group	.193	.073	.193	2.642	.009
2	(Constant)	-8.471E-16	.059		.000	1.000
	Z-score of Age Group	.106	.060	.106	1.776	.077
	Z-score of Avoidance Motivation	.588	.060	.588	9.870	.000

Dependent variable: z-score of avoidance behavior

Impact of the independent variables on RScB. The third phase of examining the three-phase model examined relationships between the TTAT IVs and RScB. Related findings are shared in Table 22, Table 23, and Table 24.

Table 22.

RScB DV SPSS regression command

SPSS Command
REGRESSION /MISSING PAIRWISE /STATISTICS COEFF OUTS R ANOVA CHANGE /CRITERIA=PIN(.05) POUT(.10) /NOORIGIN /DEPENDENT ZRScBAdj /METHOD=ENTER ZageGrpNum /METHOD=ENTER ZFctrPrcvdSusc ZfctrPrcvdSev ZfctrPrcvdEffctv ZFctrPrcvdCost ZFctrSelfEffic.

Table 23.

RScB DV regression model summary

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate	Change Statistics				
					R^2 Change	F Change	df1	df2	Sig. F Change
1	.150[a]	.022	.017	.99171	.022	3.819	1	167	.052
2	.378[b]	.143	.111	.94272	.121	4.562	5	162	.001

a. Predictors: (Constant), z-score of Age group
b. Predictors: (Constant), z-score of Age group, z-score of perceived cost, z-score of perceived severity, z-score of perceived effectiveness, z-score of perceived susceptibility, z-score of self-efficacy

Table 24.

RScB DV regression coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig
		B	Std. Error	Beta		
1	(Constant)	-7.196E-17	.076		.000	1.000
	Z-score of Age Group	-.150	.077	-.150	-1.954	.052
2	(Constant)	-4.469E-16	.073		.000	1.000
	Z-score of Age Group	-.152	.075	-.152	-2.017	.045
	Z-score of Perceived Susceptibility	.171	.076	.171	2.231	.027
	Z-score of Perceived Severity	-.084	.075	-.084	-1.114	.267
	Z-score of Perceived Effectiveness	.088	.075	.088	1.172	.243
	Z-score of Perceived Cost	.253	.084	.253	3.028	.003
	Z-score of self-efficacy	.170	.083	.170	2.038	.043

Dependent variable: Z-score of adjusted RScB (16 items)

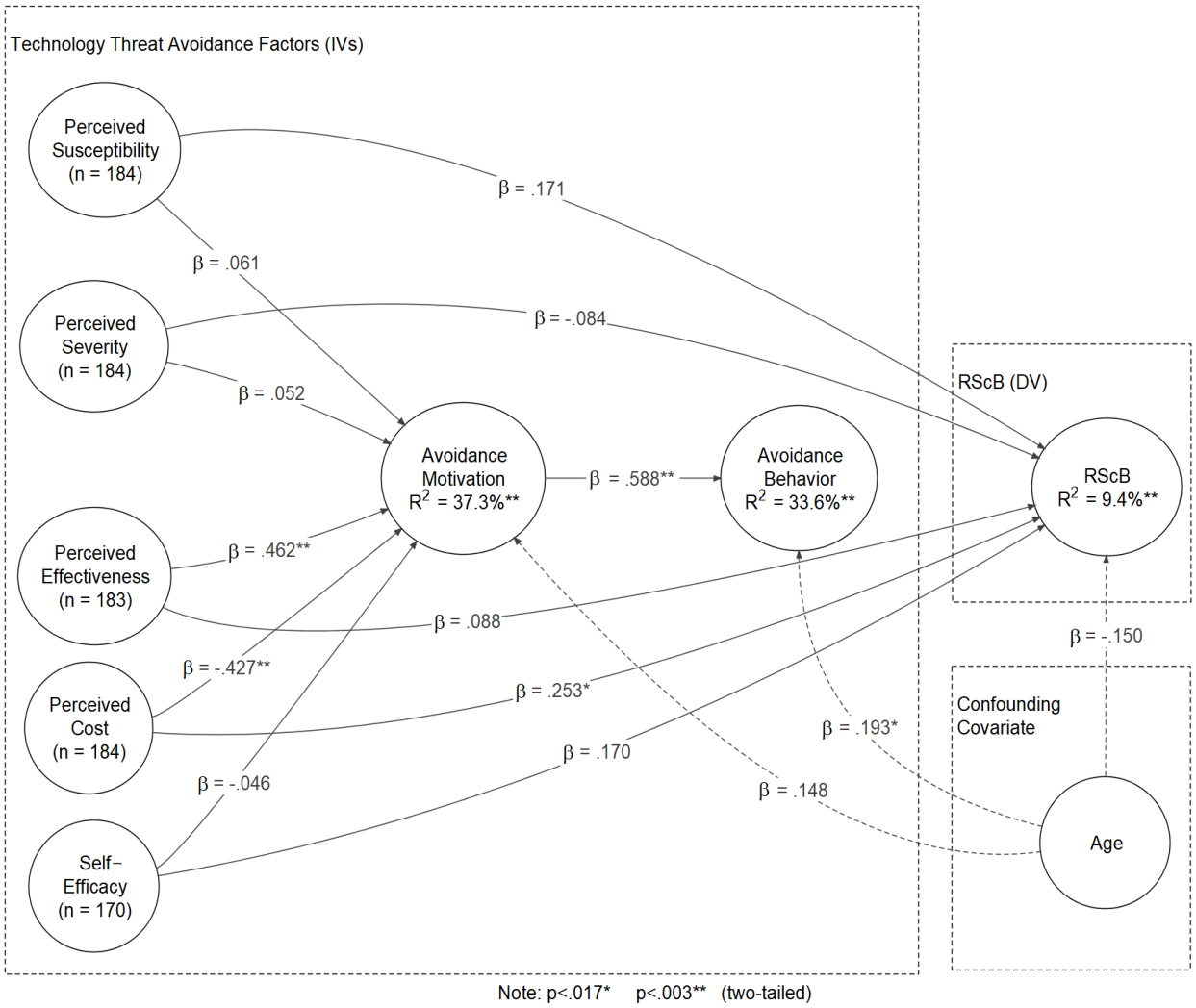


Figure 16. Overall regression findings

TTAT variables. Avoidance motivation was significantly predicted by two IVs: perceived effectiveness and perceived cost, which together accounted for over 37% of variance in the DV. Cost and effectiveness exerted conflicting influences on motivation. Age did not significantly influence the avoidance motivation latent factor. In turn, avoidance motivation exerted a significant influence on avoidance behavior, explaining almost 34% of variance in the behavioral construct. Avoidance behavior was also significantly influenced by participant age.

TTAT versus RScB. Only one TTAT variable (perceived cost) exerted a significant influence on RScB (β = .253, p = .003). Age did not exert any significant influence on the DV.

The total percentage of adjusted variance in RScB explained by the IVs exceeded 9%; notably lower the than percentage of variance explained in protective motivation and protective behavior. The relationship between avoidance behavior and RScB was informally evaluated using Pearsons's r, which showed a significant negative association with a small ES between avoidance behavior and RScB (r = -.202, p = .006, n = 184). The ES was calculated for the perceived cost versus RScB regression outcome using the regression ES formula from Cohen (1992): ES = $\frac{R^2}{1-R^2}$ = .125, which yielded a small/medium result (for multiple regression, Cohen suggests .02 as a small ES descriptor and .15 as a medium ES reference value).

Discrimination of RScB Category Membership

The regression findings from Figure 16 were used to evaluate predictive capability of RScB category membership (one of four categories) based on the technology threat avoidance variable *perceived cost*. Discriminant analysis (DA) was used for the predictive evaluation.

Box's M test ascertained no significant differences between covariance matrices for the RScB categories. The DA used group sizes to calculate prior probabilities (as opposed to using equal-sized groups). The discriminant was significantly predictive: $\chi^2(3) = 13.95$, p = .003. The single predictor correctly predicted 37 % of RScB category membership.

In DA, the ES (η^2) for an overall discriminant model is determined using Wilk's λ such that $\eta^2 = 1 - \lambda$ (Warner, 2008, p. 674). For the study sample and discriminant function using the four-state model, $\lambda = .926$, yielding an ES indicator of (1 - .926) = .074.

To further explore effects of increased theoretical power on the DA outcome, RScB categories were reduced into two higher level categories, consistent with Bryson and Phillips (1975):

- *averse* and *strongly averse* RScB categories were combined into a *comparatively averse* category, and
- *seeking* and *strongly seeking* RScB categories were combined into a *comparatively seeking* category.

The single discriminant model was applied to the aggregated RScB categories and deemed significant: $\lambda = .968$, $\eta^2 = .032$, $\chi^2(1) = 5.93$, $p = .015$. The model correctly predicted 67.9% of high-level RScB category membership.

CHAPTER 5

DISCUSSION AND CONCLUSION

Analysis revealed multiple insights relevant to the research questions. Pertinent outcomes and implications are discussed in this section, and are considered in light of general data collection, external validity, RScB and TTAT characteristics, RScB value categories, associations between TTAT and RScB variables, and operational utility of findings.

Data Collection and Filtering

An unexpected volume of survey responses were discarded; 18% of responses (53 of 294) were excluded if any of the four trap questions were answered incorrectly. The related rejection rate was notably higher than rates reported by others:

- Tsai et al. (2016) discarded fewer than 2% of over 1000 responses due to invalid trap answers, but those participants were recruited from a compensated, premium-level participant pool;
- approximately two percent of 251 responses by compensated participants were discarded by Aivazpour and Rao (2018),
- Egelman and Peer (2015) excluded 4.8% of compensated participant responses, and

- Mamonov and Benbunan-Fich (2018) discarded 2.5% of 400 responses due to answer bias, which included wrong trap question answers (their respondents were also compensated).

Talebi (2017) shared a comparable (22%) discard rate from incorrect trap responses by unpaid participants. However, responses were retained by Talebi if fewer than two traps had incorrect answers.

The proportion of discards were concerning. Percentages of excluded trap questions varied widely between the cited studies, but rejects appeared to be fewer when participants were crowd sourced. The convenience/snowball sampling technique used for this study had no such consistency driver.

Generalizability of Findings

Outcomes that apply to the research questions must be considered in light of sample characteristics, particularly whether findings from the research should be considered externally valid. Chi-squared goodness of fit tests found sample values differed significantly from the target population (i.e., working or retired adults in the United States) regarding age, education level, and employer size.

Age. Age distribution within the sample differed significantly from the overall population ($\chi^2(6) = 53.3$, $p < .001$). The median participant age group consisted of people in their 50's; notably older than the general population median of 37.2 years (US Census, 2011). Sample ages particularly diverged from the overall population distribution among people in their 20's: Twenty-somethings currently comprise 19% of adults overall in the United States, but comprised less than 3% of the sample.

Education level. Similar to sample age, education levels were significantly higher than the United States population ($\chi^2(6) = 937.6$, $p < .001$); approximately 60% of participants held graduate degrees. This contrasted with approximately 12% of the general population (US Census, 2017).

Employer size. Employer size was also compared between the sample and the target population. The distribution of participants by size of employers differed significantly from the US overall ($\chi^2(8) = 53.1$, $p < .001$): Over 60% of respondents worked for organizations with 1,000 or more employees whereas only 40% of the target population work for non-government employers of similar size (US Bureau of Labor Statistics, 2018).

Implications for external validity. Demographic variables for this research were specified based on findings from the literature review. This research precluded collection and study of cultural, racial and socioeconomic data, which are also known to affect CySec-related behaviors. Given the a) statistically significant differences between participant demographics and the overall target population, b) non-collection of racial/cultural/socioeconomic indicators, and c) impacts of snowball recruiting of study participants, findings from this study are not considered generalizable to the overall population.

Characteristics of RScB Data Values

RScB data underwent notable amounts of validation and scrubbing prior to regression analysis. Such validation was not anticipated for this study, as previous studies noted acceptable and high levels of internal consistency that obviated need for PCA. Conversely, this study noted low levels of RScB internal consistency, so PCA was needed. Fortunately, PCA outcomes improved convergent/discriminant validity for the adjusted RScB variables.

Aggregate RScB scores were lower than initially expected, despite removal of three questions. However, reconciliation against Hadlington (2017) revealed mean scores were nearly equivalent across both studies at 22% of the range maximum; no RScB mean value was noted for comparison from the 2018 replication study by Aivazpour and Rao. The low RScB mean values in comparison to the range of values captured may warrant scaling considerations by future works.

Technology Threat Avoidance Factor Qualities

Most unexpected findings arose from variables intrinsic to TTAT, the theoretical area explored most extensively by previous studies. Table 25 shares specific reflections by TTAT IV.

Table 25.

IV-based summary of internal TTAT outcomes

IV	DV	β | Significance	Comments
Perceived Susceptibility	Avoidance Motivation	.061 | $p > .05$	Unexpected non-significance
Perceived Severity	Avoidance Motivation	.052 | $p > .05$	Unexpected non-significance
Perceived Effectiveness	Avoidance Motivation	.462 | $p < .001$	Expected significance; expected direction
Perceived Cost	Avoidance Motivation	-.427 | $p < .001$	Expected significance; expected direction

IV	DV	β | Significance	Comments
Self-Efficacy	Avoidance Motivation	-.046 | p > .05	Unexpected non-significance
Avoidance Motivation	Avoidance Behavior	.588 | p <.001	Expected significance; expected direction

Lack of significance of the *threat appraisal* factor variables (susceptibility and severity) on the avoidance motivation DV was not expected: susceptibility (i.e., likelihood/probability) and severity (i.e., magnitude) of impact are widely acknowledged as key quantifiers of risk (Aven, 2016). Consequently, both were expected to significantly associate with avoidance motivation.

Similarly, the lack of significance of self-efficacy as a predictor of avoidance motivation was not expected; its impact has been found significant by earlier PMT/TTAT studies, including Workman et al. (2008) and Chen and Li (2017), whose impacts are respectively illustrated in Figure 7 and Figure 8. Moreover, in most studies where self-efficacy was a significant IV, its impact and significance were exceeded by at least one of the perceived threat IVs. Examples are Samhan (2017), Herath et al. (2014), Liang and Xue (2010), and Young et al. (2016). The reason for lack of association between self-efficacy and avoidance motivation may be a direct consequence of the sample: most participants were employed by large organizations of over 1,000 employees -- greater levels of CySec protection in large organizations may attenuate feelings of CySec vulnerability (Hadlington, 2017).

Variance in avoidance motivation. The total amount of explained variance (37.3%) in avoidance motivation appears largely consistent with previous TTAT studies, although no significant influences were noted from the perceived threat IVs (susceptibility and severity). Comparable R^2 values for avoidance motivation were shared by Liang and Xue (2010), Talebi (2018), Samhan (2017), and Tsai et al. (2016) with respective variances of 56%, 43%, 63%, and 43.2%. However, all the aforementioned studies either denote significant associations from the two threat appraisal IVs or from a greater number of coping appraisal IVs supported by augmented theoretical models. In summary, the avoidance motivation variance from this study appears reasonable, as it is bracketed by lower values from a) the TTAT replication study by Young et al. (2016) where the avoidance motivation R^2 was equal to 34% and b) the email security services-specific study by Herath et al. (2014) with an avoidance motivation variance of 30.3%.

Variance in avoidance behavior. This study treated avoidance behavior in a manner consistent with previous TTAT works: as a DV of avoidance motivation. A strong avoidance motivation standardized regression coefficient of .588 ($p < .001$) explained 33.6% of the variance in self-reported behavior. To facilitate comparison, Table 26 lists relationships between avoidance motivation and avoidance behavior from several works using regression coefficients, significance and percentage of explained behavior variance. Its contents are sorted by percentage of explained variance, in increasing order.

Table 26.

Cross study comparison - avoidance motivation versus avoidance behavior R^2

Study	β Avoidance Motivation	β Significance Avoidance Motivation	% explained avoidance behavior R^2
Liang and Xue (2010)	.43	p < .01	21%
This study	**.588**	**p < .001**	**33.6%**
Samhan (2017)	.43	p < .01	37%
Chen and Li (2017)	.490	p < .001	45.4%
Young et al. (2016)	.75	p < .001	57%

The findings from this research appear reasonable: avoidance motivation coefficients and percentages of explained variance in avoidance behavior are bracketed above and below by analogous figures from other TTAT studies.

Comparative IV effects: TTAT versus RScB

Explanation of RScB variance from IVs yielded lower than expected associations: TTAT IVs explained only 9.4% of the variance in RScB (p = .003); moreover, the explanation was limited to the influence of a single IV. However, several comparative findings still emerged from the regression analysis:

- perceived cost exhibited a significant positive effect on RScB (expected),

- perceived cost exhibited a significant negative effect on avoidance motivation (expected),
- participant age exhibited a significant association with avoidance behavior and no significant associations with avoidance motivation or RScB (all were expected to be impacted), and
- avoidance behavior was negatively correlated with RScB, as expected ($r = -.202$, $p = .006$), but the measure indicated weak correlation.

All TTAT IVs were initially expected to exhibit significant associations with RScB. A larger correlation magnitude was also expected between protective behavior and RScB than what was observed.

RScB variance is clearly affected by factors external to the technology threat avoidance realm. The complexity of RScB is hinted at by the cited works by Aivazpour and Rao (2018) and Hadlington (2017). Those items noted significant associations between RScB and impulsive behavior, internet addiction, and attitudes towards CySec. The replication study by Aivazpour and Rao (2018) noted motor impulsivity findings that explained over 40% of RScB variance (in contrast with <10% of variance that explained by impulsive behavior in the original study by Hadlington). Attitudes towards cybersecurity contributed approximately 16% of variance in Hadlington's 2017 study; the 2018 replication study noted "no major difference" (p. 5) from the original study regarding the explanatory power of CySec related attitudes as an RScB predictor. TTAT appears to coincide with many aspects of the CySec attitude measurement used in those two studies; substitution of a TTAT-based instrument for CySec attitude measurement may provide greater convergent and divergent validity and a more formalized basis to evaluate the explanatory power of impulsivity, internet addition, and CySec attitudes on RScB variance.

Discrimination of RScB category membership. Some predictive capability arose from use of RScB categories that originated from k-means cluster analysis. The DA model appeared to hold promise based on the almost 70% correct predictive ability ($p = .015$) of a single discriminant (cost) to predict membership in one of two high level RScB categories (*comparatively averse* or *comparatively seeking*). Although the model correctly predicted 67.9% of high-level RScB category membership, the prediction rate was not a meaningful measure of discriminant effectiveness; a predictor could have achieved nearly the same predictive accuracy by arbitrarily mapping every IV value into the *comparatively averse* category (actual *comparatively averse* cases outnumbered actual *comparatively seeking* cases by two-to-one in the sample). An ES was needed to evaluate the discriminant function in a less biased manner.

The primer by Ferguson (2009) provides ES interpretation guidelines that depict .04 as the "recommended minimum effect size representing a 'practically' significant effect for social science data" (p. 533). This indicated non-utility for the single discriminate model applied against the aggregated RScB categories (ES = $\eta^2 = .032$). However, the guidelines indicated meaningful utility for the single discriminant model when applied against the four RScB categories (ES = $\eta^2 = .074$).

Improved DA predictability can derive from two primary avenues: a) future TTAT/RScB studies that identify significant candidate discriminant variables within the TTAT realm and b) incorporation of candidate discriminants from non-TTAT domains; e.g., impulsiveness-related variables explored by Hadlington (2017) and Aivazpour and Rao (2018).

Research Questions Revisited

Research and discussion outcomes were considered in light of the five research questions that motivated this study. Each question was considered in sequence.

First research question. To what extent do significant associations exist between TTAT factor values and RScB? One TTAT IV exhibited significant associations with RScB: perceived cost. A small-medium ES was noted for the regression predictor. The impact of cost on RScB beyond those of other IVs highlights a glaring implication: individuals who consider the effort/cost of protective activity to be excessive are more likely to engage in risky cybersecurity behavior.

Second research question. To what extent can RScB instrument measures be categorized for descriptive classifications of RScB (e.g. to incorporate levels such as low, medium or high)? The normally distributed RScB values in the study sample readily conformed to categorization using k-means cluster analysis. Application of DA to TTAT *perceived cost* variable values yielded a discriminant model with significant prediction of RScB category membership (*highly averse, averse, seeking,* and *highly seeking*) that exceeded cutoff values for minimal utility (cutoff values as per Ferguson, 2009).

Third research question. What TTAT factors are the strongest and weakest predictors of RScB? Perceived cost was the lone significant TTAT factor that demonstrated significant influence on the RScB DV. The remaining IVs did not warrant consideration in light of the analysis results – lack of significance resulting from the regression analysis precluded them from consideration as RScB predictors in this study.

Fourth research question. To what extent do associations between TTAT factor values and RScB appear consistent with previously published associations between TTAT factor values

and measurements of protective (i.e. non-harmful) behavior? This study noted TTAT regression coefficient values that largely paralleled earlier works. In cases where regression coefficient values fell outside established ranges, magnitudes were not so different as to be perceived as dramatic; values were generally consistent with those poised elsewhere.

RScB values were consistent with Hadlington (2017) even though multiple questions were excluded for this study. Mean instrument values consistently fell at 22% of the sample maximum in both studies, and SD measures and skewness were similar across both samples.

More TTAT-specific insights regarding the fourth research question. Most prior studies have discerned significant associations between threat appraisal IVs (perceived threat, perceived severity) and avoidance motivation. However, none were noted by this study. Non-association may be a consequence of participant employment; 60% of participants work for organizations with 1,000 or more employees. Larger organizations exercise higher levels of investment in CySec. Consequently, their employees may appraise CySec threats as less likely and less damaging than do employees of smaller organizations (Hadlington, 2017).

Coping appraisal variables (perceived effectiveness, perceived cost, self-efficacy) were noted by most prior studies as significantly impactful on avoidance motivation. This work found only one of three (perceived cost) to be significant.

The perceived cost regression coefficient ($\beta = -.427$, $p < .003$) within the TTAT-specific model had greater magnitude than other cited works, where value magnitudes ranged between .102 and 0.3 (Workman et al., 2008; Young et al., 2016, respectively).

The perceived effectiveness regression coefficient was significant within the TTAT-specific model ($\beta = .462$, $p<.003$). Its value exceeded those of the other cited TTAT studies;

significant coefficient values ranged from .0148 to 0.427 (Workman et al., 2008; Chen & Li, 2017, respectively).

The self-efficacy coefficient ($\beta = -0.46$, $p > .017$) ((non-significant within the TTAT model) was lower than the same coefficient found in other cited works -- coefficient magnitudes ranged from 0.10 to 0.168 (Young et al., 2016; Workman et al., 2008, respectively). Regarding latent and dependent variables avoidance motivation and avoidance behavior – both were bracketed by other cited works; detailed comparisons are shown in Table 26.

Fifth research question. To what extent do significant associations between TTAT factors on RScB demonstrate HRD business-level utility (i.e., differences in terms of statistical effect sizes?) The greatest potential for business level utility arose from a) categorization of RScB scores into four descriptive categories and b) application of DA to determine the strength of the lone significant regression variable (perceived cost) as a predictor. The resulting discriminant embodied sufficient effect to comprise statistical and practical significance. Consequently, the single discriminant model comprises a valid starting point for further study and augmentation via a) additional TTAT variables and or b) variables associated with impulsivity, e.g., those studied by Aivazpour and Rao (2018), Hadlington (2017), and Hadlington and Murphy (2018).

Implications for Further Research

This study revealed several opportunities for further investigation. Numerous areas were noted for future research.

Opportunities for further exploratory/theoretical study. New insights may emerge if the research model is applied to randomly selected samples to a) better understand the range of

RScB, b) re-evaluate the predictive strength of TTAT IVs on RScB, and c) refine/test descriptive categories of RScB applicable to the workplace. (The participant sample for this study was not representative of the overall population regarding age, education, and organizational size of participant employers).

This study applied to RScB at work by adults in the United States. Comparative studies of RScB or similar concepts between work and non-work environments appear to be few in number. New benefit can be gained from deeper understanding of CySec risk-taking by individuals in non-work versus work settings to produce new HRD-related insights. In addition, numerous studies have analyzed TTAT; meta-analyses of these studies may yield findings that further enhance understanding of the TTAT and its core variables.

Greater light can be shed on the nature of RScB by studies that combine TTAT IVs with IVs associated with non-technology-related attributes, e.g., motor and attentional impulsivity. Substitution of a TTAT-based instrument for CySec attitude measurement in such a study may provide higher levels of convergent and divergent validity than other instruments and provide a more formal basis to evaluate the explanatory power of non-TTAT versus TTAT variables on RScB.

The cost-related TTAT impact on RScB signifies need for greater attention on hindrances to CySec protective behavior and their relative impact on perceived cost of protective activity. Such hindrances may include bureaucracy, level of difficulty of use, and financial cost/budget impact.

The analysis methodology used for this research relied on three phases of ordinary least squares regression. This approach called for lower significance limits due to Bonferroni correction, which limited significant findings (see table 24 for specific examples regarding

specific susceptibility and self-efficacy; both had p-values < .05). Subsequent analysis using an integrated technique (e.g. partial least squares) may identify additional significant IVs which do not require exclusion from statistical findings due to Bonferroni correction.

The right skewness of RScB values noted in Hadlington (2017) and paralleled in this study (each work noted RScB mean values equal to approximately 22% of its respective RScB value range) may warrant further research to understand distributions of RScB data values and how those distributions are affected by RScB internal variables and demographic properties of the sample.

Industry-specific attributes may affect mean levels of RScB behavior; this possibility was revealed by a comparison of RScB values across vertical industries, detailed in Table 12. HRD researchers and practitioners may benefit from future research that investigates employee levels of RScB in light of IVs derived from industry-specific characteristics.

Associations noted between outside-of-work CySec behaviors listed in Table 8, specifically antivirus versus firewall use and VPN versus encryption software use, may indicate potential interaction effects, or the existence of multiple factors of contemporary protective behavior. Further research may aid refinement of component-based research instruments (e.g., the RScB by Hadlington, 2017) and/or augmentation of factor-based instruments (e.g., the SeBIS by Egelman and Peer, 2015).

The dynamic nature of CySec presents ongoing opportunities to understand the problem domain in light of human vulnerabilities, protective motivation, and solution adoption. Delphi studies have repeatedly served as effective mechanisms for related discovery; Carlton and Levy (2015), Coventry et al, Parekh et al. (2018), and Sherman et al. (2017) are prime examples. However, research works that bridge gaps between Delphi activity, literature reviews, and

formalized factor presentation and evaluation appear in short supply. Such mechanisms appear positioned to produce actionable knowledge relevant to CySec and its implications for HRD.

Opportunities for operationally-focused study. Additional studies can facilitate measurement and evaluation of findings from this research in operational environments. Large IT organizations are increasingly using automated or artificial intelligence (AI)-based methods to detect breach attempts. However, successful breaches continue to manifest a CySec need to support automated solutions with IT end-user awareness for greatest effectiveness. End user awareness can be facilitated via HRD-sponsored training interventions to impart CySec knowledge and evaluate related behaviors. Table 27 conveys a related pre-post study design.

Table 27.

Pre-post study design for RScB and CySec training

Step	Description	Relevant items addressed
1	Baseline levels of RScB are established using an instrument derived from Hadlington (2017)	Capture baseline
2	A basic training intervention is delivered to members of one or more non-IT-related groups within the organization to: o Convey importance of CySec to the enterprise (reinforced by the organization infosec policy) o Share benefit of IT end-user behaviors regarding CySec	 o Impart empirical awareness o Impart empirical awareness

Step	Description	Relevant items addressed
	○ Provide conceptual descriptions and user familiarization exercises for one or more of the following: − anti-virus protection, − firewall protection, − virtual private networking, and/or − general encryption software.	○ Provide knowledge and skill to minimize time/effort (i.e., perceived cost) associated with avoiding RScB
3	A post-intervention evaluation, again using an instrument derived from Hadlington (2017), administered to provide post-training measurement of RScB in the organization.	Measure and evaluate impact of training

A control/experimental version of this study could incorporate repeated administration of the RScB mechanism to an untrained control group to allow comparison between training-induced behavior change and changes originating from increased user awareness induced by the instrument. Furthermore, longitudinal administration of the RScB instrument could be used to measure increases in RScB over time following the intervention, (i.e., deterioration of training effects to determine appropriate intervals for re-training). Finally, the above design does not incorporate actions to induce effects of normative behavior. Related considerations may be taken into account when identifying groups for training and when specifying the daily working conditions needed to facilitate transfer of the training into ongoing worker behavior.

Organizations may note more effective outcomes if actions are taken to mitigate risky behavior by IT end-users most persistently associated with RScB. Related studies may evaluate CySec training for groups of individuals who must frequently context shift while performing work (i.e., emulate media multi-tasking behavior) or who must persist an online presence to perform their job (i.e., emulate behaviors associated with internet addiction). A pre-post study design similar to the one depicted by Table 27 is also applicable to these instances.

Recommendations for Practice

The lone significant study finding yields pivotal insight for HRD practitioners. The finding shows that IT end-users more frequently demonstrate risky behavior if they consider CySec protective measures as difficult to exercise or costly to employ. Inter-IV comparisons show these considerations outweigh those associated with the potential consequences of contending with an actual breach if one were to occur. This consideration drives several considerations to support CySec protective measures and marginalize risky behavior.

Ease of use. Protective measures must be easy to employ. If individuals are dis-inclined to take protective measures due to intensive effort needed to use them, the likelihood of engaging in risky behavior increases.

Additional supporting insights. Motivation to follow protective measures and avoid risky behavior are more likely to arise if individuals a) understand organizational benefit of doing so, b) believe such efforts are in the best interest of themselves and colleagues, and c) observe standards to support adoption.

Organizational benefit. Firstly, individuals must be provided empirical insight regarding what comprises RScB and the importance of avoiding it (i.e., insights must be shared regarding

the likelihood of breaches and pitfalls associated with them, and reasonable measures needed to preclude them). HRD activity must be considered to impart the required knowledge and ability to comply.

Personal impact. Secondly, personal impacts associated with potential breach outcomes must be noted. If breaches are perceived as an organizational cost rather than an individual one, end-users may not be compelled to embrace protective behavior and/or avoid risky behavior. Greater motivation can result if targeted behaviors are associated with individual actions and are reinforced by integration with incentive programs. This can occur whether determinants are based on key performance criteria (i.e., hard skills) or elements of organization citizenship (i.e., soft skills) associated with one's general role in the organization.

Standards of behavior. Thirdly, organizational statements are important to formalize the relevance of protective action and avoidance of risky behavior to individuals within the enterprise. This is best accomplished via formal statements (i.e., infosec policies) to establish a basis for organizational expectation.

Integrating the insights. None of the aforementioned activities are likely to induce change if not addressed in a holistic manner. Infosec policies must be augmented by a) establishing and sharing empirical knowledge, b) establishing knowledge of personal impact and responsibility for CySec , and c) demonstrating normative behaviors by individuals of notable influence within the organization. These considerations are consistent with those shared by Choi and Ruona (2009); outlined in the review of the literature section.

Considerations regarding ease of use. Locked down infrastructures may be adopted by organizations motivated by a need for stringent CySec and/or a turnkey-based, easy-to-use solutions for IT. Such configurations may hinder productivity by limiting online communication

and actually hinder ease of use (Allhoff & Henschke, 2018). Some degree of individual decision-making capability may be prudent to allow related decision-making (i.e., tailoring of protective mechanisms in special circumstances) by informed IT end-users. Such flexibility must be considered in depth by IT specialists, business-specific subject matter experts, and HRD.

Conclusion

Protection of IT assets and economic goodwill are vital in an information-based economy. The impact of CySec vulnerabilities threatens work organizations and the well-being of enterprises; CySec protection is a critical factor in neutralizing these threats. As IT becomes increasingly important to human expertise in the workplace, HRD horizons must expand to accommodate this changing profile.

This research builds, presents, and uses a theoretical framework which shows HRD is tightly interwoven with CySec workplace concerns. That coupling will grow even tighter over time as individuals increasingly require access of IT assets to perform their work. To protect IT assets and achieve future performance objectives in the workplace, HRD practitioners must embrace opportunities to reconcile knowledge, skills, abilities, and behaviors with CySec concerns.

Previous CySec-related human factors studies have included TTAT-related factors as predictors of IT protective behaviors. However, levels of protective behaviors, or lack thereof, may not be synonymous with the conceptual converse of protective behavior: risky CySec behavior (RScB). No studies are yet noted which explore the role or impact of TTAT factors on RScB. This study is purported to be the first.

Findings derived from this study were based on a participant pool that was older and more highly educated than the overall United State population. The majority of participants worked for organizations with more than 1,000 employees. This relatively homogenous pool revealed findings that a) produced significant regression findings that largely paralleled previous TTAT studies, b) allowed synthesis of new insights regarding the predictive influence on technology threat avoidance variables on RScB, and c) supported formulation of a categorization scheme, to provide a basis for operational utility of RScB in work-related contexts.

The findings of this research are applicable to HRD practitioners and scholars. The most powerful findings relate to the impact of cost/effort on responsible behavior and the importance of marginalizing risky behavior; relevant aspects were discussed above as implications for the HRD practice.

Those responsible for determining training needs, specifying and designing relevant courseware, and evaluating training initiatives face certain resourcing challenges in CySec given the loss mitigation nature of the problem domain. However, given the inexorable growth of the CySc problem space and its importance to the enterprise, these challenges cannot be ignored. It hoped that the findings of this research notably serve their needs and establish a firm foundation for others who endeavor to shed additional light in this area.

REFERENCES

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ..., & Wang, Y. (2017). Nudges for privacy and security: understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, *50*(3), 44:1-44:40. doi: 10.1145/3054926

Addae, J. H., Brown, M., Sun, X., Towey, D., & Radenkovic, M. (2017). Measuring attitude towards personal data for adaptive cybersecurity. *Information & Computer Security*, *25*(5), 560-579. doi: 10.1108/ICySec-11-2016-0085

Agrawal, V. K., Agrawal, V. K., Seshadri, S., & Taylor, A. R. (2017). Trends in IT human resources and end-users involved in IT applications. *Journal of International Technology and Information Management*, *26*(4), 154-188. Retrieved from https://scholarworks.lib.csusb.edu/jitim/vol26/iss4/6

Aivazpour, Z., & Rao, V. S. (2018). Impulsiveness and Risky Cybersecurity Behaviors: A Replication. *Twenty-fourth Americas Conference on Information Systems, New Orleans, 2018*. Retrieved from https://aisel.aisnet.org/amcis2018/Replication/Presentations/2/

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211. doi: 10.1016/0749-5978(91)90020-T

Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, *8*(1), 5. doi: 10.1186/s13673-018-0128-7

Aldabbas, M., & Teufel, B. (2016). Human aspects of smart technologies' security: the role of human failure. *Journal of Electronic Science and Technology*, *14*(4), 311-318. doi:10.11989/JEST.1674-862X.605293

Allhoff, F., & Henschke, A. (2018). The Internet of Things: Foundational ethical issues. *Internet of Things*, *1*, 55-66. doi: 10.1016/j.iot.2018.08.005

Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PloS One*, *12*(3), e0173284. doi: 10.1371/journal.pone.0173284

Astakhova, L. V. (2015). Evaluation assurance levels for human resource security of an information system. *Procedia Engineering*, *129*, 635-639. doi: 10.1016/j.proeng.2015.12.083

Atkinson, J. W. (1957). Motivational determinants of risk-taking behavior. *Psychological Review*, *64*(6), 359-372. doi: 10.1037/h0043445

Atkinson, R., & Flint, J. (2001). Accessing hidden and hard-to-reach populations: Snowball research strategies. *Social Research Update*, *33*(1), 1-4. Retrieved from http://citizenresearchnetwork.pbworks.com/f/accessing%2Bhard%2Bto%2Breach%2Bpopulations%2Bfor%2Bresearch.doc

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, *253*(1), 1-13. doi: 10.1016/j.ejor.2015.12.023

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. doi: 10.1037/0033-295X.84.2.191

Barlette, Y., Gundolf, K., & Jaouen, A. (2015). Toward a better understanding of SMB CEOs' information security behavior: insights from threat or coping appraisal. *Journal of Intelligence Studies in Business, 5*(1). Retrieved from https://ojs.hh.se/index.php/JISIB/article/viewFile/109/108

Bauer, J. M., Van Eeten, M. J., Chattopadhyay, T., & Wu, Y. (2008). ITU study on the financial aspects of network security: Malware and spam. *ICT Applications and Cybersecurity Division, International Telecommunication Union, Final Report, July*. Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf

Becker, G. S. (1993). *Human capital: A theoretical and empirical analysis with special reference to education.* Chicago, IL: University of Chicago Press.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51-61. doi:10.1016/j.chb.2015.01.039

Berdrow, I. & Evers, F. T. (2014). Competence: Basis for employee effectiveness. In Chalofsky, N., Rocco, T. S., & Morris, M. L. (Eds.), *Handbook of human resource development.* (pp. 201-214). Hoboken, NJ: John Wiley & Sons, Inc.

Bergeron, M. Z., & Fornero, S. C. (2018). Centralized and decentralized approaches to managing online programs. In Piña, A. A., Lowell, A. L., & Harris, B.R. (Eds.), *Leading and managing e-learning* (pp. 29-43). Springer, Cham.

Beyer, R. E., & Brummel, B. J. (2015). Implementing effective cyber security training for end-users of computer networks. *SHRM-SIOP Science of HR Series: Promoting Evidence-Based HR*. Retrieved from https://www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/Documents/SHRM-SIOP%20Role%20of%20Human%20Resources%20in%20Cyber%20Security.pdf

Blais, A. R., and Weber, E. U. (2006). A domain-specific risk-taking (dospert) scale for adult populations. *Judgment and Decision Making 1*(1), 33–47. Retrieved from https://ssrn.com/abstract=1301089

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology, 34*(10), 1022-1035. doi:10.1080/0144929X.2015.1028448

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011, November). Measuring the human factor of cyber security. In *Technologies for Homeland Security (HST), 2011 IEEE International Conference on* (pp. 230-235). IEEE. Retrieved from https://calhoun.nps.edu/bitstream/handle/10945/25003/130.pdf?sequence=1

Bracht, G. H., & Glass, G. V. (1968). The external validity of experiments. *American Educational Research Journal*, *5*(4), 437-474. doi: 10.3102/00028312005004437

Broucek, V., & Turner, P. (2013). Technical, legal and ethical dilemmas: distinguishing risks arising from malware and cyber-attack tools in the 'cloud'—a forensic computing perspective. *Journal of Computer Virology and Hacking Techniques, 9*(1), 27-33. doi: 10.1007/s11416-012-0173-0

Bryson, K. R., & Phillips, D. P. (1975). Method for classifying interval-scale and ordinal-scale data. *Sociological Methodology, 6*, 171-190. doi: 10.2307/270896

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157-165. doi: 10.1002/asi.20459

Burov, O. Y. (2016). Educational networking: human view to cyber defense. *Information Technologies and Learning Tools, 52*(2), 144-156. Retrieved from http://journal.iitta.gov.ua/index.php/itlt/article/download/1398/1039

Caliński, T., & Harabasz, J. (1974). A dendrite method for cluster analysis. *Communications in Statistics-theory and Methods*, *3*(1), 1-27.

Carlton, M. (2016). *Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills*. Retrieved from ProQuest Dissertations & Theses (Order No. 10240271).

Carlton, M., & Levy, Y. (2015, April). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. In SoutheastCon 2015 (pp. 1-6). IEEE.

Carlton, M., Levy, Y., Ramim, M., & Terrell, S. (2015, December). *Development of the MyCyberSkills™ iPad app: a scenarios-based, hands-On measure of non-IT professionals' cybersecurity skills.* Paper presented at the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC), Fort Worth, TX

Carr, N. (2011). *The shallows: What the internet is doing to our brains*. New York: WW Norton & Company.

Cavelty, M. D. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics, 20*(3), 701-715. doi: 10.1007/s11948-014-9551-y

Cavelty, M. D. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance, 6*(2), 22-30. doi: 10.17645/pag.v6i2.1385

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). A taxonomy of operational cyber security risks version 2 (No. CMU/SEI-2014-TN-006). Carnegie-Mellon University, Pittsburgh PA Software Engineering Inst. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA609863

Chen, H., & Li, W. (2017). Mobile device users' privacy security assurance behavior: A technology threat avoidance perspective. *Information & Computer Security*, *25*(3), 330-344. doi: 10.1108/ICS-04-2016-0027

Chin, A. G., Etudo, U., & Harris, M. A. (2016). On mobile device security practices and training efficacy: An empirical study. *Informatics in Education*, *15*(2), 235. doi: 10.15388/infedu.2016.12

Choi, M., & Ruona, W. E. A. (2011). Individual readiness for organizational change and its implications for human resource and organization development. *Human Resource Development Review*, *10*(1), 46–73. doi: 10.1177/1534484310384957

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems*, *52*(4), 20-29. Retrieved from https://pdfs.semanticscholar.org/5991/6f95d9f8c8837a1b5cbe34bc5e3157fec62e.pdf

Cohen, J. (1992). A power primer. *Psychological bulletin*, *112*(1), 155-159. doi: 10.1037/0033-2909.112.1.155

Corradini, I., & Nardelli, E. (2018). Building organizational risk culture in cyber security: the role of human factors. In Ahram, T. Z., & Nicholson, D. (Eds.), *Advances in human factors in cybersecurity : Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA*. Cham: Springer

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. UK Government Report. Retrieved from http://nrl.northumbria.ac.uk/23903/1/14-835-cyber-security-behavioural-insights.pdf

Coventry, L., Jeske, D., & Briggs, P. (2014). Perceptions and actions: Combining privacy and risk perceptions to better understand-user behaviour. In: Symposium on Usable Privacy and Security (SOUPS) 2014, July 9-11, 2014, Menlo Park, CA. Retrieved from http://nrl.northumbria.ac.uk/17995/1/Coventry_et_al_2014_SOUPS_workshop.pdf

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297–334. doi: 10.1007/BF02310555

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, *48*, 281-297. doi: 10.1016/j.cose.2014.11.002

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information & Computer Security*, *24*(1), 116-134. doi: 10.1108/ICS-04-2015-0018

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security*, *24*(2), 139-151. doi: 10.1108/ICS-12-2015-0048

Davis, F.D. (1989) Perceived usefulness, perceived ease of use and-user acceptance of information technology.*MIS Quarterly*, *13*, 319–340.

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, *9*, 1-12. doi: 10.3389/fpsyg.2018.00744

Egelman, S., Harbach, M., & Peer, E. (2016, May). Behavior ever follows intention?: A validation of the security behavior intentions scale (SeBIS). In *Proceedings of the 2016 CHI conference on human factors in computing systems* (pp. 5257-5261). ACM. doi: 10.1145/2858036.2858265

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2873-2882). ACM. doi: 10.1145/2702123.2702249

Fagan, M., Albayram, Y., Khan, M. M. H., & Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences*, *7*(1), 1-12. doi: 10.1186/s13673-017-0093-6

Fan, L., Liu, X., Wang, B., & Wang, L. (2017). Interactivity, engagement, and technology dependence: understanding users' technology utilisation behaviour. *Behaviour & Information Technology*, *36*(2), 113-124. doi:10.1080/0144929X.2016.1199051

Federal Trade Commission website (n.d.). Accessed via https://www.ftc.gov/equifax-data-breach

Ferguson, C. J. (2009). An effect size primer: A guide for clinicians and researchers. *Professional Psychology: Research and Practice, 40*(5), 532. doi: 10.1037/a0015808

Fishbein, M. and Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research,* Addison-Wesley, Boston, MA.

Ghasemi, A., & Zahediasl, S. (2012). Normality tests for statistical analysis: a guide for non-statisticians. *International journal of endocrinology and metabolism*, *10*(2), 486-489. doi: 10.5812/ijem.3505

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? internet security and human vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44. Retrieved from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1761&context=jais

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security*, *9*(02), 133. doi: 10.4236/jis.2018.92010

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. doi: 10.1016/j.cose.2017.11.015

Gross, J. R. (2015). Hack and be hacked: A framework for the United States to respond to non-state actors in cyberspace. *California Western International Law Journal, 46*, 109-145. Retrieved from http://scholarlycommons.law.cwsl.edu/cgi/viewcontent.cgi?article=1513&context=cwilj

Guin, T. D. L., Baker, R., Mechling, J., & Ruyle, E. (2012). Myths and realities of respondent engagement in online surveys. *International Journal of Market Research, 54*(5), 613-633. doi: 10.2501/IJMR-54-5-613-633

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsiveness, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. doi: 10.1016/j.heliyon.2017.e00346

Hadlington, L., & Murphy, K. (2018). Is media multitasking good for cybersecurity? Exploring the relationship between media multitasking and everyday cognitive failures on self-reported risky cybersecurity behaviors. *Cyberpsychology, Behavior, and Social Networking*, *21*(3), 168-172. doi: 10.1089/cyber.2017.0524

Hanus, B. T. (2014). The impact of information security awareness on compliance with information security policies: A phishing perspective. Retrieved from ProQuest Dissertations & Theses (Order No. 3727160).

Heartfield, R., & Loukas, G. (2015, December). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM *Computing Surveys (CSUR)*, *48*(3), 37:1-37:39. doi: 10.1145/2835375

Helmer, O. (1963). *The systematic use of expert judgment in operations research*. Santa Monica, CA: Rand Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/papers/2008/P2795.pdf

Helmer, O. (1967). *Analysis of the future: The Delphi method*. Santa Monica, CA: Rand Corporation. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/649640.pdf

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journal*, *24*(1), 61-84. doi: 10.1111/j.1365-2575.2012.00420.x

Hewitt, B., Dolezel, D., & McLeod Jr, A. (2017). Mobile device security: Perspectives of future healthcare workers. *Perspectives in Health Information Management, 14*(Winter). doi:

Hobart, B., & Sendek, H. (2014). *Gen y now: Millennials and the evolution of leadership*. San Francisco, CA: John Wiley & Sons Inc.

Holmes, M. K., Bearden, C. E., Barguil, M., Fonseca, M., Serap Monkul, E., Nery, F. G., ... & Glahn, D. C. (2009). Conceptualizing impulsivity and risk taking in bipolar disorder: importance of history of alcohol abuse. *Bipolar Disorders, 11*(1), 33-40.

Huang, Z. (2015). Human-centric training and assessment for cyber situation awareness (Doctoral dissertation, University of Delaware). Retrieved from http://udspace.udel.edu/handle/19716/17558

Hughes, C., & Byrd, M. (2015). *Managing human resource development programs: Current issues and evolving trends*. New York, NY: Palgrave MacMillan.

Inan, F. A., Namin, A. S., Pogrund, R. L., & Jones, K. S. (2016). Internet Use and Cybersecurity Concerns of Individuals with Visual Impairments. *Journal of Educational Technology & Society, 19*(1), 28-40.

Indiana State University Institutional Review Board (2014). *Indiana State University policies and procedures for the review of research involving human subjects*. Retrieved from https://www.indstate.edu/sites/default/files/media/Documents/PDF/irb-manual-revised-10-6-2014.pdf

Jacobs, R. L. (2014). System theory and HRD. In Chalofsky, N., Rocco, T. S., & Morris, M. L. (Eds.), *Handbook of human resource development.* (pp. 21-39). Hoboken, NJ: John Wiley & Sons, Inc.

Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security*, *25*(2), 165-180. doi: 10.1108/ICySec-03-2017-0018

Kelley, T., Amon, M. J., & Bertenthal, B. I. (2018). Statistical models for predicting threat detection from human behavior. *Frontiers in Psychology*, *9*, 466. doi: 10.3389/fpsyg.2018.00466

Kim, H. Y. (2013). Statistical notes for clinical researchers: assessing normal distribution (2) using skewness and kurtosis. *Restorative Dentistry & Endodontics*, *38*(1), 52-54. doi: 10.5395/rde.2013.38.1.52

Kim, H. Y. (2017). Statistical notes for clinical researchers: chi-squared test and Fisher's exact test. *Restorative dentistry & endodontics*, *42*(2), 152-155. doi: 10.5395/rde.2017.42.2.152

Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the castle model of cyber-risk and cyber-security. *Government Information Quarterly*. *33*(2), 250-257. doi: 10.1016/j.giq.2016.01.012

Lewin, K. (1951). *Field theory in social science*. New York, NY: Harper and Brothers.

Liang, H.G. & Xue, Y.J. (2009) Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly, 33*, 71–90.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394–413. Retrieved from http://search.proquest.com.ncat.idm.oclc.org/docview/734860834/fulltextPDF/F67F0E8E43042C3PQ/2?accountid=12711

Lin, M., Lucas, H. C., Shmueli, G. (2013) Research commentary—too big to fail: large samples and the p-value problem. *Information Systems Research, 2*(4), 906-917. doi:10.1287/isre.2013.0480

MacQueen, J. (1967). Some methods for classification and analysis of multivariate observations. In Luncien, M., Cam, L., & Neyman, J. (Eds.). *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability: Vol. 1*, (pp. 281–297). Berkeley, CA: The University of California Press.

Maimon, D., Becker, M., Patil, S., & Katz, J. (2017, October). Self-protective behaviors over public wifi networks. In *The LASER Workshop: Learning from Authoritative Security Experiment Results* (pp. 69-76). USENIX Association

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32-44. doi: 10.1016/j.chb.2018.01.028

Matsumoto, D., & Hwang, H. C. (2013). Assessing cross-cultural competence: A review of available tests. *Journal of Cross-Cultural psychology, 44*(6), 849-873. doi: 10.1177/0022022113492891

Mayo, E. (1933). *The human problems of an industrial civilization*. New York: McMillan

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems, 21*. Retrieved from http://journal.acs.org.au/index.php/ajis/article/download/1697/796

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69,* 151-156. doi: 10.1016/j.chb.2016.11.065

Mitnick, K. & Simon, W. L. (2011). *Ghost in the wires: My adventures as the world's most wanted hacker*. New York, NY: Little, Brown & Company

Murphy, K., McLauchlan, S., & Lee, M. (2017). Is there a link between media-multitasking and the executive functions of filtering and response inhibition?. *Computers in Human Behavior, 75,* 667-677. doi: 10.1016/j.chb.2017.06.001

Ovelgönne, M., Dumitraş, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the relationship between human behavior and susceptibility to cyber attacks: a data-driven approach. *ACM Transactions on Intelligent Systems and Technology (TIST), 8*(4), 51. doi: 10.1145/2890509

Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing, 82*(4), 331e338. doi: 10.1016/j.jretai.2006.08.006

Parekh, G., DeLatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., & Sherman, A. T. (2018). Identifying core concepts of cybersecurity: Results of two Delphi processes. *IEEE Transactions on Education*, *61*(1), 11-20. Retrieved from http://publish.illinois.edu/glherman/files/2017/09/2017-ToE-Cybersecurity-Delphi-pre-print.pdf

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security, 66,* 40-51. doi: 10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, 165-176. doi: 10.1016/j.cose.2013.12.003

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing information security awareness at an Australian bank: a comparative study. *Information & Computer Security*, *25*(2), 181-189. doi: 10.1108/ICySec-03-2017-0017

Payette, J., Anegbe, E., Caceres, E., & Muegge, S. (2015, June). Secure by design: Cybersecurity extensions to project management maturity models for critical infrastructure projects. *Technology Innovation Management Review*, *5*(6), 26-34.

Perlroth, N., Tsang, A., & Satariano, A. (2018, November 30). Marriott hacking exposes data of up to 500 million guests. *The New York Times*. Retrieved from https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html

Plachkinova, M., & Maurer, C. (2018). Teaching case: security breach at Target. *Journal of Information Systems Education*, *29*(1), 11. Retrieved from http://jise.org/Volume29/n1/JISEv29n1p11.pdf

Rajivan, P., Moriano, P., Kelley, T., & Camp, L. J. (2017). Factors in an end-user security expertise instrument. *Information & Computer Security*, *25*(2), 190-205. doi: 10.1108/ICySec-04-2017-0020

Rawal, B. S., Liang, S., Loukili, A., & Duan, Q. (2016). Anticipatory cyber security research: An ultimate technique for the first-move advantage. *TEM Journal*, *5*(1), 3-14. doi: 10.18421/TEM51-01

Reddy, C. K., & Bhanukiran, V. (2014). A survey of partitional and hierarchical clustering algorithms. In Aggarwal, C. C., & Reddy, C. K. (Eds.), *Data clustering: Algorithms and applications.* New York, NY: Taylor and Francis Group

Ritzman, M. E., & Kahle-Piasecki, L. (2016). What works: A systems approach to employee performance in strengthening information security. *Performance Improvement, 55*(8), 17-22. doi: 10.1002/pfi.21614

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114. doi: 10.1080/00223980.1975.9915803

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education Monographs, 2*(4), 328-335. doi: 10.1177/109019817400200403

Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1988). Social learning theory and the health belief model. *Health Education & Behavior, 15*(2), 175-183. doi: 10.1177/109019818801500203

Rosenthal, R., & Jacobson, L. (1968). *Pygmalion in the classroom: Teacher expectation and pupils' intellectual development.* New York: Holt, Rinehart & Winston

Ruona, W.E.A. (2009). Systems theory as a foundation for human resources development. In Swanson, R. A. & Holton III, E. F. (Eds.), *Foundations of human resource development (2nd Ed.).* San Francisco, CA: Berrett-Koehler Publishers, Inc. (ISBN 978-1-57675-496-2).

Samhan, B. (2017, April). Security behaviors of healthcare providers using HIT outside of work: A technology threat avoidance perspective. In *Information and Communication Systems (ICICySec), 2017 8th International Conference on*, 342-347. IEEE.

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimization: An empirical study of social networking users. *Technological Forecasting and Social Change, 102*, 320-330. doi: 10.1016/j.techfore.2015.08.012

Sawatsky, M. L., Clyde, M., & Meek, F. (2015). Partial least squares regression in the social sciences. *The Quantitative Methods for Psychology, 11*(2), 52-62. doi: 10.20982/tqmp.11.2.p052

Sawyer, B. D., Finomore, V. S., Funke, G. J., Mancuso, V. F., Miller, B., Warm, J., & Hancock, P. A. (2015, August). Evaluating cybersecurity vulnerabilities with the email testbed: effects of training. *In Proceedings 19th Triennial Congress of the IEA, 9*, 1-6.

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors*, *60*(5), 597-609. doi: 10.1177/0018720818780472

Scott, S. G., and Bruce, R. A. (1995). Decision-making style: The development and assessment of a new measure. *Educational and Psychological Measurement, 55*(5), 818–831. doi: 10.1177/0013164495055005017

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the Conference on Human Factors in Computing Systems, 13*(1), 373–382. doi: 10.1145/1753326.1753383

Shepardson, D. (2017, November 8). *Former Yahoo CEO apologizes for data breaches, blames Russians*. *Reuters News Agency*. Retrieved from https://www.reuters.com/article/us-usa-databreaches/former-yahoo-ceo-apologizes-for-data-breaches-blames-russians-idUSKBN1D825V

Sherman, A. T., DeLatte, D., Neary, M., Oliva, L., Phatak, D., Scheponik, T., ... & Thompson, J. (2018). Cybersecurity: Exploring core concepts through six scenarios. *Cryptologia*, *42*(4), 337-377. doi: 10.1080/01611194.2017.1362063

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. *AMCIS 2006 Proceedings*, 415.

Stanciu, V., & Tinca, A. (2017). Exploring cybercrime–realities and challenges. *Accounting and Management Information Systems*, *16*(4), 610-632. doi:10.24818/jamis.2017.04009

Stevens, T. (2018). Global Cybersecurity: New Directions in Theory and Methods. *Politics and Governance*, *6*(2), 1-4. doi: 10.17645/pag.v6i2.1569

Sutton, S., & Davidson, R. (1997). Prefrontal brain asymmetry: A biological substrate of the behavioral approach and inhibition systems. *Psychological Science, 8*(3), 204-210. doi: 10.1111/j.1467-9280.1997.tb00413.x

Swanson, R. A. & Holton III, E. F. (2009). Foundations of human resource development (2nd Ed.). San Francisco, CA: Berrett-Koehler Publishers, Inc. (Kindle edition. ISBN 978-1-57675-496-2).

Swart, J., Mann, C., Brown, S., & Price, A. (2005). *Human Resource Development*. Burlington, MA: Butterworth-Heinemann

Talebi, N. (2018). *The Effect of Perceived Warning Message Characteristics on Coping Responses in Data Breach Scenarios* (Doctoral dissertation, The University of Texas at San Antonio). Retrieved from Proquest Dissertations and Theses (Order No. 10784195).

Thomas, J. E. (2017). *Human resilience and development in coupled socio-technical Systems: a holistic approach to critical infrastructure resilience* (Doctoral dissertation). Retrieved from https://repository.asu.edu/attachments/186224/content/Thomas_asu_0010E_16741.pdf

TRADOC (2010). *Cyberspace Operations Concept Capability Plan 2016-2028*. TRADOC Pamphlet 525-7-8. Fort Eustis, VA: United States Army Training and Doctrine Command.

Trim, P., & Upton, D. (2016). *Cyber security culture: Counteracting cyber threats through organizational learning and training*. Burlington, VT: Gower

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. doi: 10.1016/j.cose.2016.02.009

US Bureau of Labor Statistics website (2018). Retrieved from https://www.bls.gov/bdm/bdmfirmsize.htm

US Census website (2011). *Age and sex composition: 2010*. Retrieved from https://www.census.gov/prod/cen2010/briefs/c2010br-03.pdf

US Census website (2017). Retrieved from https://www.census.gov/data/tables/2017/demo/education-attainment/cps-detailed-tables.html

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547-559. doi: 10.1016/j.chb.2017.05.038

Van Wilsem, J. (2011). Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168-178. doi: 10.1093/esr/jcr053

Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 1-21. doi: 10.1177/0093650215627483

Warner, R. M. (2008). *Applied statistics: applied bivariate through multivariate techniques*. Thousand Oaks, CA: Sage Publications, Inc.

Weber, E. U., Blais, A. R., & Betz, N. E. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of behavioral decision making, 15*(4), 263-290. doi: 10.1002/bdm.414

White, G. L. (2015). Education and prevention relationships on security incidents for home computers. *Journal of Computer Information Systems, 55*(3), 29-37. doi: 10.1080/08874417.2015.11645769

White, G., Ekin, T., & Visinescu, L. (2017). Analysis of protective behavior and security incidents for home computers. *Journal of Computer Information Systems, 57*(4), 353-363. doi: 10.1080/08874417.2016.1232991

Whiteside, S. P., & Lynam, D. R. (2001). The five factor model and impulsivity: Using a structural model of personality to understand impulsivity. *Personality and Individual Differences, 30*(4), 669-689. doi: 10.1016/S0191-8869(00)00064-7

Williams, N., & Li, S. (2017, June). Simulating human detection of phishing websites: An investigation into the applicability of the ACT-R cognitive behaviour architecture model. In *Cybernetics (CYBCONF), 2017 3rd IEEE International Conference on* (pp. 1-8). IEEE. doi: 10.1109/CYBConf.2017.7985810

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. I*nformation Systems Security*, *16*(6), 315-331. doi: 10.1080/10658980701788165

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799-2816. doi: 10.1016/j.chb.2008.04.005

Young, D. K., Carpenter, D., & McLeod, A. (2016). Malware avoidance motivations and behaviors: A technology threat avoidance replication. *AIS Transactions on Replication Research*, *2*(8), 1-17. Retrieved from https://pdfs.semanticscholar.org/7dfc/b5725dbc9999732432cec8192bcb0757fd4e.pdf

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, smishing & vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297-307. Retrieved from http://www.cisjournal.org/journalofcomputing/Download_April_14_pdf_6.aspx

APPENDIX A: HUMAN FACTORS IN CYSEC LITERATURE SUMMARY GRID

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Addae, Brown, Sun, Towey, & Radenkovic (2017)		"develop a reliable measurement scale for quantifying and comparing attitudes towards personal data that can be incorporated into cybersecurity behavioural research model" 1st step towards establishing empirical evidence for dimensions of personal data attitudes. It also adds a sig benchmark to BOK re: understanding & modelling IT users' security behavior	six constructs of individuals' attitude towards personal data: protective behaviour, privacy concerns, cost-benefit, awareness, responsibility and security. Includes instrument question detail	exploratory and confirmatory factor analyses and MANOVA n=247		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Aivazpour & Rao (2018)	RScB	Replicated study of Hadlington (2017)	- Internet addiction is a significant predictor of RScB - positive attitude re: CySec in business are negatively related to RScB - both attentional and motor impulsiveness are significant positive predictors of RScB - non-planning was a significant negative predictor of RScB Overall, sufficient basis is supported to pursue research on effects of impulsiveness on RScB.	correlational study Amazon mechanical Turk used to recruit participants n= 245 adults in the US	- impulsiveness (ABIS) - Internet use levels (Online cognition scale, aka OCS) - Attitudes towards CySec & cybercrime in business (ATC-IB [instrument included])	Risky CySec behav (RScB, a 20-item scale partially derived from Security Behaviours Intentions Scale, aka SEBis)

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Albladi & Weir (2018)	PMT (for perception-related attributes)	re: social engineering vulnerabilities -- Proposes and validates a user-centric framework based on four perspectives (vulnerability areas): socio-psychological, habitual, socio-emotional, and perceptual	3 highest factors in vulnerability: Education (<-- surprising) Computer knowledge Security awareness (PMT)	11 CySec experts		
Barlette, Gundolf, & Jaouen (2015)	PMT	Characteristics of CEOs in small and med size enterprises re: Infosec behaviors. Uses PMT as basis,		Uses two sub-components: a) threat appraisal (3 sub-sub groups: cost and damage associated with the threat and vulnerability to the threat, and b) coping appraisal, also w/3-sub-sub groups: response efficacy, self-efficacy and response cost.		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Boehmer,LaRose, Rifon, Alhabash, & Cotten (2015)	pmt	builds on PMT to examine the role of a previously unexplored variable, personal responsibility, in protective behaviour of univ. students. Two studies are reported	new variable *personal responsibility* explained additional variance	Detailed survey instrument is included in article appendix n =565 n=206		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Bowen, Devarajan, & Stolfo (2012)		investigate new methods to measure, quantify and evaluate the security posture of human organizations especially in large enterprises	users can be trained to be cautious of suspicious looking emails, but sometimes it takes several iterations of testing.	Round 1 -- ident indivs from orig sample of 500 who were vulnerable to phishing attacks (via phishing emails). Successive versions of emails sent to susceptible indivs. 4 rounds total before all indivs identified phishing items Round 2 -- 2k indivs. Same patterns observed 4k participants over all. Divided into several stages		Dichotomous value: Click/no click

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Buchanan, Paine, Joinson, & Reips (2007)		Provide instrument to measure online privacy concerns and protection	Describes development and validation of three short scales measuring privacy-related attitudes (Privacy Concern) and behaviors (General Caution and Technical Protection)	UK based study. Three phases. Phase 1 (n=515) derived original questionnaire. Phase 2 validated from sample of Phase 1 using factor analysis. Phase 3 performed correlational analysis with previously established scales.		
Claar & Johnson (2012)	HBM PMT	understand why some indivs do not perceive a threat sufficient to prompt the adoption of computer security software.	Largest negative rels: Vulnerability and barriers preclude protective beh Largest positive rels: Self-efficacy and cues to action		HBM factors	computer security usage (CSU)

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Corradini & Nardelli (2018)	Risk and Human factors. "building a cyber security culture in the organizations cannot be tackled without people's involvement and the assessment of their risks knowledge"	Examine and profile CySec-related risk perception by corporate employees to formulate a CySec training regimen. Italian firm (authors were Italian too)	Most respondents felt ability to control a risk was the largest influencer of risk perception (parallels efficacy from PMT) Two most important considerations for management of cyber risk in an org were *risk analysis* and *training* *People* were rated the most important element to protect organizational security	N = 815 (730 first wave, 85 second wave) Five-level Likert-style survey for most q's. Others were "which is most important?" Findings are pitched by mean values of likert responses for each question (interpretation was intuitive with no stats analysis)		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Coventry, Briggs, Blythe, & Tran (2014)	PMT	Apply social and beh insights to CySec to answer: - What behs reduce CySec vulnerability? - Why do people not behave securely online? - What can behavioral theory tell us about influencing behaviour? - What is the role of comm campaigns in changing behaviour? - How can interventions be designed to motivate CySec?	Communications campaigns can help get messages out but also have: - Concurrent community pgms - Policy and law changes - Readily available prods & svcs to support the target behs - Tailored msgs for specific audiences. - Msgs being built-in to many different delivery mechanisms - Role models and champions exhibiting the behs Sec practices should default to 'on' and opt-out, not opt-in	Rapid Evidence Assessment of the literature on CySec Beh and interventions. brief email Delphi with experts in Cyber Security. We used this study to get expert opinion on the conclusions we had drawn from the literature.		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Coventry, Jeske, & Briggs (2014)		Demonstrate benefit of refining user profiles to gain behavioral insight, - cluster users on privacy and risk perception by those who were a) highly concerned and risk-sensitive; b)unconcerned but risk-aware; and c) semi- concerned but less risk-aware. Using these clusters, able to explain diff patterns of self-reported behaviours re: tech & general caution.	Hi concern and risk aware were most cautious. Mod concern but less risk aware #2 Unconcerned but risk aware #3	Cluster analysis and ANCOVA	Concern (Hi med low) Risk awareness (hi med low)	- Tech caution (self-reported) - General caution (self-reported)
Egelman & Peer (2015)	SeBIS	Develop and validate the security intentions behavior scale (SeBIS)	Validated and reliable. 24Q's. See table 5 in the work for instrument	Factor analysis n= 354, recruited via Amazon mechanical turk		
Egelman, Harbach, & Peer (2016)	SeBIS	Validation of the SeBIS behav intentions scale instrument	further validation of SeBIS	n=359 Another Amazon Mech Turk sample		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Fagan, Albayram, Khan, & Buck (2017).		explore factors which determine PW manager usage by computer users	users' of pw mgrs noted convenience and usefulness as the main reasons behind using the tool, rather than security gains. 'non-users' noted security concerns as main reason for nonuse. (lack of self-efficacy) Note: Work does not examine PW complexity verses pw mgr use – a critical missing item	n = 248 137 users and 111 hon-users		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Goel, Williams, & Dincelli (2017)	Attract/avoidance theory (contextualized messaging intended to induce a) desire for gain or b) fear of loss	Explore various characteristics of phishing emails as determinants of whether IT end-users ignore or are deceived by the phishing message	A 2-dimensional grid defined classes of phishing emails to university students. Opening the email routed participants to the survey to analyze traits. This approach appears to implement insights from Coventry, Briggs, Blythe, and Tran (2014), although that work is not cited by Goel et al. (2017).	7,225 students, with 3,513 females and 3,712 males -; large US research university	Eight bait flavors,(i.e., gift card, iPad, antivirus software, volunteer, etc.) each was cross referenced by 3 variables: Gain/loss, general motive (acquisition, defense, social), and contextualization (high/low). Four groups: Soc sci, STEM, humanities and business.	Dichotomous value: Click/no click

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Gratian, Bandi, Cukier, Dykstra, & Ginter (2017)		Examine risk-taking prefs, decision-making styles, demographics, and personality traits that influence security behav intent, securing devices, creating PWss, general awareness, and tool updating. Extends Egelman and Peer (2015)	Predictors weakest for dev securement (5% of variance) Predictors strongest for proactive awareness -- 22.8% of variance	multiple regression 369 students, faculty, and staff at a large public university	demographic factors, personality traits, risk-taking preferences, and decision-making styles	CySec Behavior intentions (SeBIS) -- 30 potential behs on four subscales: - Dev securement - Passwd generation - proactive awareness - Updating

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Hadlington & Murphy (2018)	RScB	Investigate how engaging in media multitasking (MMT) and the experience of everyday cognitive failures impact on the individual's engagement in risky cybersecurity behaviors (RScB)	- sig diff between heavy media multitaskers (HMM), avg media multitaskers (AMM), and light media multitaskers (LMM) re: RScB - HMM demonstrated more frequent risky behaviors than LMM or AMM. HMM reported more cognitive failures in everyday life than LMM grp. **regression showed everyday cognitive failures and MMT were sig predictors for RScB**	online survey of three scales Regression used to measure predictive qualities of IVs 144 participants (32 males, 112 females)	1) inventory of weekly MMT, and 2) a measure of everyday cognitive failures	RScB

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Hadlington (2017)	RScB SeBIS	explore relationship between risky cybersecurity behaviours, attitudes towards cybersecurity in a business environment, Internet addiction, and impulsiveness	- Internet addiction sig predictor of RScB - positive attitude re: CySec in business **negatively** related to RScB - both attentional and motor impulsiveness significant positive predictors of RScB - non-planning was a significant negative predictor of RScB	correlational study n= 515 adults in the UK	- implusiveness (ABIS) - Internet use levels (Online cognition scale, aka OCS) - Attitudes towards CySec & cybercrime in business (ATC-IB [instrument included])	Risky CySec behavior (RScB, a 20-item scale partially derived from Security Behaviours Intentions Scale, aka SEBis)
Herath, Chen, Wang, Banjara, Wilbur, & Rao (2014)	PMT TTAT TAM	derive a predictability model for organizational adoption of email authentication security services to mitigate risk of CySec threats which use email as an attack vector.	Top impact: External coping mech (Attitude): 0.49 usefulness Responsiveness Priv concerns Ease of use 2nd greatest impact: Threat appraisal(risk): 0.30 Lowest impact: Self-efficacy: -0.17	Partial least squares 134 adults USA Instruments included in appendices	see findings	Intention to adopt email authentication service

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Jansen & Schaik (2017)	PMT RAA (reasoned action approach -- precursor to PMT)	compare 3 social cognitive models re: intentions of precautionary online behaviour. PMT, RAA and hybrid	PMT: Response efficacy most impactful on precautionary behavior (0.49) [nearly tripled perceived sev weighting] Self-efficacy #2 (0.30) RAA: Attitude #1 (0.36) Self-efficacy #2 (0.27), Locus of ctrl #3 (0.25) Hybrid: Response efficacy #1 (0.30) Attitude #2 (0.22), Self-efficacy #3 (0.21),	online survey and analyzed using partial least squares path modelling method. 1,200 Dutch users of online banking	Factors from various models	Precautionary online beh: (1) keep sec codes secret; (2) ensure debit card is not used by others; (3) properly secure devices used for online banking (4) check bank account regularly; and (5) report incidents directly to bank.

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Mamonov & Benbunan-Fich (2018)	PMT		Computer users exposed to news stories about corporate security breaches limit the disclosure of sensitive personal information and choose stronger passwords.	Partial least squares 400 US participants recruited from Amazon Mechanical Turk (AMT-- online labor market for micro tasks)	Primary IV awareness of infosec thrts Secondary IVs Age Gender Education Privacy concerns	Password strength Refusal to disclose info

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
McCormac, Calic, Butavicius, Parsons, Zwaans, & Pattinson (2017)	HAIS-Q	examine reliability of the HAIS-Q, including test-retest reliability and internal consistency	Implies orgs can use HAIS-Q to measure a) current state of employee infosec awareness b) effectiveness and impacts of training interventions, infosec awareness programs & campaigns, and c) influence of cultural changes and the effect of security incidents. Reliability testing on the prelim over-claiming items (designed to identify indivs who provide socially desirable responses) needs greater robustness -- further development rqd and recommended. Retest scores increased < 10% from 1st iteration	two iterations of the HAIS-Q and the over-claiming items, approximately 4 weeks apart. Cronbach 197 working Australians following 2 iterations and removal of 10 outliers		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
McCormac, Zwaans, Parsons, Calic, Butavicius, & Pattinson (2017)	HAIS-Q	examine relationship between individuals' Infosec Awareness (ISA) and individual differences variables, namely age, gender, personality and risk-taking propensity.	positive relationships between: - conscientiousness and ISA, - agreeableness & ISA, & - openness and ISA. - negative correlation between risk-taking propensity and ISA	two-stage hierarchical multiple regression, based on correlations, extroversion was not included in the regression. age and gender were control vars (both found sig at 1st stage) 505 (286 females and 219 males) working Australians	Big Five Inventory (BFI) Risk Aversiveness scale	Indiv knowledge, attitude and behaviour re: InfoSec measured via 63 statements, five-point Likert scale, rated from 1 'Strongly Disagree' to 5 'Strongly Agree'.

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Ovelgönne, Dumitraş, Prakash, Subrahmanian, & Wang (2017)		investigate relationships between computer user behavior and cyber attacks against their personal computers.	gamers: 83% more malware attacks than non-gamers, professionals: 33% more malware attacks than non-pro users. Significantly more malware present on SW development hosts is than non SW dev hosts. For SW-dev hosts, # of binaries linked to the # attacks: For the other categories of users, the link between the # binaries and cyber attack risk is weaker, but still statistically significant.	users classified into 4 categories (gamers, professionals, software developers, and others, plus a fifth category comprising everyone) 35 possible combinations (5 user categories times 7 features), analyzed relationship between each of the seven features and the DV Users: gamers, pros, SW devs, Others, All	paired attributes: user type * feature type (35 in all) Features: - # of binaries present - % of low prevalence binaries - % of hi prevalence binaries - % of unique binaries - % of unsigned binaries - % of downloaded binaries - travel history	the number of attempted malware attacks detected by Symantec product

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Parekh et al. (2018)		Identify key CySec elements for 1) 1st year cybersec coursework (CCI) and 2) BOK topics for new professionals in CySec (CCA)	38 CCI topics and 53 CCA topics. See article for details if needed	Delphi studies (2)		
Parsons, Calic, Pattinson, Butavicius, McCormac, & Zwaans (2017)	HAIS-Q	Validation of the HAIS-Q instrument	Participants who scored higher on HAIS-Q were less susceptible to phishing emails	Factor Analysis -- 2 samples, first was Australian university undergrads N1 =112, 2nd to working Australians, N2=505	HAIS-Q Factors	Susceptibility to phishing email on testbed

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Parsons, McCormac, Butavicius, Pattinson, & Jerram (2013)	HAIS-Q	two aims: 1) outline the conceptual dev of the HAIS-Q, including validity and reliability testing. 2) examine rel betw knowledge of policy & procs, procedures, attitude towards policy and procedures and behavior when using a work computer.	knowledge of policy and procedures had a stronger influence on attitude towards policy and procedure than on self reported behaviour	500 Australian employees		self reported Behavior has seven focus areas: Password management Email use Internet use Social networking site (SNS) use Incident reporting Mobile computing Information handling

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Pattinson, Butavicius, Parsons, McCormac, & Calic (2017)	HAIS-Q (subset)	Two aims: 1)confirm a specific bank's employees were generally more information security-aware than employees in other Australian industries 2) identify the major factors that contributed to this bank's high levels of information security awareness	- Mean lvl of ISA at this bank consistently 20% higher than general workforce participants in all focus areas and overall. - no sig diffs between the ISA scores for those who received more frequent training compared to those who received less frequent training. **This result suggests that the frequency of training is not a contributing factor to an employee's level of ISA.**	used subset of HAIS-Q (Self-reported behavior module NOT included) Two waves --Two waves –Wave 1 198 bank employees in australia (same org for all) Wave 2: general workforce (n=500) to compare infosec awareness between bank and general population		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Rajivan, Moriano, Kelley, & Camp (2017)	Security SRK	identify factors that determine computer and end-user security expertise Undertaken on research grant by US Army	identified four factors that constitute security expertise in end-users: - basic computer skills, - advanced computer skills, - security knowledge and - advanced security skills posits security expertise instrument for end-users should measure three cognitive dimensions: security skills, rules and knowledge.	EFA and cluster analysis on survey instrument outcomes. Mixed method: (Instrument included as table 1 of cited work) and qualitative q's Security expertise represented by qualitative q's (2) 898 participants -- wide range of populations		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Ritzman & Kahle-Piasecki (2016)		overview of org interventions to supplement tech activity to provide system protection for infosec	<u>Intervention types</u> - policy - communication - training - culture - classifying data Interesting contrast Under training activity betw *security related stress* (SRS) and *technology related stress.*-- "Any performance improvement intervention designed to address information security must take SRS into consideration to be effective." (p.19)			

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Samhan (2017)	TTAT	Test the TTAT model in a healthcare env to investigate health information technology (HIT) avoidance behaviors when used in unsecure environments	Typical relationships re: TTAT factors and avoidance motivation (AM). AM in turn demonstrates a weight of 0.43 re: avoidance behavior	Confirmatory Factor Analysis from survey instrument (from Liang & Xue, 2010)	TTAT factors	AVBH from Liang and Xue (2010): Variables: - Avoid using HIT outside work - use malware protection SW - update anti-malware regularly

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Shepard & Archibald (2017)		examine relationship between end-user-security behaviour, and the use of affective feedback to educate end-users. Considers the link between categorical information users reveal about themselves online, and the information users believe, or report that they have revealed online.	confirmed disparity between info revealed, and what users think they revealed, --> deficit in security awareness. Affective feedback changes (intervention results) were mixed			

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Sherman et al. (2018)		Follow on to Parekh et al. (2018) -- case study re: formulation of training content for CySec pros	six scenarios: 1. whether to trust sender of an e-mail, and deciding how to send information securely over the Internet; 2. Analyzing security of drone pkg delivery 3. mitigate risk of injection attacks; 4. Control flow of info across nw boundaries, and handling potentially dangerous digital objects; 5. Designing a system that uses public-key cryptography to provide auth without secrecy, and 6. Devising attacks involving physical security and social engineering.			

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Stanciu & Tinca (2017)		Literature review to identify top issues in cybersec	Most prominent threats: denial of service (DoS) Ransomware Zero-day attacks	9 item survey administered verbally 14 CIOs in Romania 2 in banking 12 in private companies		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Tsai, Jiang, Alhabash, LaRose, Rifon, & Cotten (2016)	PMT TTAT	cross-sectional survey was conducted to examine how classical and new PMT factors predicted security intentions	coping appraisal variables were the strongest predictors of online safety intentions, (especially habit strength, response efficacy, and personal responsibility. Threat severity also a sig predictor. Added factors (i.e., prior experiences, subjective norms, habit strength, perceived security support, and personal responsibility) into the conventional PMT model increased the model's explanatory power by 15%.	cross-sectional survey (*N* = 988) of Amazon Mechanical Turk (MTurk) users was conducted to examine how classical and new PMT factors predicted security intentions n = 988		

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
van Schaik et al. (2017)	control was a significant predictor of precautionary behaviour	examined a set of 16 security hazards on the Internet and two comparisons in 436 UK- and US students, measuring perceptions of risk and other risk dimensions	perceived risk highest for Id theft, keylogger, cyber-bullying and social engineering. significant predictors of perceived risk were voluntariness, immediacy, catastrophic potential, dread, severity of consequences and control, as well as Internet experience & frequency of Internet use Also, control = significant predictor of precautionary behavior.	436 UK and USA university students (336 female, 100 male	CySec risk perception some aspects of PMT/TTAT although neither are named	expanded the Computer Security Usage scale (CSU; Claar & Johnson, 2012) to five items, with a 7-point Likert scale re: precautionary CySec behav. : anti-virus, firewall software, antispyware software, software updates and security updates.

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
Vishwanath, Harrison, & Ng (2016)	1) trust is a poor predictor of detecting deception b/c trust desensitizes individuals to deception cues. i.e., interpersonal deception research found when individuals trust a partners, they tend to become blind toward partner's lies (McCornack & Parks, 1986). Trust's 'darker cousin' was used instead -- deception. Trust: *degree of uncertainty one has when interacting with a particular stimulus*	Build/evaluate a model that accounts for the -cognitive, -preconscious, and -automatic processes that may lead to phishing deception.	<u>Three most impactful relationships were</u> - Systematic processing * suspicion, - Cyber-risk beliefs * heuristic processing (negative relationship), and - Deficient self-regulation * email habits (i.e. anxiety driving frequent access to email) *Heuristic processing* is more intuitive while *systematic processing* is thoughtful and reflective	The suspicion, cognition, and automaticity model (SCAM) was tested using two experimental studies where subjects were exposed to different types of email-based phishing attacks		suspicion

Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
White (2015)			Similar to White et al. (2017) -- Awareness of the problem domain was associated with increases in incidents, likely due to increased ability to recognize incidents from educ/training computer professionals and technicians have higher security incidents, higher prior experience, and higher preventive behavior.	Survey based (instrument included in pub) ANOVA and Correlation n = 945 458 male 487 female	1. Preventive behavior 2. Security-related educ 3. Job characteristics - nonusers, - users, and - computer professionals/ technicians.	– Security Incidents - quant var (Sec_Inc). This # attacks on the home computer last 3 years. Security Prior Experience - Qual var (Prior_Exp). prior experiences with security issues and attacks on the home computer for the past 3 years.

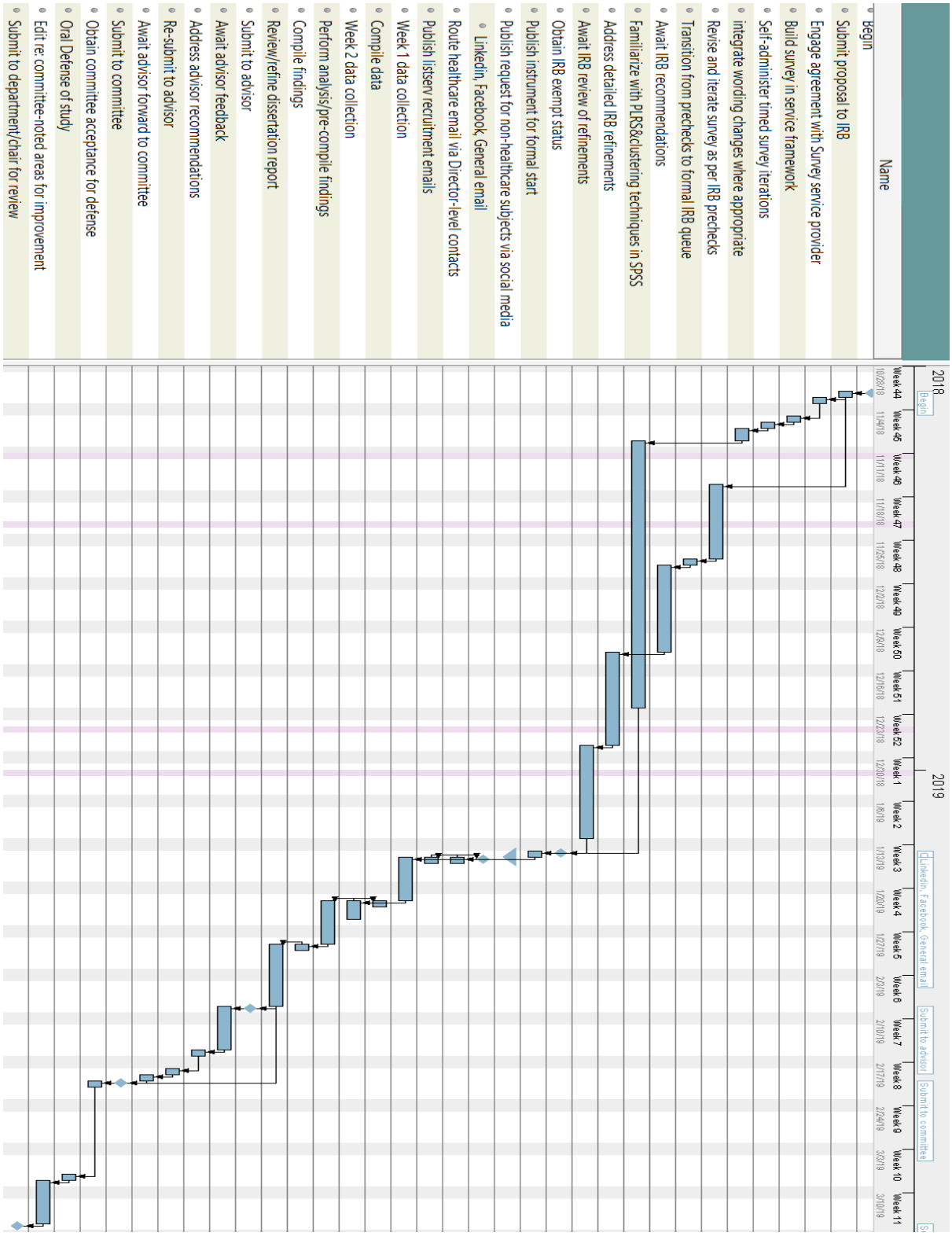
Cite	Relevant Theories/Concepts	Purpose/Intent	Findings	Methods/Sample	IVs	DVs
White, Ekin, & Visinescu (2017)	PMT, HBM (Health belief model is pred of PMT)	Role of protective behavior on home computer security incidents	Awareness of the problem domain was associated with increases in incidents, likely due to increased ability to recognize incidents from educ/training	Survey based (instrument included in pub) Analyzed using partial least squares 945 usable responses -- adults	Perceived barriers of protective behavior, Self-efficacy Cues to action	Security incidents (12 types, Likert scale answers)
Workman, Bommer, & Straub (2008)	PMT	Explore PMT factor impacts on omissive behaviors (self reported and observed)	Perceived severity had strongest relationship to omissive behavior. -- nearly 2x efficacy factors. IV associations with self-reported behavior ((subjective DV) were generally stronger than associations between IVs and the 'objective' DVs	n=588 employees of large US IT firm		Omissive behaviors (i.e., failures to act)

APPENDIX B: BASELINE TTAT INSTRUMENT – LIANG AND XUE (2010)

Perceived Susceptibility (1 = strongly disagree, 7 = strongly agree)
It is extremely likely that my computer will be infected by spyware in the future
My chances of getting spyware are great
There is a good possibility that my computer will have spyware
I feel spyware will infect my computer in the future
It is extremely likely that spyware will infect my computer
Perceived Severity (1 = innocuous, 7 = extremely devastating)
Spyware would steal my personal information from my computer without my knowledge
Spyware would invade my privacy
My personal information collected by spyware could be misused by cyber criminals
Spyware could record my internet activities and send it to unknown parties
My personal information collected by spyware could subject to unauthorized secondary use
My personal information collected by spyware could be used to commit crimes against me
Spyware would slow down my internet connection
Spyware would make my computer run more slowly
Spyware would cause system crash on my computer from time to time
Spyware would affect some of my computer programs and make them difficult to use
Perceived Threat (1 = strongly disagree, 7 = strongly agree)
Spyware poses a threat to me
The trouble caused by spyware threatens me
Spyware is a danger to my computer
It is dreadful if my computer is infected by spyware
It is risky to use my computer if it has spyware
Perceived Safeguard Effectiveness (1 = strongly disagree, 7 = strongly agree)
Anti-spyware software would be useful for detecting and removing spyware
Anti-spyware software would increase my performance in protecting my computer from spyware
Anti-spyware software would enable me to search and remove spyware on my computer faster
Anti-spyware software would enhance my effectiveness in searching and removing spyware on my computer
Anti-spyware software would make it easier to search and remove spyware on my computer
Anti-spyware software would increase my productivity in searching and removing spyware on my computer

Perceived Safeguard Cost (1 = strongly disagree, 7 = strongly agree)
I don't have anti-spyware on my PC because…
… I don't know how to get an anti-spyware software
… Anti-spyware software may cause problems to other programs on my computer
… Installing anti-spyware software is too much trouble
Self-Efficacy (1 = not at all confident, 10 = totally confident)
I could successfully install and use anti-spyware software if…
… there was no one around to tell me what to do
… I had never used a package like it before
… I had only the software manuals for reference
… I had seen someone else doing it before trying it myself
… I could call someone for help if I got stuck
… someone else helped me get started
…I had a lot of time to complete the job
… I had just the built-in help facility for assistance
… someone showed me how to do it first
… I had used similar packages like this one before to do the job
Avoidance Motivation (1 = strongly disagree, 7 = strongly agree)
I intend to use anti-spyware software to avoid spyware
I predict I would use anti-spyware software to avoid spyware
I plan to use anti-spyware software to avoid spyware
Avoidance Behavior (1 = strongly disagree, 7 = strongly agree)
I run anti-spyware software regularly to remove spyware from my computer
I update my anti-spyware software regularly

APPENDIX C: STUDY TIMELINE DETAIL



APPENDIX D: INFORMED CONSENT

4 January 2019

TECHNOLOGY THREAT AVOIDANCE PREDICTION OF RISKY CYBERSECURITY BEHAVIOR

You are being invited to participate in a research study that explores the impact of human factors-related concerns in workplace cybersecurity. This study is being conducted by Andrew R. Gillam and W. Tad Foster, from the College of Technology at Indiana State University. The study is being conducted as part of a doctoral dissertation.

There are no known risks if you decide to participate in this research study. There are no costs to you for participating in the study. The information you provide will allow researchers to explore factors of technology threat avoidance decision-making as predictors of self-reported risky cybersecurity behaviors by adults in the US workplace. The questionnaire will take about 12 minutes to complete. The information collected may not benefit you directly, but the information learned in this study should provide more general benefits.

This survey is an anonymous, web-based survey. Do not submit your name or any other identifying information while completing it. Anonymity will be provided by avoiding collection of participant internet protocol (IP) addresses. However, absolute anonymity cannot be guaranteed over the Internet. No one will be able to identify you or your answers, and no one will know whether or not you participated in the study. Individuals from the Institutional Review Board may inspect these records. Should the data be published, no individual information will be disclosed.

Your participation in this study is voluntary. If you do not wish to participate you may close your browser window. By completing and proceeding past this screen, you are voluntarily agreeing to participate. You are free to decline to answer any particular question you do not wish to answer for any reason.

If you have any questions about the study, please contact the principal investigator, Andrew R. Gillam by mail at 6208 Mountain Villa Dr., Austin, TX 78731, by phone at (512) 921-0593, or by email at agillam@sycamores.indstate.edu or the faculty sponsor, W. Tad Foster by mail at TC302H, 101 N 6th St, Terre Haute, IN 47809, by phone at (812) 237-4508, or by e-mail at Tad.Foster@indstate.edu

If you have any questions about your rights as a research subject or if you feel you've been placed at risk, you may contact the Indiana State University Institutional Review Board (IRB) by mail at Indiana State University, Office of Sponsored Programs, Terre Haute, IN, 47809, by phone at (812) 237-3088, or by e-mail at irb@indstate.edu.

IRBNet #: 1345925-2
Approved Date: January 14, 2019
Expiration Date:
Indiana State University Institutional Review Board

APPENDIX E: STUDY INSTRUMENT

Start of Block: General/Demographic

Q2 The first block of questions ask for general information. Please choose the answer for each question which most closely describes you.

Q3 What is your age group?

- 19 or younger
- 20-29
- 30-39
- 40-49
- 50-59
- 60-69
- 70-79
- 80-89

Q4 What is your highest level of formal education?

- Less than high school
- High school graduate
- Some college
- 2 year degree
- 4 year degree
- Graduate or Professional degree
- Doctorate

Q5 Your gender

- Male
- Female

Q6 What industry do you work in?

- ○ Technology products/services
- ○ Automotive
- ○ Healthcare
- ○ Legal
- ○ Hospitality
- ○ Retail
- ○ Education
- ○ Government
- ○ Military/Defense
- ○ Financial
- ○ Other

Q7 How many people work for your employer?

- ○ 1-4 employees
- ○ 5-9 employees
- ○ 10-19 employees
- ○ 20-49 employees
- ○ 50-99 employees
- ○ 100-249 employees
- ○ 250-499 employees
- ○ 500-999 employees
- ○ 1,000 or more employees

Q8 How many years have you worked in your industry?

- 0-4 years
- 5-9 years
- 10-14 years
- 15-19 years
- 20-24 years
- 25-29 years
- 30-34 years
- 35-39 years
- 40-44 years
- 45-49 years

End of Block: General/Demographic

Start of Block: PersonalTech

Q9 This block of questions asks about your use of cyber protection products on computers or mobile devices that you own.

Q10 Do you personally own a computer or a mobile device which connects to the internet?

- Yes
- No

Skip To: End of Block If Do you personally own a computer or a mobile device which connects to the internet? = No

Q11 Do you use virus protection software on computers or mobile devices you own?

- Yes
- No
- I do not know

Q12 Do you use internet firewall software on computers or mobile devices you own?

- Yes
- No
- I do not know

Q13 Do you use virtual private networking (VPN) software on computers or mobile devices you own?

- Yes
- No
- I do not know

Q14 Do you use encryption software to protect personal information on computers or mobile devices you own?

- Yes
- No
- I do not know

Q15 Do you routinely remove web browsing information from computers or mobile devices you own?

- Yes
- No
- I do not know

End of Block: PersonalTech

Start of Block: Work and RScB

All of the remaining questions in the survey pertain to your use of employer-owned computing equipment you use to perform your work.

Q17 Does/did your employer own the computer or mobile device you primarily use(d) to perform your work?

- Yes
- No

Skip To: End of Survey If Does your employer own the computer or mobile device you primarily use to perform your work? = No

Q18 To respond to this series of questions, indicate how often you do the described activities while performing your work

Q19 While working, how frequently do you share passwords with friends or colleagues?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Q20 While working, how frequently do you use or create simple passwords?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Q21 While working, how frequently do you use the same password for multiple websites?

- ○ Never
- ○ Once per year
- ○ Once every six months
- ○ Once every few months
- ○ Once every few weeks
- ○ Weekly
- ○ Daily

Q22 While working, how frequently do you use cloud storage to keep sensitive information?

- ○ Never
- ○ Once per year
- ○ Once every six months
- ○ Once every few months
- ○ Once every few weeks
- ○ Weekly
- ○ Daily

Q23 While working, how frequently do you enter payment information on websites that have no clear security information/certification (for example, no https indicator)?

- ○ Never
- ○ Once per year
- ○ Once every six months
- ○ Once every few months
- ○ Once every few weeks
- ○ Weekly
- ○ Daily

Q24 While working or while traveling for work, how frequently do you use free-to-access public Wi-Fi?

- ○ Never
- ○ Once per year
- ○ Once every six months
- ○ Once every few months
- ○ Once every few weeks
- ○ Weekly
- ○ Daily

Skip To: Q26 If While working or while traveling for work, how frequently do you use free-to-access public Wi-Fi? = Never

Q25 When using free-to-access public Wi-Fi, do you run virtual private networking (VPN) software?

- ○ Yes
- ○ No
- ○ I do not know

Q26 While working, how frequently do you rely on a trusted friend or colleague for advice on online-security?

- ○ Never
- ○ Once per year
- ○ Once every six months
- ○ Once every few months
- ○ Once every few weeks
- ○ Weekly
- ○ Daily

Note: Responses to this question were excluded from RScB totals following confirmatory factor analysis.

Q27 While working, how frequently do you download free anti-virus software from an unfamiliar provider?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Note: Responses to this question were excluded from RScB totals following confirmatory factor analysis.

Q28 While working, how frequently do you disable the anti-virus on your work computer so you can download information from websites?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Q29 While working, how frequently do you use a USB/flash drive which you personally own?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Q30 While working, how frequently do you check that software for your electronic device is up-to-date?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Note: Responses to this question were excluded from RScB totals following confirmatory factor analysis.

Q31 While working, how frequently do you download digital media (music, films, games) from unlicensed sources?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Q32 While working, how frequently do you share your current location on social media?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Q33 While working, how often do you accept friend requests on social media because you recognize the other person's photo?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Q34 While working, how frequently do you click on web links contained in unsolicited emails from unfamiliar sources?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Q35 While working, how frequently do you send personal information to unfamiliar parties or people over the Internet?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Q36 While working, how frequently do you click on web links contained in email from trusted friends or work colleagues?

- Never
- Once per year
- Once every six months
- Once every few months
- Once every few weeks
- Weekly
- Daily

Q37 How frequently do you download non-authenticated material from websites to your work computer without checking its authenticity?

- ○ Never
- ○ Once per year
- ○ Once every six months
- ○ Once every few months
- ○ Once every few weeks
- ○ Weekly
- ○ Daily

Q38 How frequently do you store company information on personally-owned electronic devices such as smartphones, tablets, or laptops?

- ○ Never
- ○ Once per year
- ○ Once every six months
- ○ Once every few months
- ○ Once every few weeks
- ○ Weekly
- ○ Daily

End of Block: Work and RScB

Start of Block: Perceived Susceptibility

Q39 To respond to this series of questions, indicate how strongly you agree with each statement. Answer choices range from *strongly disagree* to *strongly agree*

Q40 It is extremely likely that my work computer will be infected by malware (viruses, etc) in the future

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q41 My chances of getting a malware infection on my work computer are great

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q42 Barack Obama was the first American president. Please select *strongly disagree* as the answer to this question

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q43 There is a good possibility that my work computer contains malware

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q44 There is a good possibility that my work computer will contain malware in the next 12 months

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

End of Block: Perceived Susceptibility

Start of Block: Perceived Severity

Q45 To respond to this series of questions, indicate how severe you consider the described scenario.
Answer choices range from *harmless* to *extremely devastating*.

Q46 A scenario where malware steals employer information for criminal activity

- Harmless
- Somewhat concerning
- Concerning
- Serious
- Very serious
- Devastating
- Extremely devastating

Q47 A scenario where malware would make my work computer run more slowly

- Harmless
- Somewhat concerning
- Concerning
- Serious
- Very serious
- Devastating
- Extremely devastating

Note: Responses to this question were excluded following confirmatory factor analysis

---

Q48 A scenario where malware would cause my work computer to crash from time to time

- Harmless
- Somewhat concerning
- Concerning
- Serious
- Very serious
- Devastating
- Extremely devastating

Note: Responses to this question were excluded following confirmatory factor analysis

---

Q49 A scenario where my work computer is shut down with payment demanded to reactivate it

- Harmless
- Somewhat concerning
- Concerning
- Serious
- Very serious
- Devastating
- Extremely devastating

Q50 A scenario where malware would reveal my passwords to online criminals

- Harmless
- Somewhat concerning
- Concerning
- Serious
- Very serious
- Devastating
- Extremely devastating

Q51 A scenario where malware would reveal employee information (social security numbers, salaries, etc.) to others

- Harmless
- Somewhat concerning
- Concerning
- Serious
- Very serious
- Devastating
- Extremely devastating

Q52 A scenario where malware would reveal proprietary information (trade secrets, financial information, etc) to others

- Harmless
- Somewhat concerning
- Concerning
- Serious
- Very serious
- Devastating
- Extremely devastating

End of Block: Perceived Severity

Start of Block: Perceived threat (5 q), perceived effectiveness (3 q), perceived cost (3 q)

Q53 To respond to this series of questions, indicate how strongly you agree with each statement. Answer choices range from *strongly disagree* to *strongly agree*.

Q54 Malware (software containing viruses, etc) poses a threat to me at work

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q55 The trouble caused by malware threatens me at work

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q56 Malware is a danger to the computer I use for work

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q57 It would be dreadful if my work computer were infected by malware

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Note: Responses to this question were excluded following confirmatory factor analysis

---

Q58 For quality assurance purposes please select *strongly agree* as the answer to this question

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q59 It is risky to use my work computer if it contains malware

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Note: Responses to this question were excluded following confirmatory factor analysis

---

Q60 Malware protection software would be useful for addressing malware problems on my work computer

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q61 Malware protection software would increase my performance in protecting my work computer from malware

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q62 Malware protection software would enable me to handle issues with malware faster on my work computer

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q63 I do not have malware protection software on my work computer because I don't know how to get malware protection software

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Q64 I do not have malware protection software on my work computer because malware protection software may cause problems with other programs on my computer

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Q65 I am happy with receiving a very large bill from the IRS. Please select *strongly disagree* as the answer to this question.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Q66 I do not have malware protection on my work computer because installing malware protection software is too much trouble.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

End of Block: Perceived threat (5 q), perceived effectiveness (3 q), perceived cost (3 q)

Start of Block: Self-efficacy

Q67 To respond to this series of questions, indicate your level of confidence in being able to perform the activity described by each question.

Q68 I could successfully install and use malware protection software without immediate help from others

	1 2 3 4 5 6 7 8 9 10
An answer of 1 means you are not at all confident and an answer of 10 means you are totally confident	

Q69 I could successfully install and use malware protection software using only the built-in help facility

	1 2 3 4 5 6 7 8 9 10
An answer of 1 means you are not at all confident and an answer of 10 means you are totally confident	

Q70 I could successfully install and use malware protection software if I could call someone for help

	1 2 3 4 5 6 7 8 9 10
An answer of 1 means you are not at all confident and an answer of 10 means you are totally confident	

Q71 I could successfully install and use malware protection software if I had a lot of time to do it

	1 2 3 4 5 6 7 8 9 10
An answer of 1 means you are not at all confident and an answer of 10 means you are totally confident	

End of Block: Self-efficacy

Start of Block: Avoidance motivation (3 questions), avoidance behavior (2 questions)

Q72 To respond to this series of questions, indicate how strongly you agree with each statement.
Answer choices range from *strongly disagree* to *strongly agree*

Q73 I intend to use malware protection software on my work computer to avoid malware infection

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Q74 If malware protection software were available I predict I would use it to avoid malware infection on my work computer

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q75 The United States of America consists of 10 states. Please select *strongly disagree* as the answer to this question.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q76 I plan to use malware protection software to avoid malware infection on my work computer

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q77 I run malware protection software regularly to prevent or remove malware on my work computer

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q78 I regularly update my malware protection software on my work computer

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

End of Block: Avoidance motivation (3 questions), avoidance behavior (2 questions)
End of Survey

APPENDIX F: RECRUITMENT EMAIL TO HEALTHCARE PROFESSIONALS

Greetings, Healthcare Professional.

Your participation is requested in a brief survey which explores the risk-taking behaviors of people who use information technology in the workplace. Health care professionals are a notable part of this population; their interactions with technology strongly influence and guide information systems development. This trend will continue in the coming decades.

The survey examines decision-making factors and their impacts on technology use. The survey is short, and uses single-click answers. No more than 12 minutes are needed to complete it. Most people complete it in a shorter period. The questionnaire consists of 68 questions, and is available online at https://indstate.qualtrics.com/jfe/form/SV_e2H2vHMmacQD8iN. A case-sensitive password is required for access. The password is ***ISUresearch.***

Participation is anonymous for all participants; investigators cannot determine who participates and who does not. No participation information is provided to any employer, no privacy-related information is captured, nor is information which reflects your personal identity. We ask that those who choose to participate only access the survey once, and that they use personal time to participate outside of work.

Please feel free to share this request by forwarding it to friends and co-workers. Qualified participants must be working or retired adults in the United States who routinely use(d) employer-owned computers and/or mobile devices to perform their work. They can access the questionnaire using the information provided above.

Thanks and best regards,

Andy

Andrew R. Gillam
Ph.D. Candidate
agillam@sycamores.indstate.edu
Indiana State University

APPENDIX G: GENERAL RECRUITMENT EMAIL

Greetings.

I am soliciting acquaintances, friends and colleagues to participate in an online survey; the survey findings will support my doctoral research. The survey explores various decision-making factors and their impacts on technology use by people in the US who use information technology at work. Participation is anonymous for all participants; investigators cannot determine who participates and who does not.

The survey is short, and uses single-click answers. No more than 12 minutes are needed to complete it. Most people complete it in a shorter period. The questionnaire consists of 68 questions, and is available online at https://indstate.qualtrics.com/jfe/form/SV_e2H2vHMmacQD8iN. A case-sensitive password is required for access. The password is ***ISUresearch*** .

We ask that those who choose to participate only access the survey once, and that they use personal time to participate outside of work.

Please feel free to share this request by forwarding to others. Qualified participants must be working or retired adults in the United States who routinely use(d) employer-owned computers and/or mobile devices to do their jobs. They can access the questionnaire using the information provided above.

Thanks and best regards,

Andy

Andrew R. Gillam
Ph.D. Candidate
agillam@sycamores.indstate.edu
Indiana State University

APPENDIX H: LETTER OF NOTIFICATION -- IRB EXEMPT STATUS

Indiana State University
More. From day one.

Institutional Review Board

Terre Haute, Indiana 47809
812-237-3088
Fax 812-237-3092

DATE:	January 14, 2019
TO:	Andrew Gillam
FROM:	Indiana State University Institutional Review Board
STUDY TITLE:	[1345925-2] Technology threat avoidance factors as predictors of risky cybersecurity behavior within the enterprise
SUBMISSION TYPE:	Revision
ACTION:	DETERMINATION OF EXEMPT STATUS
DECISION DATE:	January 14, 2019
REVIEW CATEGORY:	Exemption category #2

Thank you for your submission of Revision materials for this research study. The Indiana State University Institutional Review Board has determined this project is EXEMPT FROM IRB REVIEW according to federal regulations (45 CFR 46). You do not need to submit continuation requests or a completion report. Should you need to make modifications to your protocol or informed consent forms that do not fall within the exempt categories, you will have to reapply to the IRB for review of your modified study.

Internet Research: If you are using an internet platform to collect data on human subjects, although your study is exempt from IRB review, ISU has specific policies about internet research that you should follow to the best of your ability and capability. Please review Section L. on Internet Research in the IRB Policy Manual.

Informed Consent: All ISU faculty, staff, and students conducting human subjects research within the "exempt" category are still ethically bound to follow the basic ethical principles of the Belmont Report: 1) respect for persons; 2) beneficence; and 3) justice. These three principles are best reflected in the practice of obtaining informed consent.

If you have any questions, please contact Ryan Donlan within IRBNet by clicking on the study title on the "My Projects" screen and the "Send Project Mail" button on the left side of the "New Project Message" screen. I wish you well in completing your study.