

2021

Human Errors in Data Breaches: An Exploratory Configurational Analysis

Gabriel A. Cornejo

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd



Part of the [Computer Sciences Commons](#), and the [Library and Information Science Commons](#)

Share Feedback About This Item

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Human Errors in Data Breaches: An Exploratory Configurational
Analysis

by

Gabriel A. Cornejo

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Assurance

College of Computing and Engineering
Nova Southeastern University

2021

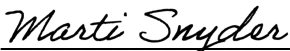
We hereby certify that this dissertation, submitted by Gabriel Cornejo conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



Yair Levy, Ph.D.
Chairperson of Dissertation Committee

11/2/21


Date



Martha M. Snyder, Ph.D.
Dissertation Committee Member

11/2/21

Date




Carla Curado, Ph.D.
Dissertation Committee Member

11/2/21

Date

Approved:



Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

11/2/21

Date

College of Computing and Engineering
Nova Southeastern University

2021

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Human Errors in Data Breaches: An Exploratory Configurational Analysis

by
Gabriel Cornejo

November 2021

Information Systems (IS) are critical for employee productivity and organizational success. Data breaches are on the rise—with thousands of data breaches accounting for billions of records breached and annual global cybersecurity costs projected to reach \$10.5 trillion by 2025. A data breach is the unauthorized disclosure of sensitive information—and can be achieved intentionally or unintentionally. Significant causes of data breaches are hacking and human error; in some estimates, human error accounted for about a quarter of all data breaches in 2018. Furthermore, the significance of human error on data breaches is largely underrepresented, as hackers often capitalize on organizational users' human errors resulting in the compromise of systems or information. The research problem that this study addressed is that organizational data breaches caused by human error are both costly and have the most significant impact on Personally Identifiable Information (PII) breaches. Human error types can be classified in three categories—Skill-Based Error (SBE), Rule-Based Mistakes (RBM), and Knowledge-Based Mistakes (KBM)—tied to the associated levels of human performance. The various circumstantial and contextual factors that influence human performance to cause or contribute to human error are called Performance Influencing Factors (PIF). These PIFs have been examined in the safety literature and most notably in Human Reliability Analysis (HRA) applications. The list of PIFs is context specific and had yet to be comprehensively established in the cybersecurity literature—a significant research gap.

The main goal of this research study was to employ configurational analysis—specifically, Fuzzy-Set Qualitative Analysis (fsQCA)—to empirically assess the conjunctural causal relationship of internal (individual) and external (organizational and contextual) Cybersecurity Performance Influencing Factors (CS-PIFs) leading to Cybersecurity Human Error (CS-HE) (SBE, RBM, and KBM) that resulted in the largest data breaches across multiple organization types from 2007 to 2019 in the United States (US). Feedback was solicited from 31 Cybersecurity Subject Matter Experts (SME), and they identified 1st order CS-PIFs and validated the following 2nd order CS-PIFs: organizational cybersecurity; cybersecurity policies and procedures; cybersecurity education, training, and awareness; ergonomics; cybersecurity knowledge, skills, and abilities; and employee cybersecurity fitness for duty. Utilizing data collected from 102 data breach cases, this research found that multiple combinations, or causal recipes, of

CS-PIFs led to certain CS-HEs, that resulted in data breaches. Specifically, seven of the 36 fsQCA models had solution consistencies that exceeded the minimum threshold of 0.80, thereby providing argument for the contextual nature of CS-PIFs, CS-HE, and data breaches. Two additional findings were also discovered—five sufficient configurations were present in two models, and the absence of strong cybersecurity knowledge, skills, and abilities is a necessary condition for all cybersecurity human error outcomes in the observed cases.

Acknowledgements

To my dissertation advisor, Dr. Yair Levy: I am forever grateful for the extensive time and support you invested in me and in this research. You are an incredible mentor and intellectual, that I admire and hope to one day, come close to emulating. Thank you! I'd like to also thank Dr. Carla Curado and Dr. Martha "Marti" Snyder for your expert guidance and leadership. You both were instrumental in numerous revisions of this research and in the final product. Thank you for your hard work and dedication.

I'd like to thank my brothers and sisters, and extended family for your love and support. I thank my strong mother Blanca who taught me to appreciate struggle and hard work, and for my late and beautiful grandmother Maria, who taught me love and respect. I dedicate this to you both.

To my wife, Arica: thank you for your incredible love and sacrifice throughout this process. I owe much of my successes to you, and I will make the time invested worthwhile. I love you! To our daughters, Alena and Caia: you have unlimited potential. Your happiness is my happiness, and I will support you in your life goals and in whatever makes you happy. I will be with you every step of the way.

Table of Contents

Abstract	iii
Acknowledgements	v
List of Tables	x
List of Figures	xi

Chapters

1. Introduction 1	
Background	1
Problem Statement	3
Dissertation Goal	7
Research Questions	10
Relevance and Significance	11
Relevance	11
Significance	15
Barriers and Issues	17
Assumptions, Limitations, and Delimitations	17
Assumptions	17
Limitations	17
Delimitations	18
Definition of Terms	19
List of Acronyms	24
Summary	25
2. Review of the Literature 27	
Introduction	27
Data Breaches	28
Information Systems and Cybersecurity	28
Data Breaches	28
Human Error in Data Breaches	29
Human Error Data Breach Examples	30
Human Error	32
Introduction	32
Human Performance	33
Human Errors and Violations	34
GEMS in Cybersecurity	35
Human Reliability Analysis	37
Performance Influencing Factors	40
Organizational Cybersecurity	44
Definition	44
Organizational Control	47
Organizational Cybersecurity CS-PIF Interaction	48

Cybersecurity Policies and Procedures	52
Definition	52
Compliance	53
Cybersecurity Education, Training, and Awareness	57
Definition	57
Cybersecurity Education	59
Cybersecurity Training	59
Cybersecurity Awareness	60
Cybersecurity Knowledge, Skills, and Abilities	63
Definition	63
Employee Cybersecurity Awareness	64
Employee Cybersecurity Skill and Employee Cybersecurity Competency	64
Cybersecurity Self-Efficacy	65
Employee Cybersecurity Fitness for Duty	69
Definition	69
Stress	70
Fatigue	70
Situation Awareness	71
Emotion	71
Motivation	71
Ergonomics	74
Definition	74
Human-Computer Interaction	74
Macroergonomics	75
PIF Relationship	78
Summary of What is Known and Unknown in the Research Literature	79
3. Methodology	81
Overview of Research Design	81
Phase 1: Instrument Development	82
CS-PIF Identification	83
CS-PIF Validation	84
Expert Panel	84
Phase 2: Fuzzy-set Qualitative Comparative Analysis	85
Overview	85
Process	86
Case Selection	87
Variable Specification	87
Data Matrix	88
Truth Table	88
Interpreting Results	89
Reliability and Validity	89
External Validity	90
Internal Validity and Measurement Validity	91
Population and Sample	91
Data Analysis	92

Pre-Analysis Data Screening	92
Data Analysis	93
Resource Requirements	93
Summary	93

4. Results	96
Overview	96
Instrument Development (Phase 1)	96
Demographic Analysis	97
Identification of Common (1 st Order) Cybersecurity Performance Influencing Factors	99
External 1 st Order CS-PIFs	99
Internal 1 st Order CS-PIFs	100
Validation of Categorization of Higher Order (2 nd Order) CS-PIFs	101
External 2 nd Order CS-PIFs	101
Internal 2 nd Order CS-PIFs	102
Results of the Instrument Development (Phase 1)	103
Fuzzy-set Qualitative Comparative Analysis (Phase 2)	105
Case Selection	105
Variable Specification	108
Set Membership Calibration	109
Data Matrix	110
Analysis of Necessary Conditions	113
Truth Table	114
Interpreting Results	115
Solutions of Sufficient Configurations of Conditions	117
RQ4b RBM: System Misconfiguration Caused Breaches	118
RQ4c SBE: Social Engineering Caused Breaches	118
RQ4d KBM: Poor Cybersecurity Hygiene Caused Breaches	119
RQ5a1 KBM: All Business Organizations	120
RQ5a2 RBM: Education/Non-Profit Organizations	121
RQ5a3 KBM: Government Organizations	121
RQ5b3 KBM: Large Organizations	122
Solutions Summary	123
Summary	124
5. Conclusions, Discussions, Implications, Recommendations, and Summary	126
Conclusions	126
Discussion	129
Implications	130
Recommendations	131
Summary	133

Appendices

A. Expert Panel Recruitment Email	138
B. International Review Board Approval Letter	139

C.	Qualitative Survey: Instrument for Identification of CS-PIFs and Validation of Higher-Order set of CS-PIFs	140
D.	Case Review Categorization Results 1-50	156
E.	Case Review Categorization Results 51-100	157
F.	Case Review Categorization Results Breakdown	158
G.	Fuzzy-set Qualitative Comparative Analysis Membership Calibration Rubric	159
H.	Sample Case Review	160
I.	Final Data Matrix Cases 1-50	161
J.	Final Data Matrix Cases 51-102	162

References 163

List of Tables

Tables

1. Summary of Data Breach Literature	31
2. Summary of Human Error Literature	39
3. Summary of Performance Influencing Factors Literature	43
4. Summary of Organizational Cybersecurity Literature	49
5. Summary of Cybersecurity Policies and Procedures Literature	55
6. Matrix of Security Teaching Methods and Measures that can be Implemented	58
7. Summary of Cybersecurity Education, Training, and Awareness Literature	61
8. Summary of Cybersecurity Knowledge, Skills, and Abilities Literature	66
9. Summary of Employee Cybersecurity Fitness for Duty Literature	72
10. Summary of Ergonomics Literature	76
11. Organization Types	91
12. QCA Case Sample Size Share	92
13. Descriptive Statistics of SMEs (N=25)	98
14. Summary of CS-PIFs and CS-HEs	109
15. Conditions and Outcomes Used	111
16. Necessary Conditions Summary	113
17. fsQCA Results Summary	116
18. RQ4b RBM: System Misconfiguration Caused Breaches Solutions	118
19. RQ4c SBE: Social Engineering Caused Breaches Solutions	119
20. RQ4d KBM: Poor Cybersecurity Hygiene Caused Breaches Solutions	119
21. RQ5a1 KBM: All Business Organizations	120
22. RQ5a2 RBM: Education/Non-Profit Organizations Solutions	121
23. RQ5a3 KBM: Government Organizations Solutions	121
24. RQ5b3 KBM: Large Organizations Solutions	122
25. FsQCA Solutions Summary	123
26. FsQCA Configurations that Fit Multiple Models	124
27. RQ4 FsQCA Solutions	135
28. RQ5 FsQCA Solutions	136

List of Figures

Figures

1. Generic Error-Modeling System	7
2. Generic Error-Modeling Comparative for Data Breach Framework	9
3. ITRC Data Breach Trend 2006–2017	12
4. Data Breach Causes	13
5. Spam Email Typology Example	14
6. Swiss Cheese Model for Spam Email Attack	15
7. Two-factor Taxonomy of End User Security Behaviors	36
8. The Three Levels of Culture	46
9. CETA to Competency Relationship	61
10. Competency Development and Human Performance Levels Comparison	65
11. Balance Theory of Job Design on Performance	79
12. Research Design for Empirical Investigation using fsQCA	82
13. Instrument Development for Cybersecurity Performance Influencing Factors	83
14. Components of Inference	90
15. Phase 1 of the Research Design for Empirical Investigation using fsQCA	97
16. External 1st Order CS-PIF SME Identification	100
17. Internal 1st Order CS-PIF SME Identification	101
18. External 2nd Order CS-PIF SME Validation	102
19. Internal 2nd Order CS-PIF SME Validation	103
20. External and Internal 1st and 2nd Order CS-PIF SME Feedback Summary	104
21. Phase 2 of the Research Design for Empirical Investigation using fsQCA	105
22. Data Breach Cause Groups and Categories	107
23. Data Breach Cause Groups by Organization Type	108
24. Utilized Fuzzy-set Criteria	110
25. Organization Size Criteria	113
26. Truth Table Example	115
27. Truth Table Example Following Frequency and Consistency Thresholds	115
28. Research Questions fsQCA Results	116

Chapter 1

Introduction

Background

Information Systems (IS)—critical for employee productivity—enable organizations to communicate, collaborate, and conduct business or operations (Hua & Bapna, 2013; Jensen et al., 2014; Sabherwal et al., 2019; Thomson & von Solms, 2005). Unfortunately, IS comes at a cost—it must be protected from nefarious actors and unintentional actions that could compromise the security of the IS. IS security involves maintaining the Confidentiality, Integrity, and Availability (CIA) of information and IS (Ayyagari, 2012; Zimmerman & Renaud, 2019). A common type of IS security compromise is known as a data breach, which can be defined as the “unauthorized access or inadvertent disclosure of sensitive information” (Ayyagari, 2012, p. 33).

Data breaches are worldwide phenomena affecting many countries and industries around the world (Ponemon Institute, 2021). Data breaches are costly to organizations in resolving the breach incident and to consumers when their records are compromised (Carre et al., 2018; Garrison & Ncube, 2011). Ponemon Institute’s (2021) Cost of Data Breach study examined 537 data breaches in 17 countries and 17 industries, and found that the average data breach cost was about \$4.24 million, or an average cost of \$161 per lost or stolen consumer data breach record.

In the United States (US), data breaches that compromise 500 or more individuals' health records must be reported to the US Department of Health and Human Services (HHS) (US Department of Health and Human Services Office for Civil Rights, 2020). All 50 US states have laws that require breached companies to notify residents that their data was compromised (Steptoe & Johnson LLP, 2018). Causes for data breaches are attributed to system glitches, external actors, and internal actors (insiders) (Garrison & Ncube, 2011; Kennedy, 2016; Pigni et al., 2018; Ramim & Levy, 2006; Zimmerman & Renaud, 2019).

Insiders are organizational members with privileged access to persons, systems, processes, and facilities (Clarke & Levy, 2017; Hua & Bapna, 2013; Nurse et al., 2014; Zimmermann & Renaud, 2019). Organizational insider threats can be malicious or non-malicious (Hua & Bapna, 2013; Nurse et al., 2014; Vroom & von Solms, 2004; Zimmerman & Renaud, 2019). Human error has increasingly been attributed as a significant cause for data breaches (Chernyshev et al., 2019; Evans et al., 2019; Metalidou et al., 2014). The Identity Theft Resource Center (ITRC) (2018) estimated that for 2017, their *Data Breach Employee Error / Negligence / Improper Disposal / Loss* attack category accounted for only 10.4% of data breach cases, but accounted for 81.5% of records breached. Furthermore, ITRC's other categories may also involve human error as a contributor to the breach.

Although human error is known to be a contributor to data breaches, the understanding of what causes human error in cybersecurity contexts is extremely limited. On the other hand, human error in safety in the context of manufacturing, healthcare, nuclear, laboratory, plants, transportation, aerospace, etc. is relatively well researched and funded

(Senders & Moray, 1991; Xing et al., 2017). In fact, formal Human Reliability Analysis (HRA) methods have been developed in safety applications with an aim to reduce the likelihood and consequence of human errors in complex systems (Evans, et al., 2019; Groth, 2009).

A key component of HRA methods are Performance Influencing Factors (PIF)—the various circumstantial and contextual factors that influence human performance to cause, or contribute to, human error (Franciosi et al., 2019; Groth, 2009). Internal (individual) or external (organizational and contextual) PIFs were assessed; following Curado et al. (2018), assessing that the antecedent at only one level does not fully explain the relationship between conditions and outcomes. In this study, PIFs in cybersecurity contexts are titled Cybersecurity PIF (CS-PIF), and human error in cybersecurity contexts are titled Cybersecurity Human Error (CS-HE).

This research examined CS-PIFs as contributors to CS-HE resulting in data breaches using existing known and documented incidents. Fuzzy-set theory was used to calibrate the degree of membership (i.e. presence or absence) of CS-PIFs and CS-HE in each case, which is appropriate as CS-PIFs and CS-HE can vary by level or degree (Pena & Curado, 2007; Ragin, 2009). Groth (2009) found that PIFs have varying levels of interdependencies and interactions to result in a human error. Thus, Fuzzy-Set Qualitative Comparative Analysis (fsQCA) was used to examine the conjunctural causal relationship of CS-PIFs resulting in CS-HE leading to the data breaches (Rihoux, 2006). Schneider & Rohlfing (2016) defined conjunctural causation as when "multiple conditions occur together for producing the outcome" (p. 530).

Problem Statement

The research problem that this study addressed is that organizational data breaches caused by human error are both costly and have the most significant impact on Personally Identifiable Information (PII) breaches (81.5%) (Greitzer et al., 2014; Evans et al., 2019; Kraemer & Carayon, 2007). The problem set of human error is not new, and Reason (1990) defined human error as “a generic term to encompass all those occasions in which a planned sequence of mental or physical activities fails to achieve its intended outcome, and when these failures cannot be attributed to the intervention of some chance agency” (p. 9). Human error has been examined broadly in the literature—mostly on the topic of safety for industries such as medicine (Chernyshev et al. 2019; Gawron et al., 2006; Reason, 1995), aviation (Miller, 1976; Miranda, 2018; Shappell et al., 2007), space exploration (Boring et al., 2019; Maluf et al., 2005), nuclear reactors, and others (Reason, 1990).

Human errors are inevitable. Humans are not perfect in their activities and errors are often necessary for human evolution—when negative consequences are minimized—for benefits to include “learning, adaptation, creativity, and survival” (Senders & Moray, 1991, p. 37). In addition, some errors are acceptable dependent on the risk to the organization and the user (Abdolrahmani et al., 2017; Zimmerman & Renaud, 2019). The Local Rationality Principle states that people do reasonable things given their goals, knowledge, and focus of attention (Dekker, 2006). However, high level of knowledge, skills, and abilities are the critical corner stone to ensure high level of competency, or lower level of human error during ones’ operations (Carlton & Levy, 2017).

The public interest of human error in safety contexts is plentiful due to potential injury, loss of life, environmental disasters, organizational reputation, or national security

risks (Alonso & Broadribb, 2018; Senders & Moray, 1991). Although human errors in cybersecurity contexts are not reported in news outlets like hacking and ransomware, their damage in data breaches is otherwise widespread and documented (Evans et al., 2019; Garrison & Ncube, 2011; Holtfreter & Harrington, 2015; Metalidou et al., 2014). In the IS discipline, human errors have been examined in areas of Information Technology (IT) implementation (Levine & Rossmoore, 1993); IT service support, delivery operations, and change management (Shwartz et al., 2010); knowledge management (Nielen et al., 2011); human-computer interaction (Maxion & Reeder, 2005); systems development (Rouse, 1985); information privacy (Liginlal et al., 2009); and cybersecurity (Evans et al., 2019; Greitzer et al., 2014; Metalidou et al., 2014; Wood & Banks, 1993).

Some of the organizational consequences of human error in IS are privacy breaches and data breaches (Liginlal et al., 2009; Metalidou et al., 2014). Human errors in IS are a risk to organizations that cannot be ignored (Carre et al., 2018; Cheng et al., 2006). A study by CERT Insider Threat Team (2013) focused on unintentional insider threats found that more than 40% of IT security professionals reported that “their greatest security concern is employees accidentally jeopardizing security through data leaks or similar errors” (p. 42). Human error can lead to disruption of CIA of information as well as IS, directly or indirectly (Enrici et al., 2010; Greitzer et al., 2014; Zimmermann & Renaud, 2019).

With a focus on safety, Reason (1990) investigated the cognitive psychological aspects of human error in various industries to include medicine and aerospace. Reason’s (1990) Generic Error Modelling System (GEMS) of error analysis was built upon

Rasmussen's Skill-Rule-Knowledge (SRK) human performance framework—tying the tripartite of human performance: Skill Based Performance (SBP), Rule Based Performance (RBP), and Knowledge Based Performance (KBP) levels, to human error: Skill Based Error (SBE), Rule Based Mistake (RBM), and Knowledge Based Mistake (KBM) (Rasmussen, 1983). Reason (1990) characterized that SBP is utilized during routine activities; RBP and KBP are utilized during problem solving activities.

Rasmussen (1983) characterized SBP as representing “sensory-motor performance during acts or activities which, following a statement of an intention, take place without conscious control as smooth, automated, and highly integrated patterns of behavior” (p. 258). SBP requires minimal cognitive processing as the actor is already an expert in the routine action (Reason, 1990). RBP is used during familiar situations when problems are solved (or attempted to be solved) using stored rules or procedures (Bolton, 2017; Rasmussen, 1983; Reason, 1990). KBP is used during novel, unfamiliar situations, using slow, conscious analytical processes to solve problems (Bolton, 2017; Rasmussen, 1983; Reason, 1990). Actors can move between SBP, RBP, and KBP levels during their problem solving (Reason, 1990).

During SBP, execution failure (observable failed actions) results in a slip, and storage failure (failure of memory) results in a lapse; slips and lapses are SBEs. In mistakes—failure of planning—the actor is aware of a problem. During RBP, the failure of expertise (misapplication of a good rule or an application of a bad rule) results in RBM. During KBP, a lack of expertise results in KBM (Reason, 1990). A summary of Reason's (1990) GEMS is shown in Figure 1. Several studies have examined human error in IS, but an empirical assessment of the conjunctural causal relationship between CS-PIFs and CS-

HE that lead to data breaches is lacking (Ahmed et al., 2012; Evans et al., 2019; Kraemer & Carayon, 2007; Zimmermann & Renaud, 2019).

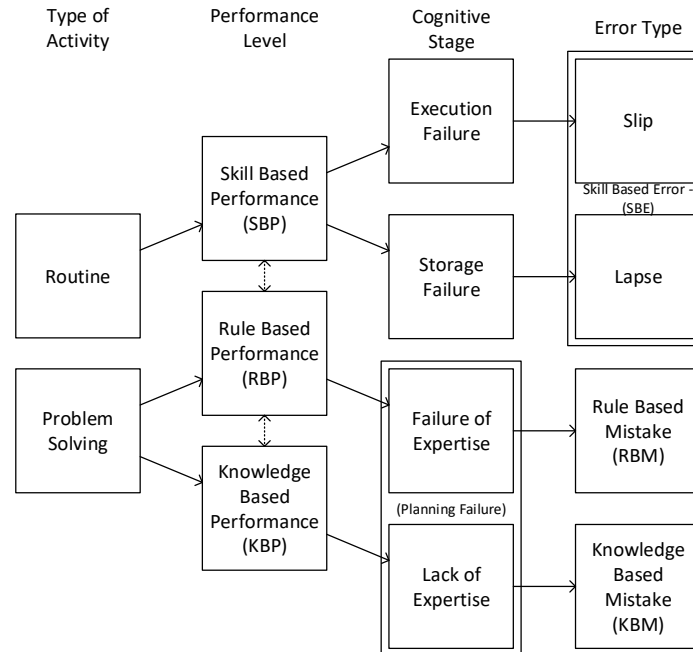


Figure 1: Generic Error-Modeling System (GEMS) adapted from Reason (1990)

Dissertation Goal

The main goal of this research study was to employ configurational analysis to empirically assess the conjunctural causal relationship of internal (individual) and external (organizational and contextual) Cybersecurity Performance Influencing Factors (CS-PIFs) leading to Cybersecurity Human Error (CS-HE) (SBE, RBM, and KBM) that resulted in the largest data breaches across multiple organization types from 2007 to 2019 in the US. The need for this research was conceptualized from the literature and empirical works from several fields. Senders and Moray (1991) summarized the knowledge presented at two scientific conferences (one in 1980 and one in 1983); an international panel of human error experts participated in these conferences to collaborate and advance the understanding of human error following several high-profile disasters, where

Reason's (1990) GEMS model was later established as a framework for human error modeling, with Rasmussen's (1983) SRK performance model contribution. The US Nuclear Regulatory Commission (NRC) developed several HRA methods over the years, to include Technique for Human Error-Rate Prediction (THERP) (Swain & Guttman, 1983), Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H) (Gertman et al., 2005), Human Event Repository and Analysis (HERA) (Hallbert et al., 2006), and Integrated Human Event Analysis System (IDHEAS) (Xing et al., 2017).

Within NRC's HRA methods, PIFs are a key component described as the influence on human performance leading to human error (Whaley et al., 2016). Groth (2009) and Boring (2010) examined several HRA methods to compare PIFs. Although the PIFs presented in previous HRA methods were focused on safety, some of the same PIFs in isolation are recognized in the cybersecurity literature as contributing to human error (Boyce et al., 2011; Doherty & Fulford, 2005; Kennedy, 2016; Kraemer & Carayon, 2007; Rhee et al., 2009; Zimmermann & Renaud, 2019). Several researchers recognized the significance of human error on cybersecurity and data breaches (Evans et al., 2019; Greitzer et al., 2014; Kraemer & Carayon, 2007; Zimmermann & Renaud, 2019). Furthermore, several data breach databases and reports describe human error as a significant cause of data breaches (Identity Theft Resource Center, 2021; Ponemon Institute, 2021; Privacy Rights Clearinghouse, 2021; Verizon, 2021). This study assessed the conjunctural role of CS-PIFs on CS-HE leading to data breaches.

This research developed the Generic Error-Modeling Comparative for Data Breach Framework (GEMC-DBF) to empirically assess the conjunctural relationship of CS-PIFs that contributed to CS-HE (SBE, RBM, or KBM) that resulted in the largest data

breaches in the US from 2007 through 2019 (LexisNexus, 2021; Privacy Rights Clearinghouse, 2021). The GEMC-DBF is shown in Figure 2. fsQCA was used to evaluate sufficient conditions (CS-PIFs) and configuration of conditions with the outcomes (error types) that led to data breaches (Balle et al., 2018; Cress & Snow, 2000; Ragin, 2009). Crisp-set QCA (csQCA) uses Boolean logic (crisp sets) to establish memberships; the derivative fsQCA instead will be used as it allows partial membership using ordinal values (e.g. an action can partially be a rule-based mistake) (Melati et al., 2021; Ragin, 2009).

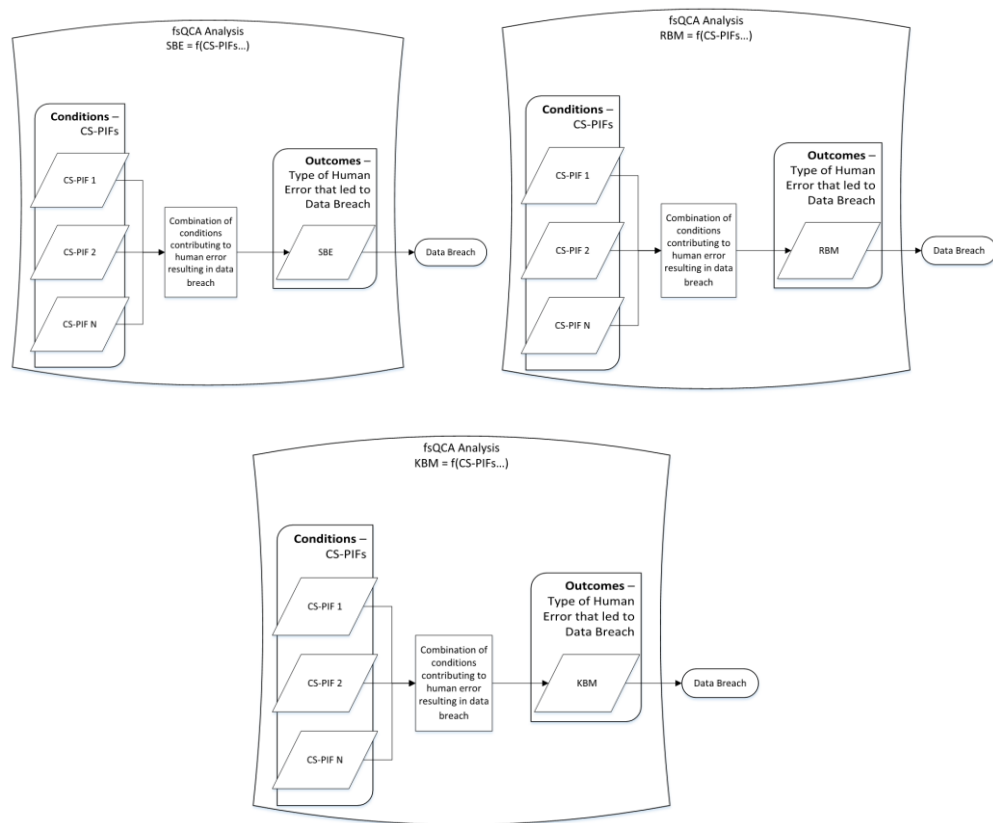


Figure 1: Generic Error-Modeling Comparative for Data Breach Framework (GEMC-DBF)

This research study had five specific goals. The first goal of this research study identified, using cybersecurity Subject Matter Experts (SMEs), the most common internal (individual) and external (organizational and contextual) CS-PIFs leading to human error that result in data breaches. The second goal of this research study validated, using cybersecurity SMEs, the higher-order set of the most common internal (individual) and external (organizational and contextual) CS-PIFs leading to human error that result in data breaches. The third specific goal of this study was to assess the alternative configurations of internal (individual) and external (organizational and contextual) CS-PIFs leading to (a) skill-based errors; (b) rule-based mistakes; and (c) knowledge-based mistakes resulting in the largest data breaches across multiple organization types from 2007 to 2019 in the US. The fourth specific goal of this study was to assess the alternative configurations of CS-PIFs responsible for CS-HE leading to various data breaches caused by: (a) unintended disclosure; (b) system misconfiguration; (c) social engineering; and (d) poor cybersecurity hygiene in the largest data breaches across multiple organization types from 2007 to 2019 in the US. The fifth specific goal of this study was to assess how alternative configurations of CS-PIFs on CS-HE leading to the largest data breaches across multiple organization types from 2007 to 2019 in the US were represented across (a) industry type and (b) company size.

Research Questions

The main research question that this study addressed was: What is the conjunctural causal relationship, using configurational analysis, of internal (individual) and external (organizational and contextual) CS-PIFs leading to CS-HE that resulted in the largest data

breaches across multiple organization types from 2007 to 2019 in the US? Additionally, the following specific research questions (RQs) were addressed by this study:

RQ1: What are the cybersecurity SMEs' identified most common internal (individual) and external (organizational and contextual) CS-PIFs leading to CS-HE that result in data breaches?

RQ2: What are the cybersecurity SMEs' validated higher-order set of the most common internal (individual) and external (organizational and contextual) CS-PIFs leading to human error that result in data breaches?

RQ3: What are the alternative configurations of internal (individual) and external (organizational and contextual) CS-PIFs leading to (a) skill-based errors; (b) rule-based mistakes; and (c) knowledge-based mistakes resulting in the largest data breaches across multiple organization types from 2007 to 2019 in the US?

RQ4: What alternative configurations of CS-PIFs are responsible for CS-HE leading to various data breaches caused by: (a) unintended disclosure; (b) system misconfiguration; (c) social engineering; and (d) poor cybersecurity hygiene, in the largest data breaches across multiple organization types from 2007 to 2019 in the US?

RQ5: How are the alternative configurations of CS-PIFs on CS-HE leading to the largest data breaches across multiple organization types from 2007 to 2019 in the US, represented across (a) industry type and (b) company size?

Relevance and Significance

Relevance

Cybersecurity issues are problematic for individuals, organizations, and governments globally (Carre et al., 2018; Levy et al., 2011; Ramim & Levy, 2006), with annual global

losses expected to reach \$10.5 trillion by 2025 (Raju et al., 2021). In addition to financial losses, there are reputational damages to organizations and privacy breaches of individuals (Carre et al., 2018; Verizon, 2021). The consequential damage from data breaches has resulted in the enactment of several US federal statutes to protect consumers, and the enactment of State notification laws that have increased personal notifications and public awareness of data breaches (Steptoe & Johnson LLP, 2018).

Data breach occurrences have been on the rise—the number of breaches has increased from 321 breaches in 2006 to 1579 breaches in 2017, according to the Identity Theft Resource Center’s (2018) reporting (see Figure 3). The overall number of records breached have also increased from 55 million in 2005 to 1.5 billion in 2018 (Privacy Rights Clearinghouse, 2019). It is unclear how much the increased reporting requirements and public pressure influenced the sharp increase in data breach estimates over the years, but actual breaches are still underreported (Park, 2019).

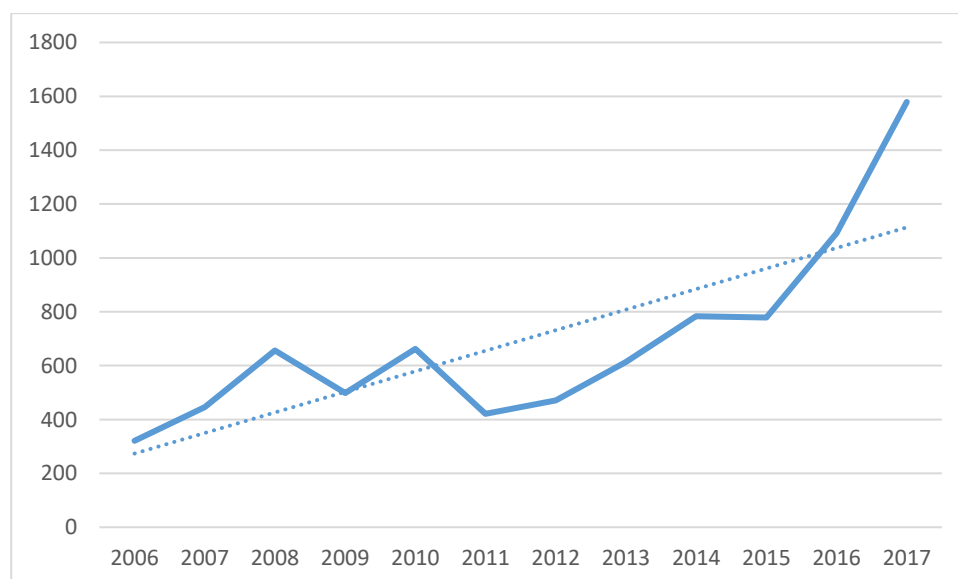


Figure 3: ITRC Data Breach Trend 2006–2017. Data retrieved from Identity Theft Resource Center 2017 Annual Data breach Year-End Review (2018)

Interest in data breach investigations have rapidly increased in the last decade. Several organizations investigate and report data breach trends annually, to include Ponemon Institute (2021), Identity Theft Resource Center (2021), Privacy Rights Clearinghouse (PRC) (2021), and Verizon (2021). Causes of data breaches vary in definition across the investigators. Due to the different categorizations, the role human error plays on data breaches vary by outlet. A summary of data breach causes and their share of cause of breaches is shown in Figure 4.

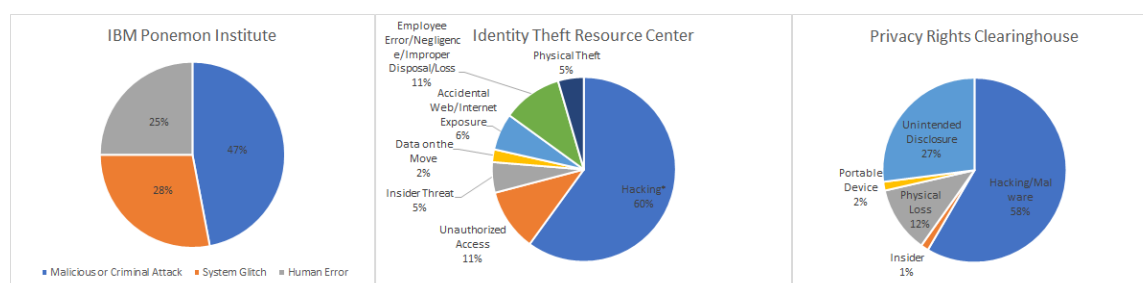


Figure 4: Data Breach Causes, data retrieved from Ponemon Institute (2017), Identity Theft Resource Center (2018), and Privacy Rights Clearinghouse (2019)

Besides the system glitch category in Ponemon Institute’s study, all other causes of data breaches may be partly attributed to human error within the organization. Although human error is acknowledged to be a major contributor to data breaches, it appears to play a larger role than the reporting figures reveal (Pollini et al., 2021). For example, ITRC categorizes phishing attacks under the HACK category, but phishing requires a human vulnerability in the form of human error and susceptibility to an attacker’s deceit given that nowadays, most individuals are aware of the phenomena of phishing. Verizon (2017) further agreed by noting, “one could persuasively argue that all breaches have an error somewhere in the chain of events, but if it did not directly lead to the breach, it is classified under some other pattern” (p. 50).

IBM Security (2017) asserted that “spam email remains a primary tool in the attacker’s toolkit, reinforcing the pervasiveness of malware and the potential for inadvertent insider attacks” (p. 10), which further support that human error facilitates attacks. A simplified hypothetical example is illustrated in Figure 5 where the attacker and technology each play only one role in a spam email attack. The hacker may send thousands of these attacks to different organizations and the varying technology and people defenses within the organization will dictate the hacker’s success; the attacker construct rarely can be directly minimized. The blue arrows are illustrated as potential acts of human error.

In Figure 5, the attacker has one role, which is to send the spam email with malicious content to users, often effortlessly, while technology has one role, attempt to block the spam email. Organizational management must support the cybersecurity professional, facilitate a security culture, and fund the spam filter. The cybersecurity professional must configure the spam filter properly and provide proper security training when using email. The user must use their security Knowledge, Skills, and Abilities (KSAs) to recognize spam emails and not fall victim to an attack.

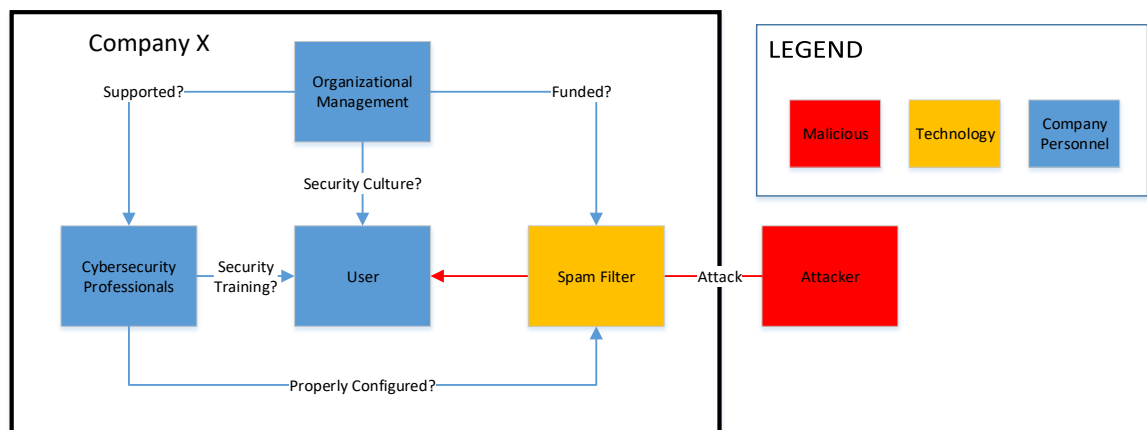


Figure 2: Spam Email Typology Example

Reason (2000)'s Swiss Cheese model of system accidents demonstrate how “defenses, barriers, and safeguards may be penetrated by an accident trajectory” (p. 769). Although originally developed for safety, Saarelainen and Jäntti (2015) modified the Swiss Cheese model to demonstrate similar human error causes for IT service incidents. The Swiss Cheese model is partially analogous to security-in-defense in security applications.

A modified Swiss Cheese model in the cybersecurity context for spam email attack is shown in Figure 6. As shown, for the hacker to be successful, they must rely on the organization's personnel to commit several errors (or failures). Schultz (2005) affirmed it by noting, “information security is primarily a people problem, not a technical problem” (p. 425). In summary, the relevance of this study is clear: data breaches are costly and more frequent, and the role of human error in data breaches is underrepresented and misunderstood.

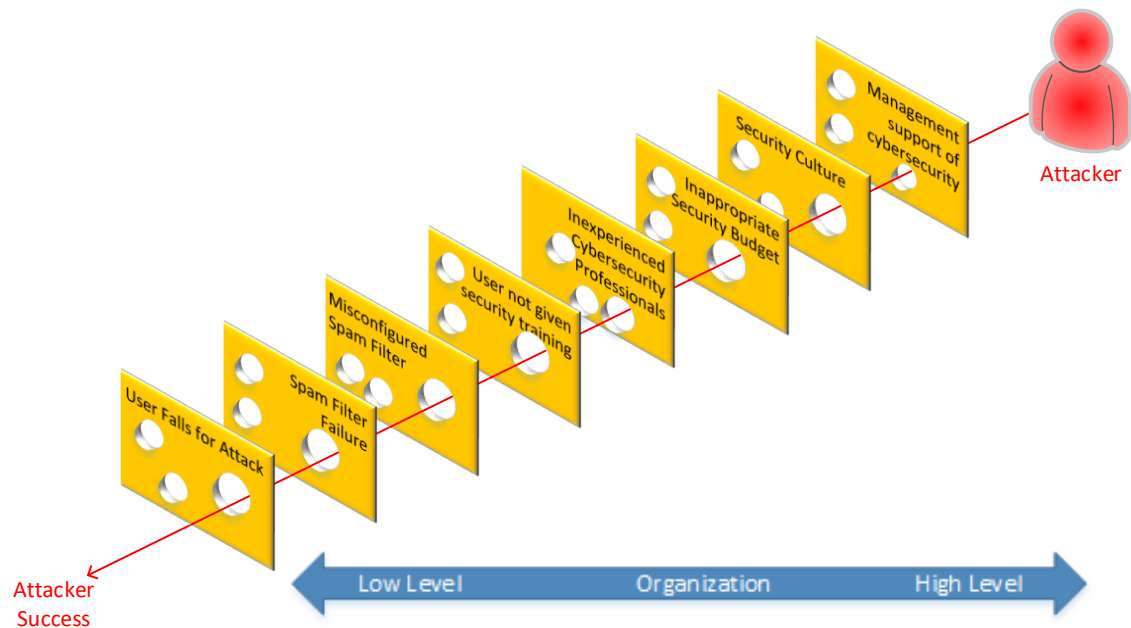


Figure 3: Swiss Cheese Model for Spam Email Attack

Significance

The significance of this research was to assess the conjunctural relationship of CS-PIFs and CS-HEs so organizations can be cognizant and proactive of the interaction in the future. PIFs are the factors that attribute to human error. In the cybersecurity context, it appeared that this had yet to be well articulated or defined. This research outlined an SME-supported list of CS-PIFs that can be attributed to CS-HE leading to data breaches. By examining historical data breaches and identifying CS-PIFs, fsQCA was used to investigate which conjunctural combinations of CS-PIFs led to CS-HE in examined breaches.

As a by-product of the research goals, this research also provided insight into the types of CS-HE that occurred in the examined data breaches. First, what type of human error was committed to cause a breach or set the conditions resulting in a breach? In a hypothetical phishing attack example, was it a Skill-Based Error (e.g. subconsciously clicking the link), Rule-Based Mistake (e.g. forwarding the identified phishing attack to a manager instead of IT, resulting in a breach), or Knowledge-Based Mistake (e.g. lack of expertise resulted in user clicking the link)? It was important to identify which type of human error occurred, as “the three levels will vary in the degree to which they are shaped by both intrinsic (cognitive biases, attentional limitations) and extrinsic factors (the structural characteristics of the task, context effects)” (Reason, 1990, p. 59). Finally, it is important for organizational leadership to understand what causes their employees to make bad decisions, as French et al. (2011) noted, “managers understand human behaviour; good managers understand human behaviour extremely well. To bring out the best in a team one needs to know how each will respond to a request, an instruction, an incentive or a sanction” (p. 754).

Barriers and Issues

There were several potential barriers this study faced. A potential barrier was collecting responses from the same SMEs for research goal one (identifying common cybersecurity PIFs) and research goal two (validating higher-order set of common CS-PIFs leading to human error that result in data breaches). For this study, having the same SMEs participate in both steps of the instrument development was important to improve the quality of the CS-PIF final set. As the SMEs were volunteers, they may have withdrawn from participating at any time, thereby skewing the results (Ellis & Levy, 2009). To address this barrier, research goals one and two were combined into the same survey.

Another potential barrier was SME participants not recognizing or understanding CS-PIF terms and their role in data breaches. To mitigate this potential barrier, a section of CS-PIF definitions were provided in the survey to provide a baseline understanding for all survey participants. The definitions provided context on how certain CS-PIFs have attributed to human error in cybersecurity and safety.

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are the factors that a researcher may take for granted as true, without proof, and may not necessarily hold true (Ellis & Levy, 2009). In this study, it was assumed that human cognition, behavior, and performance were entirely transferrable from safety to security. Although there were indicators of PIFs in cybersecurity, much was transferred to this research from the safety literature and human reliability analysis.

Limitations

Limitations are the researcher identified potential uncontrollable weaknesses in the study that may affect the internal validity of the study (Ellis & Levy, 2009). One such limitation was the scarcity of available data within data breach cases. Data breach details are generally limited as organizations are wary of sharing detailed information with regards to data breaches, either because of legal or reputational reasons. The same limitation is true for incident investigations in safety contexts (Boring, 2007). In this research, the largest breaches were examined due to more media coverage on those breaches, and thus, more information to identify the PIFs that occurred resulting in the human error leading to the breach. Future studies may be conducted with interview or survey methods to collect data breach detailed data on CS-PIF and CS-HE.

Examining only the largest breaches created another limitation: this study's findings represented the larger breaches. Breaches that were smaller in scope may have had different causes. Further research is warranted to cover the smaller to medium sized breaches with possibly other data collection methods. Another limitation was the use of historical data breach information for data collection—it is possible that CS-PIFs listed in specific breaches were represented as false-positive or false-negative, and may have influenced some of the analysis.

Delimitations

Delimitations define the boundaries and scope to make the research manageable, but also reduce generalizability (Ellis & Levy, 2009). This research did not attempt to reduce human error or the conditions leading to human error—this research instead surfaced the underlying baseline of conjunctural combination of conditions (PIFs) that resulted in human error leading to specific data breaches. Further research is warranted in using the

knowledge generated in this research to investigate reduction in human error leading to data breaches by controlling PIFs, in controlled or natural settings. Additionally, due to the level of detail made public in larger data breaches, only the largest data breaches were examined. Finally, only US data breaches were examined.

Definition of Terms

Boolean minimization—“the ‘reduction’ of a long, complex expression into a shorter, more parsimonious expression” (Rihoux & De Meur, 2009, p. 35).

Calibration—“Calibration is the process of classifying conditions in each case from full membership (1.00) to full non-membership (0.00)” (Curado, 2017, p. 83).

Case—“Each configuration of causal conditions and the associated outcome becomes a case” (Crespo et al., 2021, p. 335).

Causal asymmetry—“The presence and the absence of the outcome, respectively, may require different explanations” (Berg-Schlosser et al., 2009, p. 9).

Conditions—The variables within a case that produce the phenomenon of interest (outcome). Conditions can be thought of as the independent variables in quantitative methods (Rihoux, 2006).

Configuration—A specific combination of conditions that produces a given outcome of interest (Rihoux & Ragin, 2009, p. xix).

Configurational Comparative Methods (CCM)—An umbrella term for methods and techniques—such as csQCA, mvQCA, and fsQCA, that are used to “enable the systematic comparative analysis of complex cases, those cases must be transformed into configurations” (Rihoux & Ragin, 2009, p. xix).

Conjunctural causation—When “multiple conditions occur together for producing the outcome” (Schneider & Rohlfing, 2016, p. 530).

Crisp-set Qualitative Comparative Analysis (csQCA)—The first QCA technique developed, as an instrument using Boolean and minimization algorithms for “identifying patterns of multiple conjunctural causation” and a tool to “simplify complex data structures in a logical and holistic manner” (Ragin, 1987, p. viii).

Cybersecurity—“A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management” (Burley et al., 2017, p. 16).

Cybersecurity Performance Influencing Factors (CS-PIF)—A term coined in this research to reference performance influencing factors that contribute to human error leading to cybersecurity contexts (Groth, 2009).

Data breach—“unauthorized access or inadvertent disclosure of sensitive information” (Ayyagari, 2012, p. 33).

Data triangulation—leverages the strength of one method on the others, and provides a more comprehensive understanding of a phenomenon of interest (Sands & Roer-Strier, 2006).

Equifinality—“Different paths can lead to the same outcome” (Berg-Schlusser et al., 2009, p. 8).

Fuzzy set—“A ‘class’ with a continuum of grades of membership” (Zadeh, 1965).

Fuzzy set membership—the pinpointed qualitative state of membership between full inclusion and full exclusion in a set (Ragin, 2009).

Fuzzy-set Qualitative Comparative Analysis (fsQCA)—A type of qualitative comparative analysis, published in 2000 by Ragin to overcome the limitations of csQCA and its simple presence/absence dichotomies (crisp sets) by implementing fuzzy sets—partial membership in sets (Ragin, 2009).

Fuzzy-set theory—“A well-developed mathematical system for addressing partial membership in sets” (Ragin, 2009, p. 88).

Generic Error-Modelling System (GEMS)—A conceptual framework “within which to locate the origins of the basic human error types” (p. 53)—which are skill-based slips (and lapses), rule-based mistakes, and knowledge-based mistakes (Reason, 1990). The structure was “derived in large part from Rasmussen’s skill-rule-knowledge classification of human performance” (Reason, 1990, p. 53).

Human error—“a generic term to encompass all those occasions in which a planned sequence of mental or physical activities fails to achieve its intended outcome, and when these failures cannot be attributed to the intervention of some chance agency” (Reason, 1990, p. 9).

Human error types—Reason’s (1990) generic error-modelling system has three human error types: skill-based slips (and lapses), rule-based mistakes, and knowledge-based mistakes.

Human Event Repository and Analysis (HERA)—a system that a “data analysis method, structure, and accompanying software database for recording human

performance and reliability data that are relevant to Nuclear Power Plants (NPPs)” (Hallbert et al., 2006, p. 1).

Human Reliability Analysis (HRA)—“Formal qualitative analysis and quantification methods available for use as part of Probabilistic Risk Assessments (PRAs) in modeling risk in Nuclear Power Plants (NPPs)” (p.1), more generally modelling human error (Whaley et al., 2016).

Knowledge-Based Mistake (KBM)—Lack of knowledge failure occurs during knowledge-based performance “in novel situations where the solution to a problem has to be worked out on the spot without the help of preprogrammed solutions” (Reason, 1995, p. 81).

Knowledge-Based Performance (KBP)—“During unfamiliar situations, faced with an environment for which no know-how or rules for control are available from previous encounters, the control of performance must move to a higher conceptual level, in which performance is goal-controlled” (Rasmussen, 1983, p. 259).

Necessary Condition—“A condition is *necessary* for an outcome if it is always present when the outcome occurs. In other words, the outcome cannot occur in the absence of the condition” (Rihoux & Ragin, 2009, p. xix).

Outcomes—The phenomenon or consequence of interest in a case. Outcomes can be thought of as the dependent variable in quantitative methods (Rihoux, 2006).

Performance Influencing Factor (PIF)—Originally called Performance Shaping Factors (PSFs), PIFs are the various circumstantial and contextual factors that influence human performance to cause, or contribute to, human error (Groth, 2009).

Qualitative Comparative Analysis (QCA)—An umbrella term that encompasses csQCA, msQCA, and fsQCA (Rihoux & Ragin, 2009).

Rule-Based Mistake (RBM)—Failures of expertise during rule-based performance occurring in several forms: “the misapplication of a good rule (usually because of a failure to spot the contraindications), the application of a bad rule, or the non-application of a good rule” (Reason, 1995, p. 81).

Rule-Based Performance (RBP)—A problem-solving activity “typically controlled by a *stored rule* or procedure which may have been derived empirically during previous occasions, communicated from other persons’ know-how as instruction or a cookbook recipe, or it may be prepared on occasion by conscious problem solving and planning” (Rasmussen, 1983, p. 259).

Skill-Based Error (SBE)—Failures during skill-based performance termed as slips (failure of action) and lapses (failure of memory) (Reason, 1995).

Skill-Based Performance (SBP)—“Sensory-motor performance during acts or activities which, following a statement of an intention, take place without conscious control as smooth, automated, and highly integrated patterns of behavior” (Rasmussen, 1983, p. 258). SBP occurs during routine and familiar activities where there are no problems identified (Reason, 1990).

Skill-rule-knowledge framework—Jens Rasmussen’s (1983) categorization of the “three levels of performance correspond to decreasing levels of familiarity with the environment or task” (Reason, 1990, p. 43). The three levels are skill-based, rule-based, and knowledge-based levels of performance (Rasmussen, 1983; Reason, 1990).

Sufficient Condition—“A condition is *sufficient* for an outcome if the outcome always occurs when the condition is present. However, the outcome could also result from other conditions” (Rihoux & Ragin, 2009, p. xix).

Technique for Human Error-Rate Prediction (THERP)—“A method to predict human error probabilities and to evaluate the degradation of man-machine systems likely to be caused by human errors alone or in connection with equipment functioning, operational procedures and practices, or other system and human characteristics that influence system behavior” (Swain & Guttman, 1983, p. 5-3).

Truth Table—“A table of configurations” (Rihoux & De Meur, 2009, p. 44).

List of Acronyms

Configurational Comparative Methods (CCM)

Crisp-set Qualitative Comparative Analysis (csQCA)

Cybersecurity Performance Influencing Factors (CS-PIF)

Fuzzy-set Qualitative Comparative Analysis (fsQCA)

Generic Error-Modelling System (GEMS)

Human Event Repository and Analysis (HERA)

Human Reliability Analysis (HRA)

Knowledge-Based Mistake (KBM)

Knowledge-Based Performance (KBP)

Performance Influencing Factor (PIF)

Qualitative Comparative Analysis (QCA)

Rule-Based Mistake (RBM)

Rule-Based Performance (RBP)

Skill-Based Error (SBE)

Skill-Based Performance (SBP)

Technique for Human Error-Rate Prediction (THERP)

Summary

The purpose of this chapter was to introduce the research study. The background section described the need for information systems, the wide occurrence and damage of data breaches, and the threat human error has on causing data breaches. Additionally, human error in safety contexts was discussed, and specifically the construct of performance influencing factors was established.

The problem statement was provided in the following section, which described how significant the cost and impact human error has on data breaches and PII breached. The dissertation goal section began with the main research goal, which is to employ configurational analysis to empirically assess the conjunctural causal relationship of internal (individual) and external (organizational and contextual) Cybersecurity Performance Influencing Factors (CS-PIFs) leading to Cybersecurity Human Error (CS-HE) (SBE, RBM, and KBM) that resulted in the largest data breaches across multiple organization types from 2007 to 2019 in the US. Additionally, five specific goals were stated, which sequentially help in achieving the main goal. The main research goal and five research questions were also provided.

The relevance of human error's role in data breaches was provided, which appears to be a relatively new research stream and research area of interest in cybersecurity. The significance section described how the research study could benefit organizations and cybersecurity practitioners by providing granularity and depth into human error. Barriers,

assumptions, limitations, and delimitations were discussed to provide clarity on the details of the research. Finally, a definition of terms and list of acronyms were provided. The next chapter reviews the literature with respect to data breaches, human error, and performance influencing factors.

Chapter 2

Review of the Literature

Introduction

The literature review presented in this chapter spans the disciplines of cybersecurity, psychology, and human reliability. First, data breaches are defined and subsequently examined across time, place, and contexts. Second, human error is defined, dissected, and explained from a cognitive psychological perspective. Finally, the human error causes—performance influencing factors—is explained and examined. Specifically, six performance influencing factors are examined: organizational cybersecurity; cybersecurity policies and procedures; cybersecurity education, training and awareness; cybersecurity knowledge, skills, and abilities; cybersecurity fitness for duty; and ergonomics.

Due to the novel nature of this research, the literature review criteria had to be expanded in time and academic discipline. Many of these constructs and their influence on human error were “borrowed” or recognized from the safety literature (e.g. fatigue, situation awareness, etc.), and were not always recognized in the cybersecurity literature as tying these constructs (PIFs) to human error in cybersecurity contexts. The three main themes of this research are data breaches, human error, and performance influencing

factors; their relationship and their influence on the research problem are the primary motive for the scope of this review.

Data Breaches

Information Systems and Cybersecurity

Information Systems (IS) connect the world to facilitate communications, commerce, and education. IS consist of the environment, the technology, and the people (Taylor & Robinson, 2015). IS's inherent vulnerabilities and numerous threats paved the way for the discipline of IS Security—also known as cybersecurity. The Federal Information Security Modernization Act (FISMA) of 2014 described information security as providing CIA to protect information and IS from “unauthorized access, use, disclosure, disruption, modification, or destruction” (US Congress, 2014, p. 128). Confidentiality can be defined as “preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information” (US Congress, p. 128). When organizations fail to maintain confidentiality of their consumer's or customer's private data, a data breach occurs.

Data Breaches

Rahulamathavan et al. (2016) defined a data breach as “a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, or lost” (p. 363). Data breaches can occur when information is compromised in paper or electronic format (Holtfreter & Harrington, 2015). The unauthorized access can be deliberate (e.g., hacker) or unintentional (e.g., inadvertant recipient of email with PII content). Data breaches range in scope and severity. A data breach can affect as little as one computer or personal record, to as many as millions (Privacy Rights Clearinghouse, 2021).

Organizational data breaches harm the organization and the consumer (Garrison & Ncube, 2011; Pigni et al., 2018). Data breaches can harm an organization's brand, degrade consumer confidence, and cause monetary damages in the form of customer notifications, additional IT security investments, loss of revenue, and government fines (Carre et al., 2018; Zamosky, 2014). Additionally, different industries face breaches with different causes and information types. For example, where businesses, such as retail and finance, may compromise customer credit card or banking information in data breaches, medical organizations are more concerned with compromise of Personal Health Information (PHI) (Ayyagari, 2012; Chernyshev et al., 2019; Pigni et al., 2018).

Human Error in Data Breaches

Cybersecurity is a multifaceted problem—involving organizational, environmental, technological, and human components (Angst et al., 2017; Kraemer & Carayon, 2007; Zimmermann & Renaud, 2019). In contrast to technological security countermeasures, relatively few studies have examined IS security from a psychological lens (Enrici et al., 2010; Evans et al., 2019). In addition, many technical cyberattacks exploit human vulnerabilities. Human errors often introduce or contribute to vulnerabilities that lead to data breaches (Enrici et al., 2010; Evans et al., 2019). As a result, understanding and mitigating human errors can reduce accidental causes of data breaches (Evans et al., 2019; Kraemer & Carayon, 2007).

Cybersecurity issues are caused by external and internal threats, either intentionally or unintentionally (Cheng et al., 2017). Accidental causes can be a result of natural causes such as an electrical surge that takes down a network, or human error non-deliberate acts such as a misconfiguration of a network or a lost device (Enrici et al., 2010; Evans et al.,

2019). Deliberate causes are conscious acts committed by internal or external actors, such as a hack or malware upload (Enrici et al., 2010; Pigni et al., 2018). Deliberate causes such as cyberattacks are often related to human errors, as the cyberattack can exploit a human error—such as a misconfigured and vulnerable device or a succumbing to a phishing attack (Enrici et al., 2010; Evans et al., 2019; Kraemer & Carayon, 2007).

Other deliberate acts can be non-malicious, but intentional. For example, an employee may send an unencrypted email with PII to a colleague (against policy), and the email gets compromised by a hacker. Ayyagari (2012) argued that employees are the source of most data breaches, and employee non-compliance to security policies are one of the major causes. Human error is one of the most underestimated unintentional causes of cybersecurity incidents, as they often introduce and contribute to information security vulnerabilities that are dormant for attackers to capitalize on (Enrici et al., 2010; Evans et al., 2019).

Human Error Data Breach Examples

Verizon (2021) categorized several error varieties leading to data breaches: misconfiguration (allowing for unintended access), misdelivery (sending data to incorrect recipient), publishing error (exposing data on public website), loss, programming error, and *other*. An example of a publishing error—the US Department of Health and Human Services (HHS) Office of Civil Rights (OCR) fined Columbia University and New York-Presbyterian Hospital \$1.5 million and \$3.3 million, respectively, after an employee accidentally made 6,800 patient medical records publicly available (Zamosky, 2014). Data breaches caused by human error don't exclusively happen in the cyberspace domain; an example of a disposal error—a US credit union members' credit card information was

stolen after the credit union inadvertently and improperly disposed their records in a dumpster (Taylor & Robinson, 2015). A brief data breach literature summary is shown in Table 1.

Table 1

Summary of Data Breach Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Angst et al., 2017	Empirical Study	5,000 hospitals and 938 data breaches	Organization characteristics, symbolic / substantive adoption, IT security investment	Institutional factors within an organization create the conditions that make IT security investments more effective in reducing data breaches. IT security alone does not.
Ayyagari, 2012	Content Analysis	2633 data breaches		Review of data breaches cases revealed data breaches caused by hackers is on decline, while breaches caused by human element are increasing. Additionally, implementation and enforcement of security policies account for many of human-induced security risks
Enrici et al., 2010	Literature Review and Theoretical	105 papers	Keywords: Human, psychology, cognitive,	Defined four levels of psychological relevance

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
			information, technology, security	approach to security: human errors approach, human factors approach, cognitive approach, and psychology of security approach
Garrison & Ncube, 2011	Content Analysis	947 data breaches reported in Privacy Rights Clearinghouse Data Breach Database from 2005–2009.	Breach type, institutions, records breached	Analysis resulted in increased knowledge of characteristics of breaches, and followed with recommendations such as technical controls (error-proofing software) and administrative controls (initial and reoccurring security training)
Kraemer & Carayon, 2007	Exploratory study via interview	16 network administrators and security specialists were interviewed	Security breaches, human errors, individual elements, task elements, workplace environment elements, technology elements, organizational elements	Frequently cited causes of human related cybersecurity breaches are communication, security, policy and organizational structure

Human Error

Introduction

As noted, many data breaches are caused by human error, and human error is the result of failure in human performance. Human error is not exclusive to cybersecurity though, as a great deal of research has been done in human factors (Rasmussen, 1983), psychology (Reason, 1990), and human reliability analysis (Evans et al., 2019; French et al., 2011). Interest in these fields is warranted due to human error having caused, as of the time of their publication, over 90% of failures in the nuclear industry (Reason, 1990); over 80% of failures in the chemical and petro-chemical industries, over 75% of marine casualties, and over 70% of aviation accidents (French et al., 2011).

Human Performance

Rasmussen (1983) distinguished three levels of human performance: skill-based, rule-based, and knowledge-based performance. Skill-Based Performance (SBP) is performed during routine activities, and does not involve conscious attention or control. Rule-Based Performance (RBP) is performed consciously, is goal-oriented, and accomplished using stored rules or procedures (acquired previously or provided). Knowledge-Based Performance (KBP) is performed consciously during unfamiliar situations, is goal-oriented, and accomplished using higher level decision making.

French et al. (2011) recognized that human behavior is complex and influenced by internal and external factors; this posits their position that terminology such as “error” in HRA as invalid as they are socially defined. In other words, the employee or user more-often-than-not committed a reasonable action provided the internal and external condition influences (PIFs), and context that led to the unreasonable outcome. French et al. (2011) provided the example of the Three Mile Island Accident in 1979, “where the formation of a hydrogen bubble which forced down cooling water exposing the core” (p. 758), was

unanticipated and unprecedented in reactor designs; the operators behaved and executed as best as they could, provided the circumstances. Compare this to potential cybersecurity lapses where an effective zero-day social engineering tactic is used against a well-intentioned and security aware user.

Human Errors and Violations

Following Rasmussen's (1983) Skill, Rule, and Knowledge (SRK) based performance framework, Reason (1990) developed the Generic Error Modelling System (GEMS) that ties the three levels of human performance to human error. Skill-Based Errors (SBE) occur during periods of SBP. SBE can be separated into slips and lapses—a slip is the failure of action (Norman, 1981) and lapse is the failure of memory (Reason, 1990). Rule-Based Mistakes (RBM) occur during RBP, when the actor misapplies a good rule or applies a bad rule. Knowledge-Based Mistakes (KBM) occur during KBP and are a result of a lack of expertise.

A fourth departure from desired human performance are violations. While SBE, RBM, and KBM are committed due to faulty information and cognitive processing, violations are undesired deliberate acts in the social context—those that oppose governed policies and procedures (Reason et al., 1990). Violations can be deliberate, but non-malicious (Kraemer & Carayon, 2007). Malicious violations are categorized as *sabotage*, and although problematic, are outside the scope of this research.

Regarding violations, are those that drink alcohol and drive intoxicated *bad people*? Or have they simply made a bad decision even though they are fully aware of the law and sanctions? The same can be said in cybersecurity contexts; if connecting USB drives are banned in an organization, and the user that was informed still commits the infraction to

expedite their work, are they automatically a *bad person*? Parker et al. (1992) suggest that the Theory of Planned Behavior (TPB) can be used to explain how several factors may contribute to inappropriate decisions. In this study, non-malicious violations are grouped into KBM.

Human error is not a black and white problem, and, the contributors to human error can vary, especially across contexts. Gawron et al. (2006) found that medical errors can be attributed to incorrectly followed procedures, over-stressed workflows, poor readability of instructions, or physician knowledge. Shappell et al. (2007) used SMEs to examine over 1,000 commercial aviation accidents and found that aircrew and their environment caused most of the accidents, as opposed to unsafe supervision or organizational influences. The National Highway Traffic Safety Administration's 2018 report of 2.5 million US crashes between 2005–2007 found that drivers were the critical reason (i.e. last event in the crash causal chain) for crashes roughly 94% of the time, with the vehicle failure and environment each accounting for 2% (Singh, 2018). In other words, when it comes to human error, context matters.

GEMS in Cybersecurity

Stanton et al. (2005) developed a two-factor taxonomy of end user security behaviors comprising of intentions (malicious to benevolent) and expertise (novice to expert) (see Figure 7). Employees with malicious intentions can cause serious damage—but again, they are outside the scope of this research. Employees with benevolent intentions seek to cause a benefit to the organization. In this research we will examine security behaviors that are not intentionally malicious but may lead to data breaches.

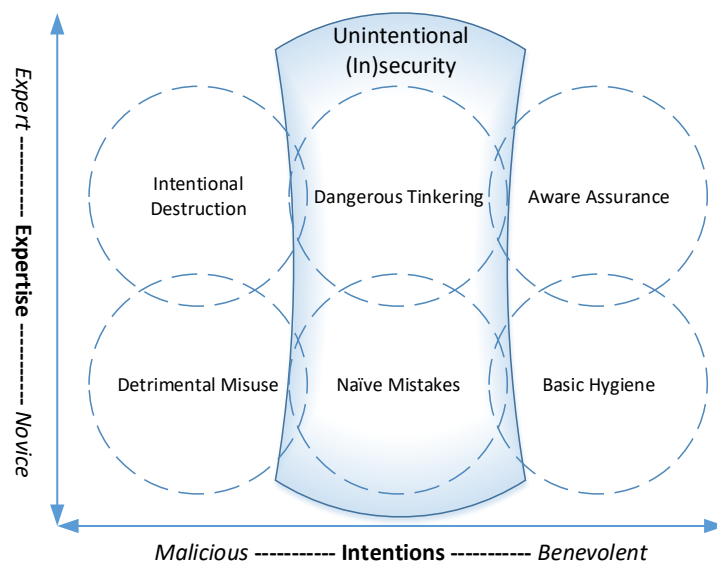


Figure 7: Two-factor Taxonomy of End User Security Behaviors. Adapted from Stanton et al. (2005)

Cybersecurity human error can occur in all levels of the organization—from the end user, the system administrators, to the policy makers and management that institute corporate strategy and guidance. An end user may engage in unsafe web browsing at work that can lead to inadvertent actions resulting in malware or data breach (Goode et al., 2018). This consequence may have been a result of a (ill-advised) violation against policy. Some users make a rationalized decision to commit violations of organization IT policies that put the system at risk (Barlow et al., 2013; Gcaza et al., 2017; Siponen & Vance, 2010). The user’s intention may not be to cause malice, but rather, circumvent the policies to achieve a positive business outcome (Vance & Siponen, 2012). The policy by itself may not be sufficient for compliance, but in conjunction with training or education to understand the “why” the policy is in place.

Other examples of human error may not be so clear-cut or identifiable as to which human error type it is. As an example, an experienced network engineer setting up a new network may inadvertently open a security exploit in the network configuration, by committing a SBE, RBM, or KBM—depending on the circumstance or context. For example, the engineer may have been distracted and misconfigured the switch (SBE) or inexplicably forgot to save the configuration (SBE); followed a bad procedure (RBM), or their lack of experience failed them in configuring the switch properly (KBM) (Pollini et al., 2021; Stanton et al., 2005). Configuration mistakes can leave security applications, systems, or network boundaries vulnerable (Ahmed et al., 2012; Pollini et al., 2021). In the safety industry, human reliability analysis helps to understand the problem of human error.

Human Reliability Analysis

Human Reliability Analysis (HRA) methods are used to classify and quantify human performance (Boring, 2007; Evans et al., 2019). Additionally, HRA methods evaluate risks contributed by human error by identifying human errors, predicting the likelihood of human error, and reducing the likelihood (Evans et al., 2019; Ung & Shen, 2011). HRA originated from the 1960s US nuclear energy development programs to mitigate potential disasters caused by human factors (French et al., 2011). Over the years, HRA methods have evolved with increasing levels of dimensions where they are classified as either first generation, second generation, or even third generation HRA methods (Boring, 2007; French et al., 2011). There is not a consensus on what constitutes an HRA method being a first or second-generation model; for example, French et al. (2011) described first

generation models as assessing human error via simple event tree analysis and focusing on *omission*—failure to respond to events appropriately.

Second generation models more generally have the features of cognition, context, commission, and chronology (Boring, 2007). Cognition adds the element of cognitive psychological aspects to factors influencing performance (i.e. PIFs). Context recognizes the time and space in which the human made the error. As opposed to *omission* defined above, *commission* refers to inappropriate human actions. Chronology refers to the later released HRA methods. Still though, there is overlap between HRA methods, thereby classifying some methods as 1.5th generation (Boring, 2007).

First and second generation HRA methods are static in nature—capturing human performance a specific point in time (Boring, 2007). Third generation methods explain how a change in one PIF affects other PIFs and the eventual event progression. These newer methods also consider dynamic progression—PIFs may change throughout the course of an event, for example, fatigue may increase throughout an eight-hour workday (Boring, 2007). Additionally, a dynamic initiator is when a sudden change in the scenario affects the PIFs.

As the HRA methods have evolved, so have the complexities of PIFs and the understanding of PIFs on human performance. In the cybersecurity context, this is apparent in how cybersecurity researchers think about the context that cognitive factors influence inappropriate human actions (commission). Additionally, dynamic CS-PIFs that evolve over time (dynamic progression; e.g. fatigue over course of the day), and changes in a scenario that affect PIFs (dynamic initiator; e.g. social engineering attack on

emotion) are other dimensions to consider. In the next section, performance influencing factors will be examined. A brief human error literature summary is shown in Table 2.

Table 2

Summary of Human Error Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Boring, 2007	Theoretical			Outlines evolution of Human Reliability Analysis (HRA) methods and describes transition from static to dynamic HRA.
French et al., 2011	Theoretical			Human reliability analysis methods have historically been focused on low-level simple tasks and do not account for multi-dimensional factors that contribute system failure in complex systems.
Pollini et al., 2021	Empirical study: Questionnaire, scenario-based analysis, field	11 managers, 44 IT experts, 69 users	Individual, organizational, and	Provided evidence that organizational, human factors,

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
	observation, focus group, interviews		technological factors	and technical systems interact to improve security posture
Siponen & Vance, 2010	Empirical study via scenario method	54 information security professionals	Neutralization and Intention to Violate IS Security Policy	Neutralization is a strong predictor of intention to violate IS Security Policy.
Stanton et al., 2005	Empirical study via interview, behavior rating exercise, and survey	110 individuals interviewed, 49 IT SMEs conducted behavior rating exercise, and 1167 US end users surveyed to obtain self-reports of their password-related behaviors.	End User Behavior	Developed six-element category of end-user behavior, between two dimensions: intentionality (malicious, neutral, benevolent) and technical expertise (low, medium, high).

Performance Influencing Factors

In the discipline of human reliability—there have been numerous Human Reliability Analysis (HRA) methods developed with intentions to understand and mitigate causes of human error in safety systems. Within HRA, Performance Influencing Factors (PIFs) (also previously called Performance Shaping Factors (PSF)) are the variables that affect human performance leading to human error (Franciosi et al., 2019; Groth, 2009; Holland et al., 2019). PIFs can be internal (individual) or external (situation or environment)

factors (Boring et al., 2007; Franciosi et al., 2019). Internal PIF examples include stress, education, and experience; external PSF examples include environmental factors (e.g. temperature, noise), management, and procedures (Boring et al., 2007; Franciosi et al., 2019). When categorizing or measuring PIFs, it is important for reliability and validity to distinguish between direct and indirect PIFs: direct PIFs can be measured directly and indirect PSFs cannot be measured directly—where the magnitude of the PSF can only be determined subjectively (Alavi et al., 2016; Boring et al., 2007).

As discussed in previous sections, human error is problematic in creating vulnerabilities that lead to data breaches. Scholars and practitioners often point at the “human element” as the largest threat to cybersecurity (Goode et al., 2018; Evans et al., 2019; Karjalainen & Siponen, 2011; Schultz, 2005). Not often, is the cybersecurity “human element” examined with the scrutiny and detail that is seen in safety-related human reliability analysis methods (Evans et al., 2019). More common though, are that the human element constructs that attribute to cybersecurity lapses examined in isolation.

Additionally, several researchers have identified that several factors work together to affect the chance of human error; for example, Dekker (2006), using the local rationality principle stated that people do reasonable things given their goals (i.e. motivation), knowledge (i.e. experience), and focus of attention (i.e. awareness). Carlton and Levy (2017) alternatively attributed higher levels of knowledge, skills, and abilities to lower levels of human error. Security policies, SETA and computer monitoring directly influences user perceptions of sanctions, which in turn affect IS misuse intention (D’Arcy et al., 2009). Siponen (2000) described that “performance depends on ability, motivation, and working conditions” (p. 33). Other researchers found that a lack of knowledge and

training, failure to follow security procedures, carelessness, lack of supervision, and the lack of concentration were contributors to cybersecurity human error (Ahmed et al., 2012; Pollini et al., 2021). Carayon and Smith (2000) developed the Balance Theory, integrating various bodies of literature to understand the design of work factors that affect individual's human performance (Pollini et al., 2021).

Although not referred to as performance influencing factors in the cybersecurity literature, many of the same PIFs in safety contexts exist in cybersecurity contexts. For example, the Integrated Human Event Analysis System (IDHEAS) HRA method lists the following as common high-level PIFs in HRA methods: time available, task complexity, workload, Human-System Interfaces (HSIs), procedures, training/knowledge, experience, work process, stress, and fatigue (fitness-for-duty) (Xing et al., 2017). In the SPAR-H HRA Method, eight PIFs were identified, and their combination in influencing human error was explored (Gertman et al., 2005).

In the next few sections, major PIFs that are common among both contexts will be reviewed. This is not an exhaustive literature review for each PIF, as each construct could possibly warrant their own dissertation. Instead, the literature review on PIFs provides an overview of each construct, the subconstructs, and observed interdependencies with other constructs to influence human performance and human error in cybersecurity contexts. Specifically, six PIFs will be examined: Organizational Cybersecurity; Cybersecurity Policy and Procedures; Cybersecurity Education, Training, and Awareness; Ergonomics, Cybersecurity Knowledge, Skills, and Abilities; and Employee Cybersecurity Fitness for Duty. A brief performance influencing factors literature summary is shown in Table 3.

Table 3

Summary of Performance Influencing Factors Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Boring et al., 2007	Theoretical			Proposed two categories of performance shaping factors: direct and indirect. Direct PSFs can be measured directly, and Indirect PSFs can be measured through another factor. Recognizing the difference reduces measurement error in HRA.
Carayon & Smith, 2000	Analysis			Expansion of Balance Theory— which defines how different levels of the organization (individual, task, environment, technology, and organization) affect an individual— positively or negatively.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Groth, 2009	Model development		Organization-based (e.g. Training program, safety culture, procedures), Team-based (e.g. communication, direct supervision, team cohesion), Person-based (e.g. attention, physical and psychological abilities, knowledge, experience), Machine/design-based factors, Situation-based factors (e.g. task load, time load), Stressor-based factors.	Developed a causal model which displays visual relationship between Performance Shaping Factors (PSFs) leading to human error. PSFs can have organizational or personal components. Many errors were a result of team and organizational factors.
Holland et al., 2019	Content analysis and focus groups	82 incident reports	Treatment related problem solving, distractions / interruptions, high workload, staff unfamiliarity with procedure, use variability of error prevention strategy, therapist miscommunication, procedure and roles variability, equipment	89% of sample was slip/lapse error type, 11% were mistake error type. Treatment related Problem solving and distractions and interruptions were highest causal factors

Organizational Cybersecurity

Definition

Organizational cybersecurity is a high-level CS-PIF that includes cybersecurity culture and organizational control. In a quantitative study, Friedlander and Evans (1997) found that culture explained 30% of safety human error among three electric company cases. Deal and Kennedy (1982) described culture as the most important factor in deciding the success of an organization. Culture is a unit that resides in individuals and is also a force that drives individuals' behavior inside and outside of an organization (Schein, 2009). Cultures are inherent within each social group, family, community, organization and country, and each member of a unit is affected by and affects the culture thereby acting as both a member and leader simultaneously (Schein, 2009). Schein (2009) defined culture as:

a pattern of shared tacit assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems. (p. 27)

Schein (2009) cautioned against trying to understand culture by oversimplifying it—“the way we do things around here” and “our basic values” are manifestations of culture; culture actually is better understood as existing at three levels: Artifacts, Espoused Values, and Underlying Assumptions (Curado et al., 2021; Schein, 2009). The description and relationship of the three levels of culture is shown in Figure 8. Provided that culture is encapsulated in several levels—culture has profound implications of being stable and difficult to change (Schein, 2009). Understanding the underlying concepts of culture will allow us to better understand the cybersecurity subculture (Huang & Pearlson, 2019). Of further note, it is possible for organizations to have multiple

cybersecurity subcultures—consisting of various groups of employees differentiated by geographical location, job level, generation group, gender, or religion (da Veiga & Martins, 2017). Da Veiga (2016) defined cybersecurity culture as “the intentional and unintentional manner in which cyberspace is utilized from an international, national, organizational or individual perspective in the context of the attitudes, assumptions, beliefs, values, and knowledge of the cyber user” (p. 1008).

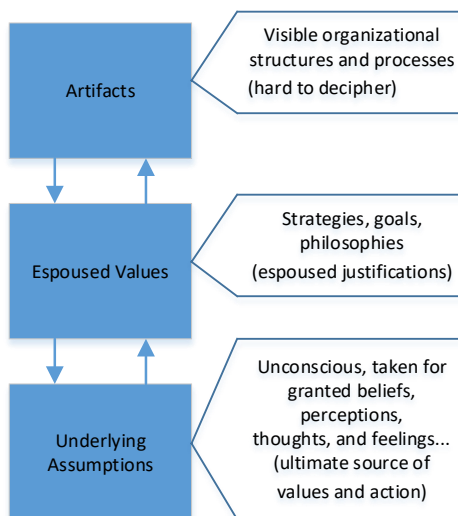


Figure 8: The Three Levels of Culture. Adapted from Schein (2009)

Vroom and von Solms (2004) applied Schein’s three levels of culture to cybersecurity. They categorized locked doors as an example of an artifact, senior executive cybersecurity policy as an example of espoused values, and at the subconscious individual level—the “underlying beliefs and values of the people in the company” as underlying assumptions (Vroom & von Solms, 2004, p. 196). Security culture can have a profound effect on the security of the organization as it ties into all aspects of the organization (Reegård et al., 2019; Vroom & von Solms, 2004).

The layers in Schein’s culture taxonomy also affect the layer above or below it, as shown in Figure 8 (see also Reegård et al., 2019). An example provided by Vroom and

von Solms (2004): “Shared knowledge of the information security policies and an underlying belief in the importance of information security would result in a change in behaviour of individuals and eventually in the organization as a whole” (p. 196). There are dependencies between the organization and the individual on shaping the culture: the organization shapes the individual and the individual shapes the organization.

Organizational Control

Organizational control is a factor involved with directing and motivating individuals to comply with organizational objectives (Boss et al., 2009; Reegård et al., 2019). Behavior control is when managers specify how they would like employees to behave and rewarding them when they comply; outcome control is when targets are articulated to employees and employees are rewarded when the target is achieved. Clan control is when managers and employees have shared values and norms, and behave with such values and norms.

Technical controls alone do not achieve security—management involvement with creating and enforcing security policies is also necessary (Stewart & Jürjens, 2017). Employees are sometimes resistant to complying with security policies—when this happens, security fails. Employee’s perception of mandatory enforcement and management oversight is effective in complying with security policies. Boss et al. (2009) examined what factors affect the perception of mandatoriness and how does mandatoriness affect compliance behavior. Boss et al. (2009) defined mandatoriness as “the degree to which individuals perceive that compliance with existing security policies and procedures is compulsory or expected within the organization” (p. 153).

Controls are implemented in organizations to motivate individuals to comply with desired behavior (Li et al., 2019). When management implements a control, it is implied that compliance is required—otherwise, management would not have communicated the control. Boss et al. (2009) found that specification and evaluation are critical aspects of exercising control attributing to individual perceptions of mandatoriness. Specification is the communication of controls through formal documented policies and procedures and evaluation is the oversight or verification that employees are complying with prescribed policies and procedures. The perceived mandatoriness also contributes to security precautions taken.

Organizational Cybersecurity CS-PIF Interaction

Alnatheer et al. (2012) developed an information security measurement model to distinguish which factors influence security culture and which factors constitute security culture. Through eight qualitative interviews with information security experts from various organizations and industries, they discovered that top management involvement in information security, information security policy enforcement, and security training drive security culture. Others argue that top management involvement in information security are both a component and influencer of information security culture (Gcaza & von Solms, 2017; Thomson & von Solms, 2005). Additionally, information security management protects information assets and reduces risks with technology and management processes (Chang & Lin, 2007; Reegård et al., 2019)

Alnatheer et al. (2012) found that collective security awareness and security ownership were reflections for security culture. The security awareness in this context is from the perspective of the employees—“A state where users in an organisation are

aware, ideally committed to, of their security mission” (Siponen, 2000, p. 31), as opposed to the security awareness in SETA—which is in the perspective of the organization providing the awareness. Alnatheer et al. (2012) also described regarding security ownership, “it is important for staff in any organisation to understand their security roles and responsibilities, in order to enhance their security performance and thus the organisation’s security performance” (p. 5).

Culture’s influence on human performance is apparent in safety (Friedlander & Evans, 1997) and security (Gcaza et al., 2017; Vroom & von Solms, 2004) disciplines (Reegård et al., 2019). Culture is a reflection and impacts all aspects of an organization: shared knowledge of information security policies and attitudes towards information security (Reegård et al., 2019; Vroom & von Solms, 2004); motivation and compliance, SETA, policies and procedures (Boss et al., 2009; Gcaza & von Solms, 2017); collective security awareness and security ownership (Alnatheer et al., 2012); fitness for duty (Gertman et al., 2005; Pollini et al., 2021); and behavior (Schein, 2009). Culture has been recognized as an organizational-based PIF (Whaley et al., 2016). A brief organizational cybersecurity literature summary is shown in Table 4.

Table 4

Summary of Organizational Cybersecurity Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Alnatheer et al., 2012	Empirical study via interview and survey	8 interviews of IT experts of various industries to specify constructs, survey of 254	Factors constituting security culture (security awareness and security ownership) and	Interviews: Specification of what influences security culture and constitutes

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
		employees of various Saudi Arabian organizations to validate information security culture model	influencing security culture (top management involvement in information security and information security policy enforcement)	security culture.
Boss et al., 2009	Empirical study via survey	1698 employees from a large medical center in southeastern United States	Mandatoriness and security policies	If an individual perceives that security policies or procedures are mandatory, they will comply.
Da Veiga & Martins, 2017	Empirical study via case study with survey questionnaire	A financial services organization was subject of case study, employees surveyed on four different years: 2006 (n=1941), 2007 (n=1571), 2010 (n=2320), 2013 (n=2159). The organization operated across twelve countries at the time of the last survey.	Dominant IS culture and IS subculture	Dominant IS culture and IS subcultures defined. Also, high risk subcultures can be improved with targeted interventions.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Friedlander & Evans, 1997	Empirical study via survey	~1,00 employees	Organizational culture and human error	Organizational culture significant (30%) to occurrence of human error.
Huang & Pearlson, 2019	Model development via focus group interview, and validation via case study	60 senior executives, managers, and researchers from large global and US based companies of various industries	External influences; organizational mechanisms; cybersecurity beliefs, values, attitudes; behaviors	<i>Organizational Cybersecurity Culture Model</i> was developed using literature and focus group, and validated by identifying constructs in strong security culture organization
Vroom & von Solms, 2004	Theoretical		Artifacts, espoused values, and basic assumptions	Auditing and enforcing information security behavior is difficult, a softer and more indirect approach in gradually changing the security culture will eventually change the behavior of individuals in an unforced manner.

Cybersecurity Policies and Procedures

Definition

Policies and procedures work in tandem to guide behaviors in an organization (Reegård et al., 2019; von Solms & von Solms, 2004). Policies communicate guidance and procedures for employees to comply with to meet the wishes of management, and procedures provide how employees should comply from a procedural perspective (Reegård et al., 2019; von Solms & von Solms). Policies and procedures are related; for example, procedures to properly discard anything with sensitive information may prevent a hard copy data breach, but a policy must require for it to be enforced (Verizon, 2017).

Vroom and von Solms (2004) defined information security policies as “the processes and procedures that the employee should adhere to in order to protect the confidentiality, integrity and availability of information and other valuable assets” (p. 192). In other words, a policy is a medium for management to communicate messages to employees (Reegård et al., 2019; von Solms & von Solms, 2004). In the case of an information security policy, management communicate and dictate on how employees should behave with respect to information security. It provides the organization with a strategy and defines the working culture and expected behaviors of employees (Buckley et al., 2014).

Cram et al. (2017) described three levels of security policies. The enterprise information security policy, also known as the security program policy, is the highest-level security policy that defines strategic direction, scope, and tone for the organization’s security efforts (Cram et al., 2017). Issue-specific security policies operate at one level below, and address specific technologies such as e-mail, use of personal electronic devices, or the configuration of organizational workstations (Cram et al., 2017). The final

level of policies are technical security policies that define user-facing, but define the configuration or maintenance of a system (Cram et al., 2017). The issue-specific security policy level more directly affects employees and user, as the enterprise information security policy is more philosophical, and the technical security policies is more aligned with computer security (Cram et al., 2017).

Information security policies provide acceptable use expectations to the users, and is related to the security culture and security awareness campaigns within the organization (Buckley et al., 2014; Cram et al., 2017). Not only must a policy be created and implemented, but it must also be meaningful, communicated effectively, and be understood, for the policy to be successful (Buckley et al., 2014; Cram et al., 2017; Vroom & von Solms, 2004).

Although there are insider threats that have malicious motives, many simply choose to ignore security policies (Gcaza et al., 2017; Herath & Rao, 2009; Zimmermann & Renaud, 2019). They may rationalize their violations and unknowingly (and mistakenly) create vulnerabilities. Barlow et al. (2013) provided the following example: “employees may choose to share a network password because they rationalize that no one is being injured as a result of their actions. These rationalizations cause even non-malicious employees to knowingly violate security policies” (p. 2). The mere existence and promulgation of IS Security Policies is not enough—employees must also comply with the policies (Gcaza et al., 2017; Pahnla et al., 2007; Siponen & Vance, 2010).

Compliance

There are numerous studies that attempt to explain why users do and do not comply with organizational security policies (Boss et al., 2015; Bulgurcu et al., 2010; D’Arcy &

Lowry, 2019; Herath & Rao, 2009; Siponen & Vance, 2010; Vance et al., 2020).

Attitude, normative beliefs (culture), and habits have a significant effect on intention to comply with information security policies, but more importantly, the quality of the information within the policies has a significant effect on the actual compliance (D'Arcy & Lowry, 2019; Pahlila et al., 2007). The substance of what is in the policy is important. For example, D'Arcy et al. (2009) found that a user's perceived severity of sanction (written in policy) has a direct negative effect on IS misuse intention. Policies can also address both intentional and unintentional insider threats—with topics such as integration and deterrence for intentional threats, and motivation, training, ergonomics, pressure, workload, and awareness for unintentional insider threats (Reegård et al., 2019; Yayla, 2011).

Siponen and Vance (2010) provided supplementing theories on why employees comply (or don't comply) with information security policies: general deterrence theory and neutralization theory. The criminological theory of general deterrence focuses on disincentives or sanctions to dissuade policy non-compliance (and persuade towards policy compliance), with two subconstructs: "(1) certainty of sanction and (2) severity of sanction" (Straub, 1990, p. 258). Neutralization theory suggest that persons rationalize their violative behaviors; an example Siponen and Vance (2010) provided: "a person performing a deviant action justifies his/her behavior by claiming that no damage will really be done. In this way, the person avoids guilt by reasoning that there is no criminal behavior involved; after all, no one got hurt" (p. 489). In this research, what's important to realize is that policies must be communicated so that users may understand the sanctions that are in place and to understand why (rationalization) certain policies are in

place (Barlow et al., 2013). Other predictive factors for user intention to violate IS security policies are shame, moral beliefs and perceived benefits (Vance & Siponen, 2012). Moody et al. (2018) proposed a unified model of 11 theories, to explain security policy compliance.

Security policies alone do not directly reduce the occurrence or severity of security breaches, to include those caused by human error (Pollini et al., 2021). It is speculated that security policies, along with other factors—security culture compatibility, awareness programs, enforcement—work together to improve human performance and mitigate human error (Doherty & Fulford, 2005; Enrici et al., 2010; Reegård et al., 2019). In summary, cybersecurity policies and procedures direct management’s strategy (culture) and execution, but to be effective, they must be communicated (SETA). The importance of policies and procedures are also observed in HRA methods (Forester et al., 2006; Swain & Guttman, 1983). A brief policies and procedures literature summary is shown in Table 5.

Table 5

Summary of Cybersecurity Policies and Procedures Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Buckley et al., 2014	Empirical investigation	15 security policies against 60 accidental insider threat cases	Enterprise security policies and accidental insider compromise	Developed accidental insider threat classification scheme to identify central components, and to assess policies.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Cram et al., 2017	Literature Review and Theoretical	114 papers	Keywords: Security policies, literature review,	Created initial research framework to synthesize current research and identify gaps on security policies
Herath & Rao, 2009	Empirical study via survey	312 employees from 78 organizations	Constructs from General Deterrence Theory, Protection Motivation Theory, Theory of Planned Behavior, Decomposed Theory of Planned Behavior, Organizational Commitment	Organizational, environmental, and behavioral factors affect adoption of information security policies and procedures.
Moody et al., 2018	Meta-analysis and empirical survey	Review of 11 security policy compliance theories, 274 Finland university graduates for study 1, 393 Finland university graduates for study 2	Response efficacy, threat, habit, role values, fear, intention neutralization, reactance	Developed and empirically examined Unified Model of Information Security Policy Compliance (UMISPC).
Von Solms & von Solms, 2004	Theoretical		Information security polices and information security culture	Information security policies prescribe actions and

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Vroom & von Solms, 2004	Theoretical		Artifacts, espoused values, and basic assumptions	behaviors of employees, but they must be communicated and align with corporate culture to be effective. Auditing and enforcing information security behavior is difficult, a softer and more indirect approach in gradually changing the security culture will eventually change the behavior of individuals in an unforced manner.
Siponen & Vance, 2010	Empirical study via scenario method	54 information security professionals	Neutralization and Intention to Violate IS Security Policy	Neutralization is a strong predictor of intention to violate IS Security Policy.

Cybersecurity Education, Training, and Awareness

Definition

Education, training, and awareness are three separate, but complementary functions that produce a knowledgeable individual in a specific function. For example, physicians

go to medical school to formally learn about their trade (education), but in many countries, they must also complete “rotations”—training—to practice medicine. Alternatively, airline pilots must complete a requisite number of flight *training* hours before getting their license, and the airlines that hire them may provide *awareness* programs to notify of recent airline mishaps (Shappell et al., 2007), to increase awareness and reduce complacency. Consider the education and training required to get a driver’s license, and the flashing LED signs on the highway that alert drivers to “slow down” when it’s raining, or when a traffic delay is imminent.

Education, training, and awareness in security contexts serve similar purposes. The mere existence of effective security policies and procedures serve no purpose if they are not communicated to users (Alshboul & Streff, 2017). SETA programs are designed to educate, train and make employees aware of the organizational requirements. Quality Cybersecurity Education, Training, and Awareness (CETA) programs “raise employee awareness of responsibilities in relation to their organizations’ information assets, provide instruction on the consequences of abuse, and develop the necessary foundational cybersecurity skills to help fulfill these requirements” (Goode et al., 2018, p. 70). Table 6 (adapted from Caballero, 2009, p. 249) provides high-level differences between the three.

Table 6

Matrix of security teaching methods and measures that can be implemented

	Awareness	Training	Education
Attribute:	“What”	“How”	“Why”
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding

	Awareness	Training	Education
Teaching Method:	<u>Media</u> -Videos -Newsletters -Posters, etc.	<u>Practical Instruction</u> -Lecture -Case study workshop -Hands-on practice	<u>Theoretical Instruction</u> -Discussion Seminar -Background reading
Test Measure:	True/False Multiple Choice (identity learning)	Problem Solving (apply learning)	Essay (interpret learning)
Impact Timeframe	Short-term	Intermediate	Long-term

Cybersecurity Education

Using socio-technical philosophies, it is important to address the “why” in cybersecurity education, on why certain policies and procedures are in place in order to increase user motivation and compliance (Goode et al., 2018; Siponen, 2000). Persuasion techniques are recommended so that listeners can internalize the principles (Siponen, 2000). Cybersecurity education programs are more structured in nature and will impact users for a longer period (Caballero, 2009).

Cybersecurity Training

Training in organizations has been shown to improve competitiveness, motivation, creativity, and attitude (Bernardino & Curado, 2020). It has also been shown to improve knowledge, skills, and long-term performance; although small to medium sized enterprises find it more difficult to offer training activities with their limited resources (Caballero, 2009; Curado & Sousa, 2021). In safety, the Federal Railroad Administration imposed requirements that require railroad companies to maintain training programs that would reduce the amount of human error caused accidents (American Society of Safety

Professionals, 2012); the same can be true of security. Non-malicious insider threats can be minimized through employee cybersecurity training (Hua & Bapna, 2013; Huang & Pearlson, 2019) by improving compliance behavior (Puhakainen & Siponen, 2010) and skills (Siponen, 2000).

Additionally, cybersecurity training with lessons learned of prior errors may help future users from committing the same errors (Dormann & Frese, 1994; Huang & Pearlson, 2019). In psychophysiological experimentation, Holroyd and Coles (2002) reaffirmed *reinforcement learning* where actions producing positive feelings are likely to be occur again in the future, and actions producing negative feelings (e.g. errors) are less likely to occur again. This is more ideally realized in cybersecurity training scenarios, such as embedded training email systems used to train users to recognize and avoid email phishing attacks (Kumaraguru et al., 2007).

Cybersecurity Awareness

Cybersecurity awareness programs reinforce the “what” and are short term reminders to cybersecurity compliance (Caballero, 2009). Social psychological techniques can be implemented in cybersecurity awareness programs to modify attitudes and consequently, behaviors (Pollini et al., 2021; Thomson & von Solms, 1998). The specifics of techniques are beyond the scope of this dissertation; it is important to note that the quality of the cybersecurity awareness program is important for the individual to receive and comply with the message.

CETA by and large is important for cybersecurity human performance, but is also tied to other aspects. Reegård et al. (2019) (and von Solms & von Solms, 2004) tied the communication of policies to the cybersecurity culture of an organization, and CETA has

been found to positively influence cybersecurity culture (da Veiga & Martins, 2015). CETA has also been attributed to changes in Information Security (IS) knowledge, IS attitude, IS normative beliefs, IS intention, and ultimately IS behaviors (Khan et al., 2011; Huang & Pearlson, 2019). Cybersecurity training improves knowledge and skills, motivates personnel, and improves attitudes (Rouse, 1985). Finally, Siponen (2000) ties cybersecurity education to motivation, cybersecurity training to skills, and cybersecurity awareness programs to increased cybersecurity awareness, which aligns well with the constructs of CETA to the constructs of competency (see Figure 9). A brief CETA literature summary is shown in Table 7.

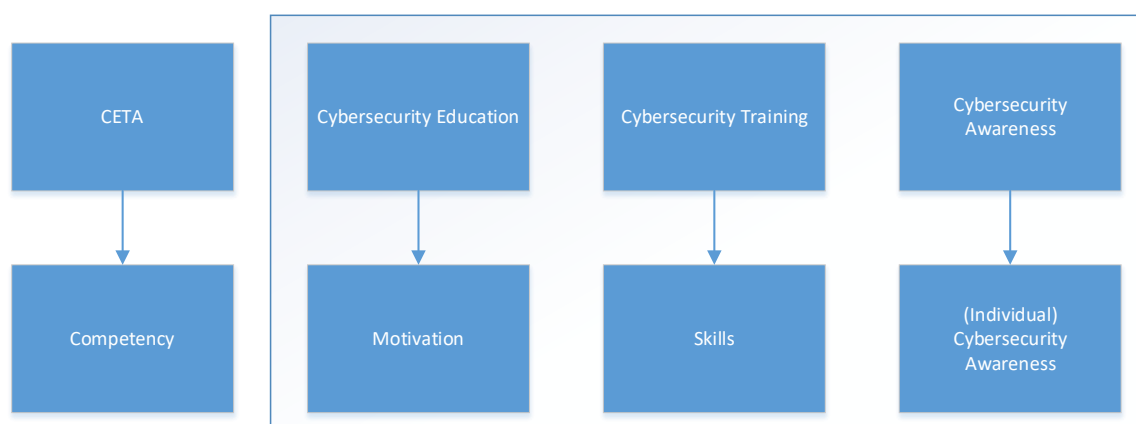


Figure 9: CETA to Competency Relationship

Table 7

Summary of Cybersecurity Education, Training, and Awareness Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Da Veiga & Martins, 2015	Empirical study via case study with survey questionnaire	A financial services organization was subject of case study, employees surveyed on	Eight constructs to measure employee perception to protect information (i.e. information	Information security training and awareness positively influences information

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Goode et al., 2018	Delphi study	four different years: 2006 (n=1941), 2007 (n=1571), 2010 (n=2320), 2013 (n=2159). The organization operated across twelve countries at the time of the last survey.	security culture), training and awareness	security culture.
Goode et al., 2018	Delphi study	38 cybersecurity subject matter experts	Two program types (typical and socio-technical) and 3 CCA categories (Awareness of: policy, SETA, and monitoring).	Development and SME validation of SETA topics to be covered, the most valuable method for delivery, to what degree these factors play a part in employees' IS security practice.
Puhakainen & Siponen, 2010	Action research via interviews, survey, and participatory observation	16 participants surveyed and interviewed	IS security training and employee compliance	After surveying, interviewing, and observing employee problems with regard to information security policy, the researchers intervened to recognize

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Siponen, 2000	Conceptual analysis		Review of approaches of information security awareness and education programs, to include descriptive vs prescriptive, behavioral and persuasive strategies	existing and uncover new research streams for security training effectiveness. A successful information security awareness program leading to user commitment and compliance requires a systematic approach.

Cybersecurity Knowledge, Skills, and Abilities

Definition

In this research, Cybersecurity Knowledge, Skills, and Abilities (CKSA) will be used to encompass the various terms to describe how well a user is equipped to perform. Some of the terms described herein are awareness, skill, and self-efficacy. These attributes are developed through osmosis with the cybersecurity culture, via CETA programs and the cybersecurity policy doctrines, or the user may have developed in previous organizations or contexts. These terms are relatively static in nature—developed over time. Personal norms and attitude—internalized factors lasting months to years—are included in this section (Pollini et al., 2021; Siponen, 2000). In the cybersecurity context, Safa et al.

(2016) defined personal norms as “the employees’ values and views on information security compliance with organizational policies” (p. 5) and attitude as an individual’s “positive or negative feeling towards engaging in specific behavior” (p. 5).

Employee Cybersecurity Awareness

Information security awareness, Information Security Policy (ISP) awareness, cybersecurity countermeasures awareness, and other terms, have been used to define how well a user responds in cybersecurity contexts. Wiley et al. (2020) defined information security awareness as “the extent to which employees understand the significance of their organisation’s information security policies, rules, and guidelines, and the extent to which they behave in accordance with these policies, rules and guidelines (p. 2). Siponen (2000) explicitly described that awareness reduces human error. In addition, there is also ISP awareness, which is the level of awareness of organizational security policies and procedures (Alshboul & Streff, 2017). Cybersecurity countermeasures awareness is the “employee awareness of security policies, SETA programs, computer monitoring, and computer sanctions” (Goode et al., 2018, p. 69). Information security awareness and ISP awareness are both seen to affect employee behavior (Alshboul & Streff, 2017; Enrici et al., 2010).

Employee Cybersecurity Skill and Employee Cybersecurity Competency

Employee Cybersecurity Skill is the “combination of abilities, knowledge, and experience that enables an individual to complete a task well” (Carlton & Levy, 2017, p. 17). Over time, this skill transitions into competency (Carlton & Levy). Developing skill begins with (1) declarative knowledge (i.e. initial skill acquisition), followed by (2) procedural knowledge (i.e. developing internalized patterns), and ending with (3)

autonomous (i.e. executing the ability autonomously) (Anderson, 1982; Carlton & Levy). The three-step incremental process (Anderson; Carlton & Levy) appears compatible with Rasmussen's (1983) SRK human performance framework (see Figure 10); Marcolin et al. (2000) described competency as an antecedent to performance. Information security experience is the "familiarity with information security incidents, skills and the ability to prevent, manage, and mitigate the risk of information security events" (Safa et al., 2016, p. 4). General computer and internet experience have been shown to improve self-efficacy in information security (Rhee et al. 2009).

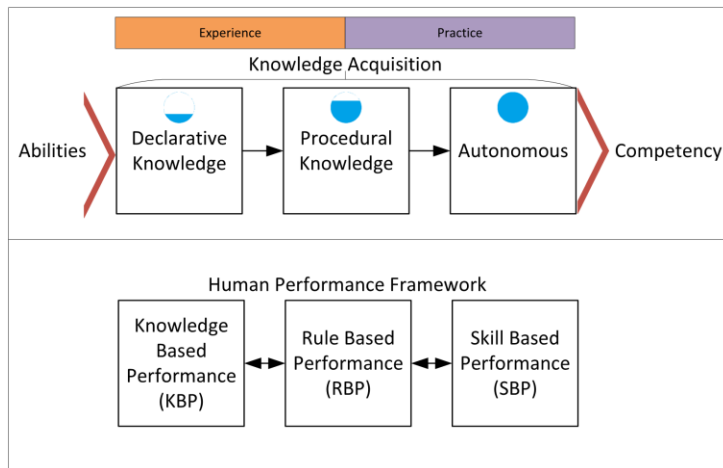


Figure 10: Competency Development and Human Performance Levels Comparison

Cybersecurity Self-Efficacy

An important construct of social cognitive theory, cybersecurity self-efficacy is a form of self-evaluation that is an antecedent to behavior (Rhee et al. 2009). Individuals with high levels of self-efficacy have stronger convictions to utilize their motivation and cognitive resources to likely increase cyber resilience (Huang & Pearlson, 2019).

Following the identification that the context of self-efficacy is important (Agarwal et al., 2000; Huang & Pearlson, 2019; Rhee et al., 2009), several SE concepts in information

systems have emerged. Computer self-efficacy is an individual's conviction of their ability to use a computer (Rhee et al., 2009). Self-Efficacy in Information Security (SEIS) is the belief in one's ability to protect information and information systems from "unauthorized disclosure, modification, loss, destruction, and lack of availability" (Rhee et al., 2009, p. 818); SEIS contributes to stronger cybersecurity conscious behaviors (Enrici et al., 2010; Huang & Pearlson, 2019).

Awareness, skill, and self-efficacy individually affect performance. Choi et al. (2013) examined Cybersecurity Skills (CS), Computer Self-Efficacy (CSE), and Cybersecurity Countermeasures Awareness (CCA) and their relationship to computer misuse intention. Surveying 185 US government employees in the US Northwest, their findings indicated that CS, CSE, and CCA directly or indirectly influenced the user's intention to misuse information systems (Choi et al., 2013). With respect to disregard to information security policies, competency is a key factor in determining violations. Interesting to note, is that PIFs within CKSA interact to influence performance and intentions (Choi et al., 2013), but also can interact with other PIFs such as fitness for duty to influence performance (Baxter & Bass, 1998; Wiley et al., 2020). A brief CKSA literature summary is shown in Table 8.

Table 8

Summary of Cybersecurity Knowledge, Skills, and Abilities Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Carlton & Levy, 2017	Theoretical		Knowledge, ability, experience, cybersecurity	Strong cybersecurity skills are paramount for cyber

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
			skills, competency	threat mitigation; poor cybersecurity skills result in IT human error.
Choi et al., 2013	Empirical study via survey	185 employees of a large government transportation agency in the northeastern US	Computer Self-Efficacy (CSE), Cybersecurity Countermeasures Awareness (CCA), Cybersecurity Skills (CS), Computer Misuse Intention (CMI)	Users' Awareness of Computer Monitoring (UAC-M) and Cybersecurity Initiative Skill (CIS) are significant to CMI. UAC-M and CSE were significant to cybersecurity computing skill. Users' Awareness of Security Policy (UAS-P) were significant to Cybersecurity Action Skill (CAS).
Enrici et al., 2010	Literature Review and Theoretical	105 papers	Keywords: Human, psychology, cognitive, information, technology, security	Defined four levels of psychological relevance approach to security: human errors approach,

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Rhee et al., 2009	Empirical study via survey	415 graduate students	Self efficacy in Information Security (SEIS)	human factors approach, cognitive approach, and psychology of security approach. SEIS is an excellent predictor in individuals' security practice for technology and behaviors, and higher efforts to enhance information security.
Safa et al., 2016	Empirical study via survey	462 employees from 4 Malaysian companies of different industries.	Information Security Organizational Policies and Procedures (ISOP) attitude toward compliance, knowledge sharing, collaboration, intervention, experience, attachment, commitment, personal norms, ISOP compliance behavioral intentions	Knowledge sharing, collaboration, intervention, experience, commitment, and personal norms have significant effect on attitude toward compliance with ISOP, which in turn has significant effect on ISOP

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Siponen, 2000	Conceptual analysis		Review of approaches of information security awareness and education programs, to include descriptive vs prescriptive, behavioral and persuasive strategies	compliance behavioral intentions. A successful information security awareness program leading to user commitment and compliance requires a systematic approach.

Employee Cybersecurity Fitness for Duty

Definition

The human mind is extremely complex—and every mind is different, with infinite perspectives, emotions, assumptions, and motivations. Additionally, the numerous variables that influence the mind can change from moment to moment, and can affect every individual differently. This PIF—Employee Cybersecurity Fitness for Duty (CFFD)—is a dynamic state which involves the numerous cognitive, behavioral, and physiological factors that may compose a human’s state of mind and state of being. CFFD can be defined as “whether or not the individual performing the task is physically and mentally fit to perform the task at the time” (Gertman et al., 2005, p. 25). Fitness for duty and related PIFs have a strong presence in safety contexts; in this research, we will include stress, fatigue, situation awareness, emotion, and motivation into fitness for duty.

Stress

Specified in safety contexts explicitly and often, stress is one of the more important factors contributing to performance (Swain & Guttman, 1983; Xing et al., 2017); stress is the human response to a stressor, and “psychological and physiological stresses result from a work environment in which the demands placed on the operator by the system do not conform to his capabilities and limitations” (Swain & Guttman, 1983, p. 2-5). There should be an optimum level of stress—with too much stress being disruptive, and too little stress leading to insufficient arousal to stay alert (Swain & Guttman, 1983). Stress’ role as a contributor to human performance and human error is not as prevalent in cybersecurity contexts—even the literature that focuses on psychological components (Enrici et al., 2010; Pollini et al., 2021; Schultz, 2005). Stress is identified as a factor in certain cybersecurity contexts—such as the medical industry (Liginlal et al., 2009). Liginlal et al. (2009) also include fatigue in this context.

Fatigue

The National Highway Traffic Safety Administration (2018) reported that 795 deaths in the US were a result from drowsy-driving-related crashes in 2017. In organizational contexts, fatigue is an important factor contributing to human error, being closely tied to human factors engineering and ergonomics (Liu & Guo, 2016). Organizations that require individuals to work unusually long hours may cause fatigued workers (Swain & Guttman, 1983). Additionally, physically or cognitively demanding tasks may contribute to fatigue (Gertman et al., 2005; Paul & Dykstra, 2017). Heightened stress and fatigue may attribute to reduced situation awareness (Endsley, 1995; Whaley et al.,

2016). Fatigue can also result in the failure to follow policies and procedures (Luciano et al., 2010).

Situation Awareness

Endsley (1995) defined situation awareness as “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future” (p. 36). Situation awareness is a state of knowledge, pertaining only to the state of a dynamic environment (Endsley, 1995). Situation Awareness (SA) directly affects task performance (Baxter & Bass, 1998) and decision making (Endsley, 2015). In cybersecurity contexts, the design of human-computer interface is important to ensure that high levels of sustained situation awareness are not required, as it could lead to human errors (Boyce et al., 2011; Pollini et al., 2021).

Emotion

Emotion is phenomena of feelings, behaviors and bodily reactions aroused by external events, and the reactions to those events (Cairns et al., 2014). A two-dimension construct consisting of valence (either positive or negative) and the degree of emotional arousal can categorize an individual’s emotional state; emotion is known to affect a person’s thinking: positive emotions enhance decision making whereas negative emotions impairs processing task efficiency (Cairns et al., 2014). A person is more likely to be make errors when they are emotionally upset (Swain & Guttman, 1983).

Motivation

Motivation dictates the difference between what people can do (maximum performance) and what people will do (typical performance) (Klehe & Anderson, 2007). The more intense the motivation, the more mental and physical efforts will be exerted

towards the achievement of a goal (Whaley et al., 2016). Skills and abilities, in combination with motivation, influence performance (Klehe & Anderson, 2007; Pollini et al., 2021).

Fitness for duty is a dynamic state: an individual can be in an ideal state (rested, happy, motivated, etc.) one day delivering good performance, and the next day be in a problematic state (fatigued, miserable, low situation awareness, etc.), caused by personal or other reasons. Fitness for duty has been shown in safety contexts to directly affect performance. Ergonomics has been shown to improve fitness for duty. A brief CFFD literature summary is shown in Table 9.

Table 9

Summary of Employee Cybersecurity Fitness for Duty Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Cairns et al., 2014	Empirical study via laboratory experiment	28 University of York participants	PowerPoint images to measure valence, computer spreadsheet to measure number entry performance	Users in a negative emotional state are likely to make more number entry errors; users in a positive emotional state are likely to make less number entry errors.
Klehe & Anderson, 2007	Empirical study via laboratory experiment	138 psychology department university	Typical and maximum performance, self-efficacy, task valence,	Motivation is higher under evaluative situations (maximum

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
		student volunteers	motivation, declarative knowledge, and procedural skills	performance) than under typical situations (typical performance), thus participants work harder under maximum performance.
Liginlal et al., 2009	Empirical study via interview	9 privacy officers from medium to large-sized healthcare organizations	Perceived causes of human error leading to privacy breaches	Proposed error management strategies and measures, consisting of 3 dimensions: organization- focused, human- focused, and technology- focused.
Luciano et al., 2010	Theoretical		User Behavior, Information Security Policy Awareness, Information Security Awareness, Organizational Environment, Stressful Work Conditions	From the information security literature, recognized interactions of various factors that contribute to information security breaches, to include stressful work conditions and

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Paul & Dykstra, 2017	Empirical study via survey	126 participants, 361 operation assessments, in a 14 month window	Fatigue, frustration, cognitive workload	organizational environment. National Security Agency operators’ fatigue, frustration, and cognitive workload increased during tactical cyber operations— leads to errors, decreased performance, burnout.

Ergonomics

Definition

In this section, the term ergonomics was chosen to describe concepts such as Human-Computer Interaction (HCI) and macroergonomics. Included in this definition is everything to include the environment, context, technology, supervisory and organizational factors that affect the user’s performance. Improved performance and reduced human error can be accomplished using a multidimensional lens, considering psychological, contextual, environmental, and technological factors (Carayon & Smith, 2000; Rouse, 1985; Zimmermann & Renaud, 2019).

Human-Computer Interaction

In computer and cybersecurity contexts, systems were originally engineered around the system, without much regard to the user (system-centered design), whereas the successor User-Centered Design (UCD) begins with the user's needs, abilities, and knowledge in mind (Renaud & Flowerday, 2017; Rizzo et al., 1996). A goal of Human-Computer Interaction is to minimize human errors through technology design (Rizzo et al., 1996; Abdolrahmani et al., 2017). The *Principle of Least Surprise* tells engineers to design their applications as the user expects them (Bratus et al., 2008). Many errors can be attributed to misuse or improper use of technology, and interaction between human and technology is of critical importance to security (Enrici et al., 2010; Pollini et al., 2021; Renaud & Flowerday, 2017). In fact, the fields of Human-Computer Interaction and Security (HCISEC) (Maxion & Reeder, 2005) and Human-Centered Security and Privacy (HCSP) (Renaud & Flowerday, 2017) have emerged to address the role users play in securing systems.

Macroergonomics

Within human factors engineering, macroergonomics is the science and practice which considers the physical, organizational and social contexts in which interventions are implemented (Carayon, 2009; Zimmerman & Renaud, 2019). Simply possessing the knowledge will not guarantee that the knowledge will be accessible when needed—the context and environment are critical factors (Pollini et al., 2021; Rizzo et al., 1996). Poor psychosocial work factors (e.g. workload and job control), poor physical work factors (e.g. workplace layout, noise, and lighting), and unsuitable cognitive work factors (e.g. cognitive demands) may influence job stressors (Carayon, 2009; Carayon & Smith, 2000; Pollini et al., 2021), and increase human error (Paul & Dykstra, 2017, Rouse, 1985).

As described previously, context matters. Ergonomics may appear insignificant to human performance in typical office environments with typical operating systems and applications. In some environments or contexts though, ergonomics may be more significant. For example, novel software may be developed in a way that may cause users to leave sensitive file unsecured more often. Other situations may require users to work dangerously long hours or increased workload, causing diminished performance. A brief ergonomics literature summary is shown in Table 10.

Table 10

Summary of Ergonomics Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Carayon & Smith, 2000	Analysis			Expansion of Balance Theory— which defines how different levels of the organization (individual, task, environment, technology, and organization) affect an individual— positively or negatively.
Carayon, 2009	Analysis			Renewed examination of Balance Theory has included how different levels of

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Maxion & Reeder, 2005	Empirical study via laboratory experiment	24 students and research staff volunteers from Carnegie Mellon University.	Task relevant information: speed, accuracy, and errors.	organization affect both qualitative and quantitative level of individual performance. Participants performed better (less error, higher speed) on task using experimental interface (Salmon) than on control interface (Windows XP file-permissions interface).
Renaud & Flowerday, 2017	Literature Review and Theoretical	1600 research paper titles from ACM Conference on Human Factors in Computing Systems	HCI waves of maturity: first, second, and third waves	Meta review of Human-Centered Security & Privacy (HCSP) research, and categorized state of the research progress in 3 waves; majority of research as of 2017 still in first wave

PIF Relationship

Carayon and Smith (2000)'s Balance Theory of Job Design has five elements that interact to produce a *stress load*. These five elements are the environment, the task, technologies, organizational factors, and the individual. The interactions of the elements create physical and psychological stressors, such as fatigue, decision-making, emotion, and motivation. If sustained, these stressors can be detrimental to health, safety, and performance (Carayon & Smith, 2000). Inversely, these factors can also produce positive outcomes, such as motivation and increased performance (Pollini et al., 2021). At the root of the Balance Theory concept is that all elements must be considered to improve performance, health and safety (Carayon & Smith, 2000; Pollini et al., 2021; Rouse, 1985). Compatible with the PIFs discussed, Figure 11 maps the five elements to the PIFs.

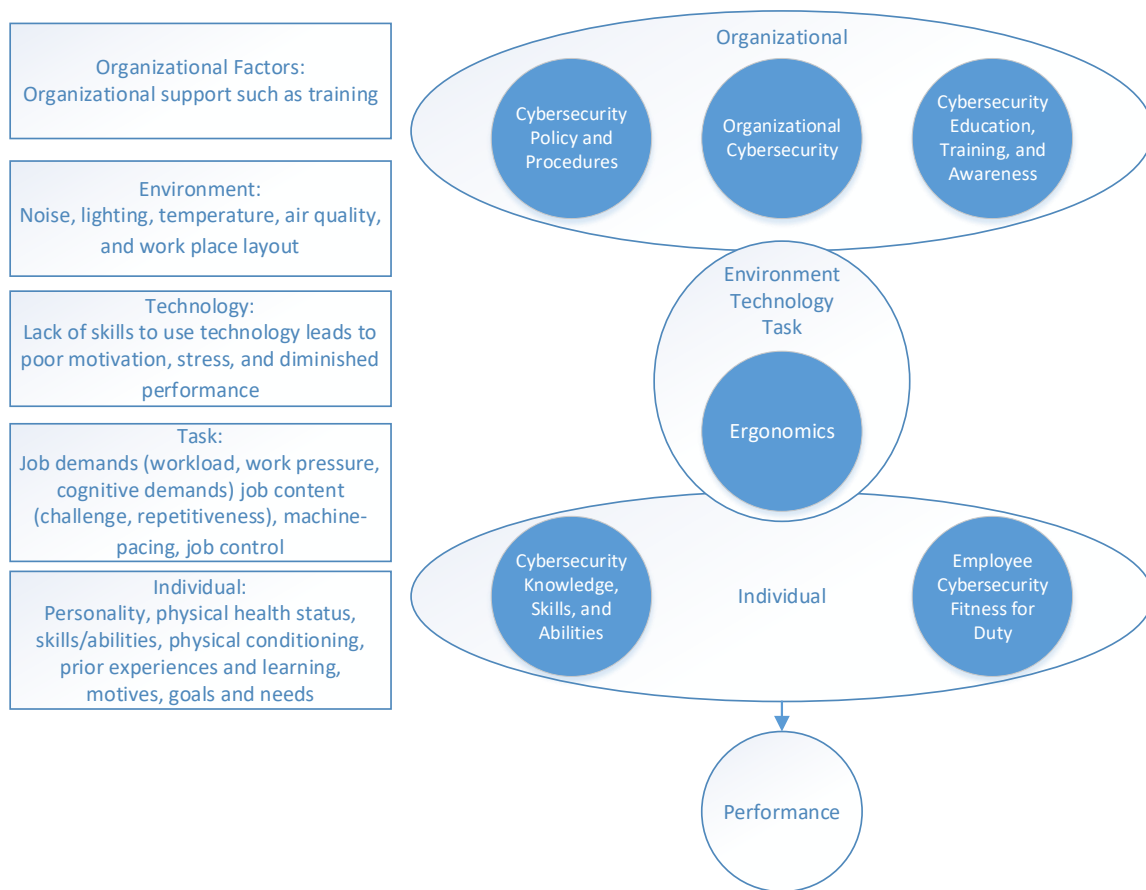


Figure 11: Balance Theory of Job Design on Performance. Adapted from Carayon and Smith (2000)

Summary of What is Known and Unknown in the Research Literature

This literature review examined three major topics: data breaches, human error, and performance influencing factors. In the Data Breaches section, context is provided to further establish relevance and significance of the research problem. In the Human Error section, further details of human performance and human error is uncovered, as found in the psychology and safety literature.

The Performance Influencing Factors section goes in depth on PIFs identified to be present in cybersecurity contexts. Literature from the cybersecurity, management, safety, sociology, and psychology fields were utilized to provide a comprehensive look at factors that influence human performance. Six higher-order CS-PIFs were reviewed: organizational cybersecurity; cybersecurity policy and procedures; cybersecurity education, training, and awareness; cybersecurity knowledge, skills, and abilities; employee cybersecurity fitness for duty; and ergonomics. First-order CS-PIFs were uncovered in research goal one, and the second-order (higher-order) sets were validated in research goal two.

Although cybersecurity human error has been identified as problematic in the cybersecurity literature (Evans et al., 2019; Kraemer & Carayon, 2007; Liginlal et al., 2009; Zimmermann & Renaud, 2019) and data breach reports (Ponemon Institute, 2021; Verizon, 2021), what was missing (i.e. unknown) in the cybersecurity literature is that there are underlying factors and causes for human error. Much more so, is that a comprehensive CS-PIF list was non-existent. Additionally, what was also unknown was the realization that the combination of CS-PIFs may interact to cause human error, and quite possibly, a specific type of human error.

Chapter 3

Methodology

Overview of Research Design

This research was based on an interpretive philosophy—assumed that human-error caused data breaches are context specific, and multiple factors may combine or interact to lead to human error. Additionally, this research approach was inductive—it provided a holistically novel evaluation of factors that led to cybersecurity human errors resulting in real world data breaches (Pappas & Woodside, 2021). This research study examined case studies (data breaches), and qualitatively extrapolated data for analysis, and used fsQCA as the data method.

This study was comparative research using fsQCA. The research design comprised of two phases. The first phase was Instrument Development, which involved CS-PIF Identification (RQ1) and CS-PIF Validation (RQ2). The second phase was Fuzzy-set Qualitative Comparative Analysis: fsQCA Application (RQ3), and for alternative configurations, analyzed the type of breach (RQ4) and organization breached (RQ5) (see Figure 12). Phase 1 included CS-PIF identification and validation.

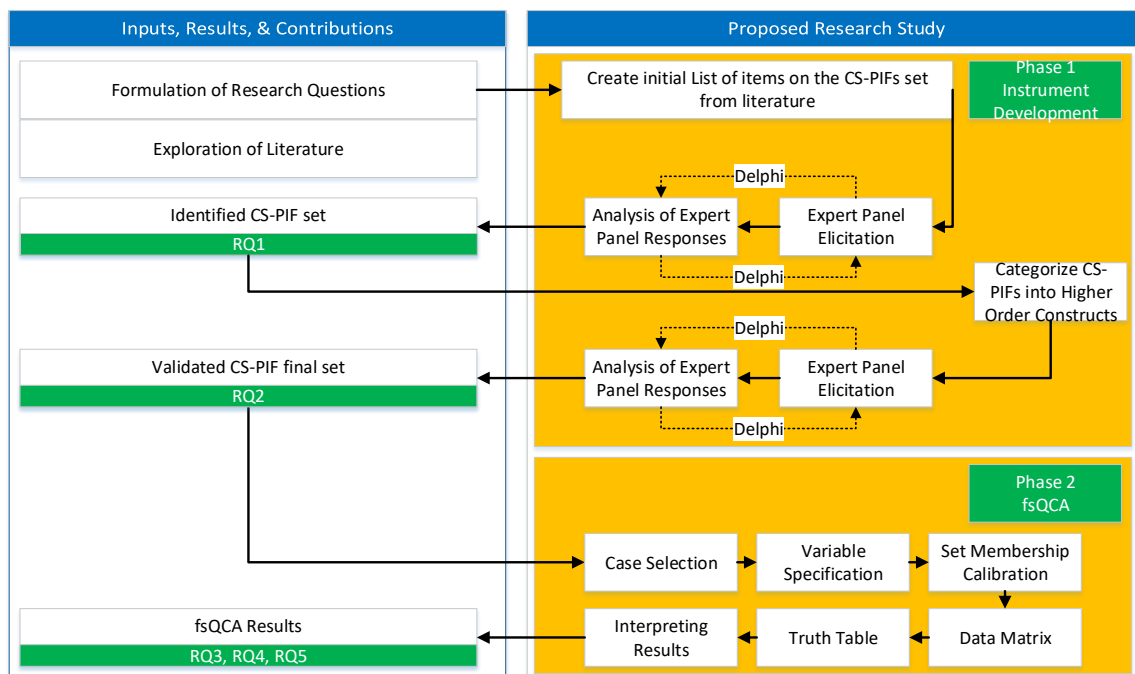


Figure 12: Research Design for Empirical Investigation Using Fuzzy-set Qualitative Comparative Analysis (fsQCA)

Phase 1: Instrument Development

In this research, two sets of constructs were measured: conditions and outcomes. As illustrated in Figure 2 (GEMC-DBF) previously, the conditions are the CS-PIFs—the factors that can influence human performance, and the outcome is the type of CS-HE (SBE, RBM, or KBM). The CS-HE types are identified and established—as developed in the psychological literature by Reason (1990). PIFs in cybersecurity contexts (CS-PIF) on the other hand, had yet to be holistically identified and validated in research. PIFs in safety contexts have varying range (i.e. count) per application with as few as one, with over 50 PIFs, or even applications with undefined amounts (Boring, 2010). Therefore, it was necessary to establish CS-PIFs because PIFs are context specific (Holland et al.,

2019). The Instrument Development process is illustrated in Figure 13 and explained in further detail next.

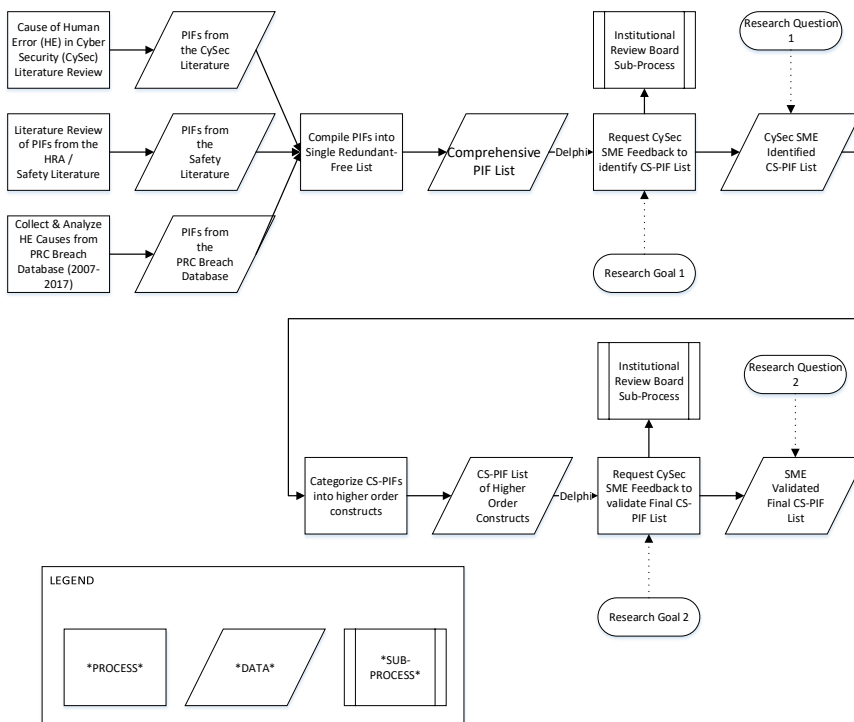


Figure 13: Instrument Development for Cybersecurity Performance Influencing Factors

CS-PIF Identification

This research developed a baseline of CS-PIFs using data triangulation: (1) by identifying and compiling causes of human error in the cybersecurity literature, (2) compiling PIFs from the safety literature, and (3) compiling PIFs from the actual data breach cases derived from PRC database. Data triangulation leverages the strength of one method on the others, and provides a more comprehensive understanding of a phenomenon of interest (Fusch et al., 2018; Sands & Roer-Strier, 2006). The three sources of PIFs were compiled into one redundant-free list. Cybersecurity SMEs were

used—using the Delphi technique—to identify the most common CS-PIFs. The Delphi technique is further described below.

CS-PIF Validation

The identified CS-PIFs were consolidated into higher-order CS-PIFs, and validated by SMEs, also using another phase of the Delphi technique. With regard to selecting causal conditions (in this case, CS-PIFs) for fsQCA—it was prudent to minimize the number of conditions selected for exploration within the cases (Douglas et al., 2020). The greater the number of conditions, the greater the possibility that each case will be unique in the condition configuration (Amenta & Poulsen, 1994; Douglas et al., 2020; Schneider & Wagemann, 2010). Marx et al.'s (2013) analysis of QCA studies found that the number of conditions range from two to 10, with most using only four to five conditions.

Expert Panel

It has been demonstrated previously that an analyst's subjective interpretation of human error in HRA has proven problematic as they may fail to take adequate consideration of the context, and different analysts may provide different results (Stanton, 2009). To account for this deficiency, 31 cybersecurity SMEs were used to provide feedback. The Delphi technique was used to utilize an expert panel to review the redundant-free PIF list and identify PIFs that could cause human error that could potentially lead to data breaches. The recruitment email used is presented in Appendix A.

The Delphi technique, also called Delphi methodology and Delphi method is appropriate when accurate information is unavailable and opinionated but informed input is important (Goode et al., 2018; Ramim & Lichvar, 2014). It is designed to encourage SME debate for consensus building, through “anonymity, iteration, and controlled

feedback” (Goode et al., 2018, p. 71). Similar to a peer review, the Delphi technique obtains a representative view by involving as many experts in the field as possible to provide feedback (Ramim & Lichvar, 2014). Cybersecurity SMEs were used as experts. Best practice suggests 15 to 30 cybersecurity professionals with various backgrounds, age, and education; consensus range from 55%-100%, with 70% as the standard (Goode et al., 2018).

Phase 2: Fuzzy-set Qualitative Comparative Analysis

Overview

fsQCA is a type of Qualitative Comparative Analysis (QCA) (Ragin, 2008). QCA is a formal comparative case-oriented research method and collection of techniques used to understand how different conditions combine to generate an outcome (Marx et al., 2013). QCA was introduced in 1987 by sociologist Charles Ragin for the social sciences and has spread across disciplines (Thomann & Maggetti, 2017).

The original version of QCA—Crisp-Set QCA (csQCA)—combines strengths of qualitative and quantitative methods, based on set theory and Boolean algebra (Marx et al., 2013; Pappas & Woodside, 2021). csQCA uses Boolean values—0 and 1—to assign set membership values for conditions and outcomes. Many conditions and outcomes, however, vary by level of degree of membership. The fuzzy-set theory is a mathematical system that allows partial membership in sets (Ragin, 2009; Zadeh, 1965). fsQCA was developed to address the deficiencies and, thus, a complement to csQCA as it allows partial membership based on fuzzy set calibration criteria established by the researcher (Ragin, 2009). Calibration is “the process of classifying conditions in each case from full membership (1.00) to full non-membership (0.00)” (Curado, 2017, p. 83).

fsQCA is useful for data exploration, synthesis, and typology building, by summarizing data and interpreting cases into a truth table of set relations (Marx et al., 2013). Therefore, fsQCA systematically integrates within-case and cross-case analysis (Marx et al., 2013). fsQCA is conjunctural in its logic and examines set relations for logical implications or hypotheses of necessary and sufficient conditions leading to outcomes (Balle et al., 2018; Schneider & Wagemann, 2010; Thomann & Maggetti, 2017). A necessary condition is present in all instances of an outcome; a sufficient condition by itself can produce the outcome (Marx et al., 2013; Ragin, 1999; Thomann & Maggetti, 2017). It must be noted that fsQCA is appropriate for detecting these types of set relations, but inadequate for detecting correlations (Schneider & Wagemann, 2010).

fsQCA has three aspects of causal complexity: conjunctural causation, equifinality, and causal asymmetry (Douglas et al., 2020; Pappas & Woodside, 2021). Conjunctural causation refers to the single conditions quite possibly not resulting in an outcome unless combined with other specific conditions, i.e. the “Swiss cheese model” (Thomann & Maggetti, 2017). Equifinality allows for different, mutually exclusive causal configurations leading to the same phenomenon (Thomann & Maggetti, 2017). Causal asymmetry refers to “the conditions explaining the occurrence of an outcome can differ from those explaining its nonoccurrence” (Thomann & Maggetti, 2017, p. 5). In addition, QCA rejects permanent causality as is seen in traditional statistical techniques, since QCA views causation as conjuncture and context specific (Berg-Schlosser et al., 2009).

Process

This research used fsQCA to evaluate the conjunctural causal relationship of CS-PIFs on the various CS-HE types that led to data breaches. Data breaches were the cases

examined, and the conditions (CS-PIFs) and outcomes (CS-HE) were identified for each case and coded based on fuzzy-set calibration (Basurto & Speer, 2012; Douglas et al., 2020). fsQCA research design has specific requirements including case selection, variable specification, and set membership calibration (Schneider & Wagemann, 2010). The raw data are then input into a data matrix, transformed into a truth table, then the solutions are interpreted (Thiem, 2017) (see Figure 12).

Case Selection

Cases of data breaches selected must have had enough information about the circumstances leading to the breach (the user's erroneous actions and the characteristics of the user and organization) to be able to make inferences on potential CS-PIF and CS-HE. Content analysis is a research technique to make inferences on textual data (Ayyagari, 2012; Gaur & Kumar, 2018). Further specification of case selection is presented in the *Population and Sample* section. fsQCA is an iterative process that requires the researcher to revisit cases and data—a “back-and-forth between ideas and evidence” (Thomann & Maggetti, 2017, p. 4).

Variable Specification

The variables in this research are the CS-PIFs and CS-HEs present or absent in data breach cases. CS-PIFs are identified in RQ1, and higher order sets used for fsQCA are validated in RQ2 (Douglas et al., 2020; Schneider & Wagemann, 2010). CS-HEs are SBE, RBM, and KBM. CS-PIFs and CS-HEs must be calibrated for fsQCA.

Set Membership Calibration

Fuzzy set membership must be calibrated; substantive and theoretical knowledge facilitates the pinpointing of qualitative states for a case to fall between full membership

and full non-membership of a set (Curado et al., 2016; Gonçalves et al., 2021). The scores were generated via the calibration of sets (Douglas et al., 2020; Schneider & Wagemann, 2010). Ragin (2009) asserted that:

Such calibration is possible only through the use of theoretical and substantive knowledge, which is essential to the specification of the three qualitative breakpoints: full membership (1), full non-membership (0), and the crossover point, where there is maximum ambiguity regarding whether a case is more “in” or more “out” of a set (0.5). (p. 90)

Data Matrix

Following calibration of the variables, the cases were manually reviewed using the content analysis technique. Inferences were made on the presence or absence of CS-PIFs for each case (data breach) and coded based on set membership calibration previously conducted. Additionally, the human error (SBE, RBM, and KBM) leading to the breach was coded based on the fsQCA calibration. The raw qualitative data were interpreted and coded into a data matrix: a spreadsheet with one axis being the data breach case, and the other axis being the CS-PIFs and CS-HEs data (Thiem, 2017).

Truth Table

Once all cases were reviewed and coded into the data matrix, the data file could then be uploaded into fsQCA software for transformation into the truth table. A truth table lists all possible logical combinations of causal conditions and outcomes (configurations) relating to the cases (Kraus et al., 2017; Ragin, 2008). Establishing a consistency score (0.8) will ensure a cutoff to determine conjunctural relationships (causal recipes) of CS-PIFs resulting in CS-HE. The fsQCA software calculates the three solutions (complex,

parsimonious, and intermediate) from the cases to provide indication of how certain conditions (CS-PIFs) combine to create outcomes (CS-HEs) (Santos et al., 2021).

Interpreting Results

The results of the fsQCA application provided data to be interpreted. The results answered RQ3: what are the alternative configurations of internal (individual) and external (organizational and contextual) CS-PIFs leading to (a) skill-based errors; (b) rule-based mistakes; and (c) knowledge-based mistakes resulting in the largest data breaches across multiple organization types from 2007 to 2019 in the US? Further investigation into the results allowed insight how the sufficient configurations interact to create different data breaches (RQ4), and different organizations (RQ5).

Reliability and Validity

Like other empirical social research methods, QCA establishes inference by using known facts (theoretical and substantive knowledge) to learn new facts (Ragin, 1999; Thomann & Maggetti, 2017). Establishing inference is completed by achieving internal validity (& measurement validity), external validity, and adopting a mode of reasoning (Thomann & Maggetti, 2017) (see Figure 14). Theory building--mode of reasoning--was established in the literature review; external and internal validity are described in the next two sections.

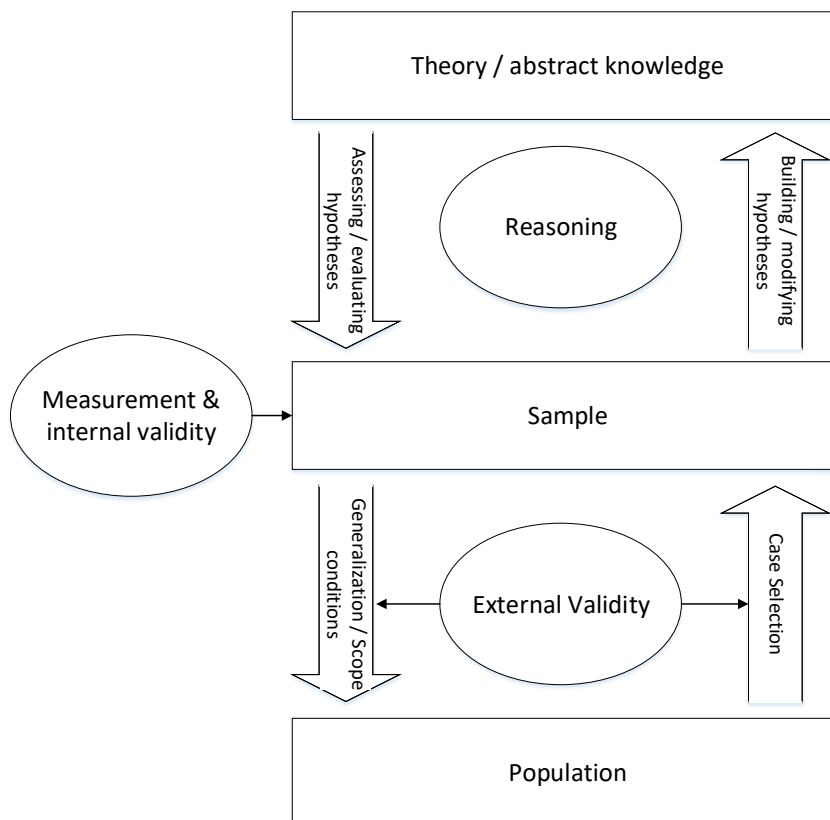


Figure 14: Components of Inference adapted from Thomann and Maggetti (2017)

External Validity

Modest generalization is achieved through the analysis of carefully selected cases (Thomann & Maggetti, 2017). In this research, the cases were data breaches. The data breaches selected were those reported on the PRC database that took place from 2007–2019, in the US. The top 100 data breaches from each organization type were examined, as to represent the range of industries and improve external validity (see Table 11, adapted from Privacy Rights Clearinghouse, 2021). The largest data breaches were selected as their scope of magnitude more likely results in more media coverage and details in revealing the conditions and outcomes leading to the breach. Because the sample size was not large in comparison to exclusively quantitative analysis, “cases are

selected for which obtaining in-depth knowledge is crucial, relevant, and feasible for answering the research question” (Thomann & Maggetti, 2017, p. 11).

Table 11

Organization Types

Code	Description
BSF	Businesses—Financial and Insurance Services
BSO	Businesses—Other
BSR	Businesses—Retail/Merchant—Include Online Retail
EDU	Educational Institutions
GOV	Government and Military
MED	Healthcare, Medical Providers and Medical Insurance Services
NGO	Nonprofits
UNKN	Unknown

Internal Validity and Measurement Validity

Familiarity with the cases before, during, and after QCA analysis was a requirement for improving internal validity and in-depth case knowledge (Schneider & Wagemann, 2010; Thomann & Maggetti, 2017). Data triangulation was used to examine each data breach case in the PRC dataset against various data breach databases and media reports; confirming validity of data breach data (Ayyagari, 2012; Fusch et al., 2018). Careful set membership calibration in addition to SME feedback, assisted in the accurate descriptive and explanatory inferences for cases and concepts under observation (Thomann & Maggetti, 2017). Proper and confident categorization required thorough understanding of the subject matter—CS-HE and CS-PIFs.

Population and Sample

To select the cases, and to understand which causes are relevant, Ragin (1999) recommended substantive literature review or an in-depth analysis of cases. Additionally,

fsQCA accepts purposeful sampling, that is, the researcher may select, add, or drop cases throughout their research, provided the cases share enough background characteristics (Rihoux & Ragin, 2009). This research explored publicly reported data breaches in the PRC database, and cross-examined with other sources (e.g. media outlets) for an exhaustive understanding of each breach–CS-PIFs and CS-HE (Ayyagari, 2012; Fusch et al., 2018).

PRC has been used in several studies examining data breaches (Ayyagari, 2012; Culnan & Williams, 2009; Rosati & Lynn, 2021). As explained in a previous section, the top 100 data breaches from each organization type within the PRC database were selected for the sample, to enhance external validity and due to the publicly availability content of larger breaches. Of those reviewed, only a proportionate number of cases were a result of human error. This resulted to the final case sample size of 102–exceeding the threshold for large-N QCA studies as defined by Rihoux et al (2013). Rihoux et al. (2013) analyzed QCA journal articles from 1984 to 2011; Table 12 shows the share of small-N, medium-N, and large-N QCA studies during this period.

Table 12

QCA Case Sample Size Share

Size	Criteria	Share (percentage)
Small-N	Less than 10 cases	12%
Medium-N	10–50 cases	60%
Large-N	More than 50 cases	28%

Data Analysis

Pre-Analysis Data Screening

Prior to data analysis, the data were examined and cleaned to resolve data irregularities (Levy, 2003). This is called pre-analysis data screening or pre-analysis data preparation. The first reason to do this is for data accuracy, to ensure the data scribed in the data matrix are accurate. This was accomplished by reviewing cases iteratively to ensure consistent condition and outcome scoring against the set membership calibration. Another reason for pre-analysis data screening is to ensure there were no missing data. With 800 cases reviewed, and multiple conditions and outcomes, it is imperative for fsQCA to use complete data to avoid inaccurate data analysis (de Block & Vis, 2019).

Data Analysis

There are several csQCA/fsQCA software packages with various features, algorithms, and outputs, used to conduct qualitative comparative analysis. The specific QCA software package used was fsQCA 3.1b for Windows 10, developed by Charles Ragin and Sean Davey (Ragin & Davey, 2017). Use of the software, required data to be inputted or imported in rows and columns (e.g. Excel or CSV format), with the rows representing the individual cases, and the columns representing the conditions and outcomes. Upon execution, the program outputs the solution(s) for interpretation of the results (Thiem & Duşa, 2013).

Resource Requirements

This research study obtained Institutional Review Board (IRB) approval for the cybersecurity SMEs that participated for CS-PIF identification and CS-PIF validation (See Appendix B). An online survey tool was used to collect responses from cybersecurity SMEs. Finally, fsQCA software was used for data input and fsQCA output.

Summary

This chapter defined the research methodology that was used to address the research goals. The research methodology used consisted of two main phases. The first phase was instrument development—identification and validation of CS-PIFs (conditions) using an expert panel (Delphi technique). The second phase progressed through the fsQCA process: case selection, variable specification, set membership calibration, data matrix, truth table, and interpretation of results.

Carefully administering the research methodology directly answered the Main Research Question: What is the conjunctural causal relationship, using configurational analysis, of internal (individual) and external (organizational and contextual) CS-PIFs leading to CS-HE that resulted in the largest data breaches across multiple organization types from 2007 to 2019 in the US? Additionally, the following research questions were answered as progressing through the two phases:

- RQ1. What are the cybersecurity SMEs' identified most common internal (individual) and external (organizational and contextual) CS-PIFs leading to CS-HE that result in data breaches?
- RQ2. What are the cybersecurity SMEs' validated higher-order set of the most common internal (individual) and external (organizational and contextual) CS-PIFs leading to human error that result in data breaches?
- RQ3. What are the alternative configurations of internal (individual) and external (organizational and contextual) CS-PIFs leading to (a) skill-based errors; (b) rule-based mistakes; and (c) knowledge-based mistakes resulting in the largest data breaches across multiple organization types from 2007 to 2019 in the US?

RQ4. What alternative configurations of CS-PIFs are responsible for CS-HE leading to various data breaches caused by: (a) unintended disclosure; (b) system misconfiguration; (c) social engineering, and (d) poor cybersecurity hygiene, in the largest data breaches across multiple organization types from 2007 to 2019 in the US?

RQ5. How are the alternative configurations of CS-PIFs on CS-HE leading to the largest data breaches across multiple organization types from 2007 to 2019 in the US, represented across (a) industry type and (b) company size?

Chapter 4

Results

Overview

This chapter covers Phase 1 and Phase 2 of the Research Design (Figure 12). Phase 1 (Instrument Development) used cybersecurity SMEs to identify 1st order CS-PIFs and validate 2nd order CS-PIFs, using the Delphi method. As a result, this answered Research Questions 1 and 2. Following Phase 1, Phase 2 (Fuzzy-set Qualitative Comparative Analysis) involved the processes of case selection, variable specification, set membership calibration, production of the truth table and interpretation of results. Eight hundred data breach cases were evaluated, which resulted in the positive identification of 291 data breaches that were caused by human error. Of those 291 cases, only 102 cases had enough qualitative information to transform into fuzzy-set values.

Instrument Development (Phase 1)

Thirty-one Cybersecurity SMEs were asked to identify the applicability of proposed common CS-PIFs (1st order), and to validate the appropriateness of the proposed categorization of higher order CS-PIFs (2nd order), using a Google Forms survey. Of the 31 SMEs requested, 25 SMEs of various backgrounds participated in the survey, meeting the 15 to 30 participant target. This response accounts to an 80.6% participation rate. The survey contained three sections: (1) External CS-PIFs; (2) Internal CS-PIFs; and (3)

Demographics. Section (1) and (2) have three sub-sections: (A) CS-PIF definitions are provided, (B) identification of 1st order CS-PIFs, and (C) validation of 2nd order CS-PIFs. The Survey Instrument is contained in Appendix C. Figure 15 outlines in red, Phase 1 of the Research Design.

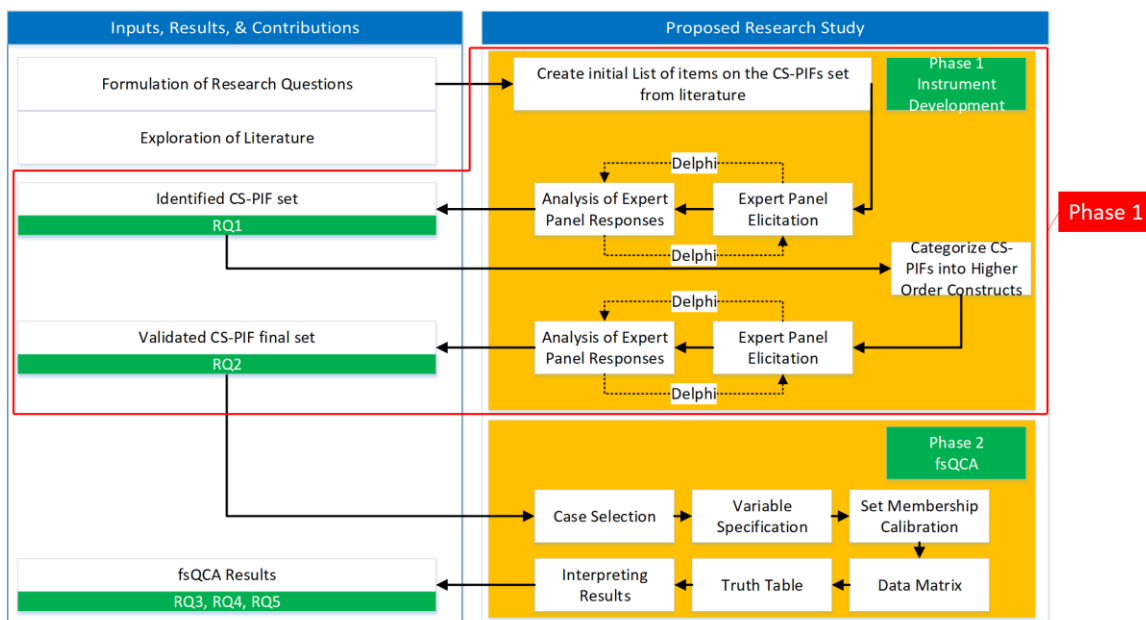


Figure 15: Phase 1 of the Research Design for Empirical Investigation using fsQCA

Demographic Analysis

Analysis of the demographic responses revealed that 76% of respondents were male, aligned with reported North America figures of 74% (International Information System Security Certification Consortium, 2020). Eighty percent of the respondents were between the ages of 31 and 60, with 12% below and 08% above the range. 92% of the respondents had at least a bachelor's degree, with one respondent having only a high school diploma, and one respondent having an associate's degree. Sixty percent of respondents had at least six years of cybersecurity experience, but provided the age brackets, it is assumed that individuals have supplemental experience in information

technology. A majority percentage (96%) of respondents work in industry, whereas only one respondent worked in academia. About half (48%) experienced a cybersecurity incident or data breach while they were in a management role. The demographics of the participants are shown in Table 13.

Table 13

Descriptive Statistics of SMEs (N=25)

Demographic Item	Frequency	Percentage
Gender:		
Male	19	76%
Female	6	24%
Age:		
20-30	3	12%
31-40	6	24%
41-50	6	24%
51-60	8	32%
61-70	2	08%
Highest Level of Education:		
Some College	1	04%
Associate's Degree	1	04%
Bachelor's Degree	7	28%
Master's Degree	12	48%
Doctoral/Medical/JD Degree	4	16%
Years of Experience in Cybersecurity:		
0-5 years	10	40%
6-10 years	6	24%
11-15 years	3	12%
16-20 years	3	12%
Over 12 years	3	12%
Years of Computer Use:		
11-20 years	5	20%
Over 20 years	20	80%
Current Employment:		
Academia	1	04%
Industry	24	96%
Experienced a Cybersecurity Incident or Data Breach in a Management Role:		
No	13	52%
Yes	12	48%

Identification of Common (1st Order) Cybersecurity Performance Influencing Factors

Survey participants were provided Common External CS-PIF definitions in Section 1A and Common Internal CS-PIF definitions in Section 2A. This provided a standard definition for the CS-PIFs as provided in the cybersecurity and safety literature. Based on the provided definitions and their expertise, the participants were asked to choose to Keep, Adjust or Remove each CS-PIF. They were also asked to provide comments if they chose to adjust or remove the CS-PIF. The external and internal 1st order CS-PIF identification results are examined in the next two sections.

External 1st Order CS-PIFs

Figure 16 reveals the survey results for external 1st order CS-PIFs as identified by cybersecurity SMEs. Keeping Cybersecurity Awareness as a 1st order external CS-PIF ranked lowest at 84%, indicating this is the Cybersecurity SME's least perceived important CS-PIF contributing to human error; 84% still exceeds the 70% SME threshold as discussed in Chapter 3. The average consensus for 1st order external CS-PIFs was 90%. Several interesting comments were provided by the SMEs. A summary is provided next.

Respondent 4 preferred the terms cybersecurity management or cybersecurity leadership, over organizational cybersecurity control. Respondent 6 recommended to add language to the Organizational Cybersecurity Control definition to include management and leadership commitment within the organization. Respondent 8 recommended that policies be written to the organization, and not just a template that was copied and pasted from another organization. Respondent 10 brought up the construct of "social cultural factors", in that employees want to help, hence succumbing to social engineering.

Respondent 16 agreed with procedures, but did not buy into policies, and felt that organizations only use them when it is convenient for them. Respondent 24 believed that cybersecurity culture in military and private organizations is not where it needs to be in equipping end users with the necessary education in cybersecurity concepts to protect organizations. None of the comments were indicative of requiring a change.

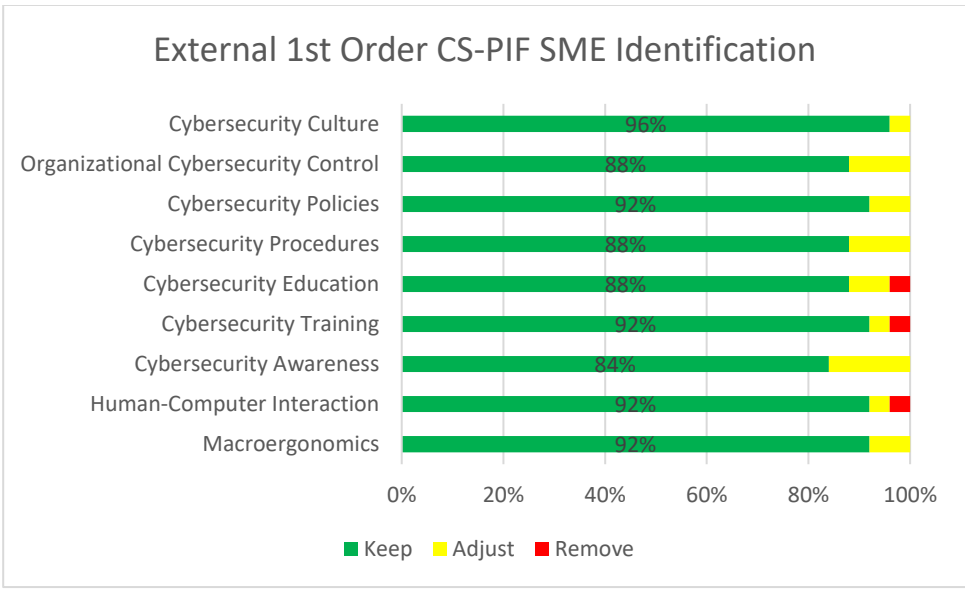


Figure 16: External 1st Order CS-PIF SME Identification (N=25)

Internal 1st Order CS-PIFs

Figure 17 reveals the survey results for internal 1st order CS-PIFs as identified by cybersecurity SMEs. Keeping Stress, Fatigue, and Emotion as 1st order Internal CS-PIFs ranked lowest at 84%, above the 70% SME threshold as discussed in Chapter 3. The average consensus for 1st order internal CS-PIFs was 92%. Several interesting comments were provided by the SMEs. A summary is provided next.

Respondent 2 recommended adding internal bribery as a 1st order CS-PIF. Respondent 6 recommended updating the definition of stress to reflect a cybersecurity perspective.

Respondent 24 was not sure why emotion was a CS-PIF and if it should be included. As in the external 1st order CS-PIFs, none of the comments were indicative of a required change.

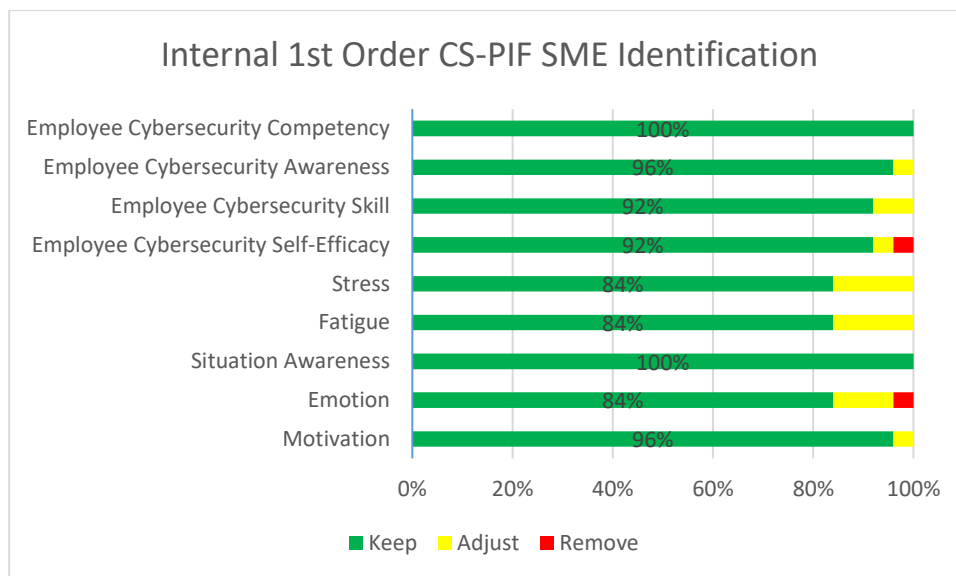


Figure 17: Internal 1st Order CS-PIF SME Identification (N=25)

Validation of Categorization of Higher Order (2nd Order) CS-PIFs

Following the identification of 1st Order External (Section 1B) and Internal (Section 2B) CS-PIFs, the participants were asked to validate 2nd Order External (Section 1C) and Internal (Section 2C) CS-PIFs. The participants were provided a proposed categorization and asked to rate the 2nd Order CS-PIF categorization, with the following criteria: (1) Absolutely Inappropriate, (2) Inappropriate, (3) Slightly Inappropriate, (4) Neutral, (5) Slightly Appropriate, (6) Appropriate, and (7) Absolutely Appropriate. If they selected (1) – (5), they were asked to provide recommended adjustments. The external and internal 2nd order CS-PIF validation results are examined in the next two sections.

External 2nd Order CS-PIFs

Figure 18 reveals the survey results for external 2nd order CS-PIFs as validated by cybersecurity SMEs. Validating Cybersecurity Policies and Procedures as a 2nd order CS-PIF was ranked lowest at 88%, above the 70% SME consensus threshold as discussed in Chapter 3. The average consensus for 2nd order external CS-PIFs was 93%. Several interesting comments were provided by the SMEs. A summary is provided next.

Respondent 4 was not sure if HCI should be separated from macroergonomics. Respondent 9 believed that cybersecurity human error occurs due to “fat finger” errors, and that external CS-PIFs have little effect on human error data breaches. Respondent 16 did not believe that cybersecurity policies and procedures needed to be combined into a 2nd order. Respondent 25 recommended adding “standards” to cybersecurity policies and procedures.

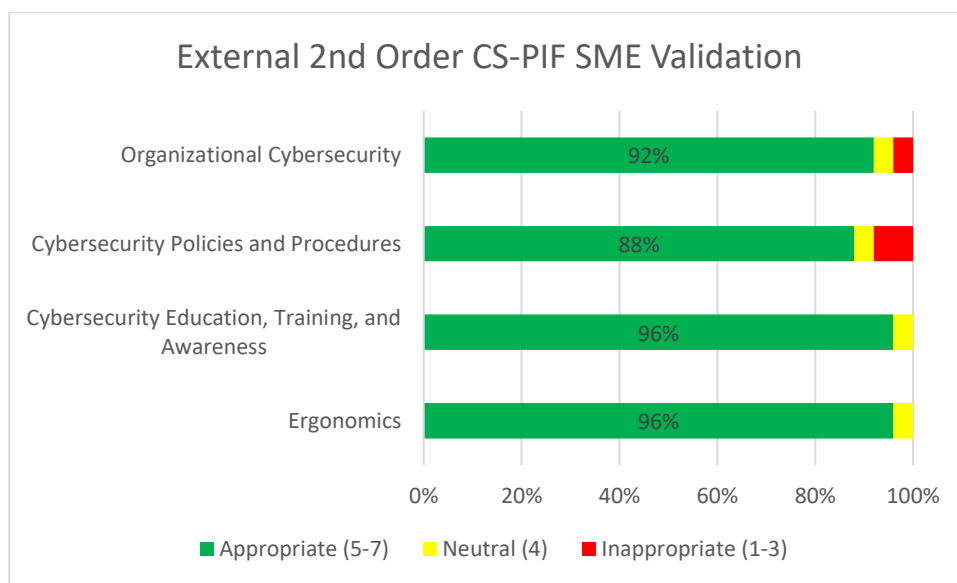


Figure 18: External 2nd Order CS-PIF SME Validation (N=25)

Internal 2nd Order CS-PIFs

Figure 19 reveals the survey results for internal 2nd order CS-PIFs as validated by cybersecurity SMEs. Validating Employee Cybersecurity Fitness for Duty as a 2nd order

CS-PIF was ranked lowest at 92%, above the 70% SME consensus threshold as discussed in Chapter 3. The average consensus for 2nd order internal CS-PIFs was 94%. Two comments from the respondents stood out. Respondent 4 felt there was insufficient delineation between self-efficacy and factors such as motivation; additionally, they believed cybersecurity fitness for duty was too “military” of a term, and recommended alternate terms like alertness, composure, readiness. Respondent 17 noted that an employee’s cybersecurity KSA may sometimes be deficient, and the manager’s work assignment or workload should be considered—indicating a relationship.

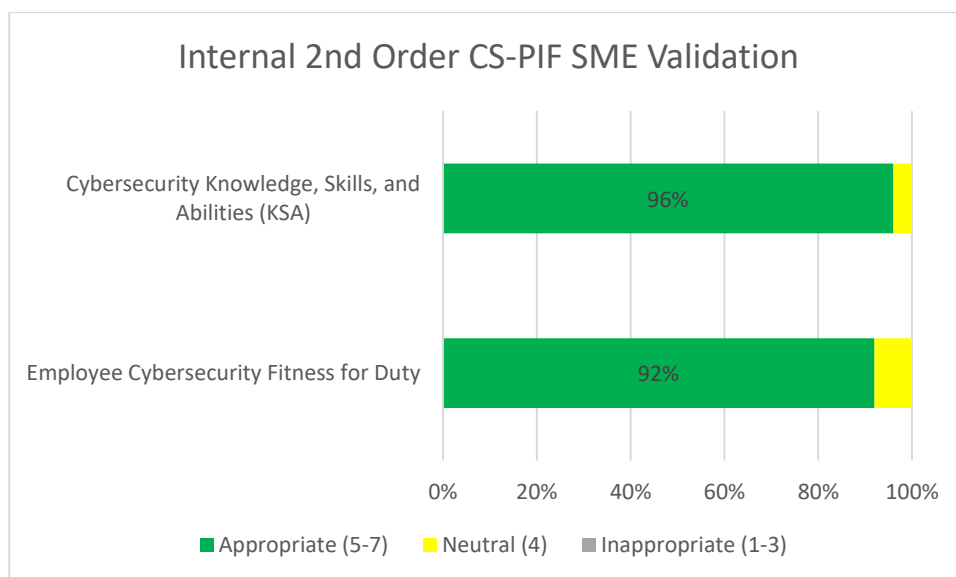


Figure 19: Internal 2nd Order CS-PIF SME Validation (N=25)

Results of the Instrument Development (Phase 1)

This study originally intended to have multiple rounds of SME feedback, but this study far exceeded the minimum consensus of 70% for the Delphi Method in the first round (Goode et al., 2018). The lowest subsection consensus was 84%, with an average consensus of 91% for 1st order CS-PIF identification, and 93.5% for 2nd order CS-PIF validation. By terminating SME feedback in the first round, this study avoided a

disadvantage of the Delphi method in that “during the course of multiple sequential rounds of collecting Delphi data some members of the experts may not return one or more of the survey questionnaires” (Kalaian & Kasim, 2012, p. 2). There was a risk in additional rounds by not having as much participation.

The proposed 1st Order Common Internal and External CS-PIFs were recognized by the SMEs as contributors to human error, leading to data breaches. Additionally, the proposed 2nd Order Categorization of CS-PIFs were validated by the SMEs to be appropriate. During case review, the presence or absence of 1st Order CS-PIFs was identified using fuzzy-set criteria. This 1st Order identification translates to 2nd Order CS-PIF categorization. The complete 1st Order and 2nd Order CS-PIFs and confidence scores are shown in Figure 20.

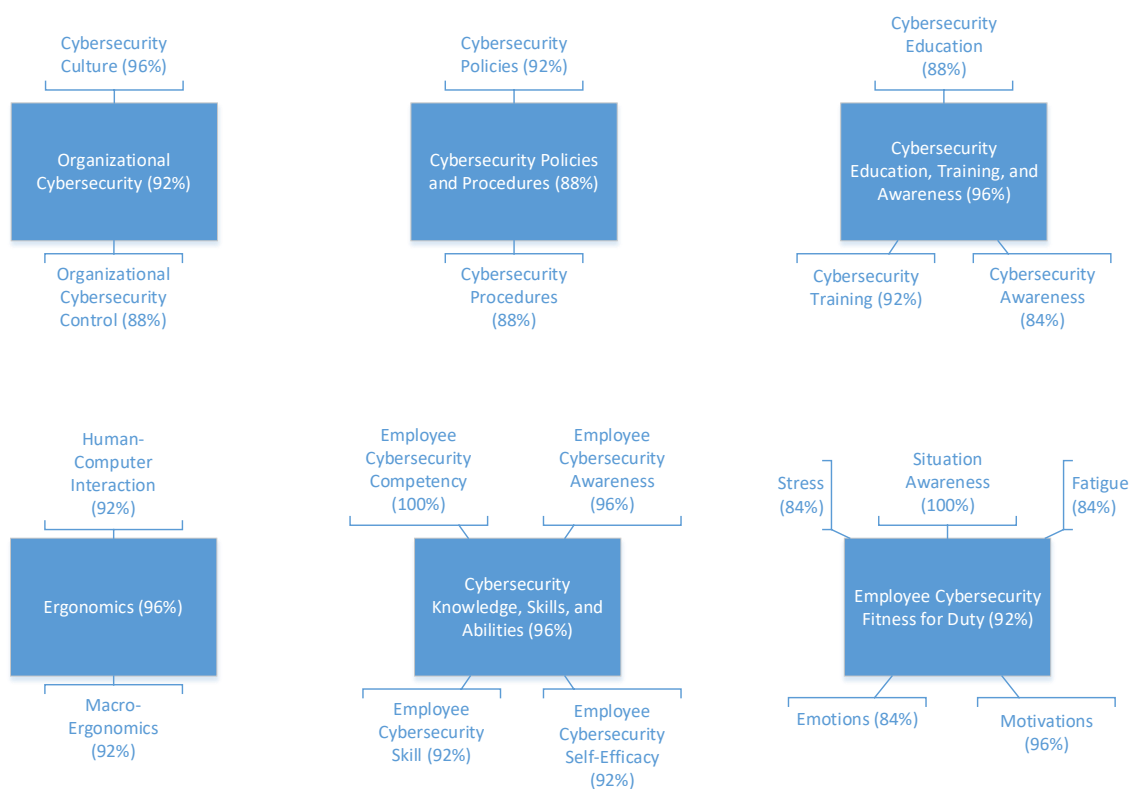


Figure 20: External and Internal 1st and 2nd Order CS-PIF SME Feedback Summary

Fuzzy-set Qualitative Comparative Analysis (Phase 2)

Phase 2 of the Research Design focused on the fsQCA process. It is a six-step process: case selection, variable specification, set membership calibration, data matrix, truth table, and interpreting results. Figure 21 outlines Phase 2 of the Research Design.

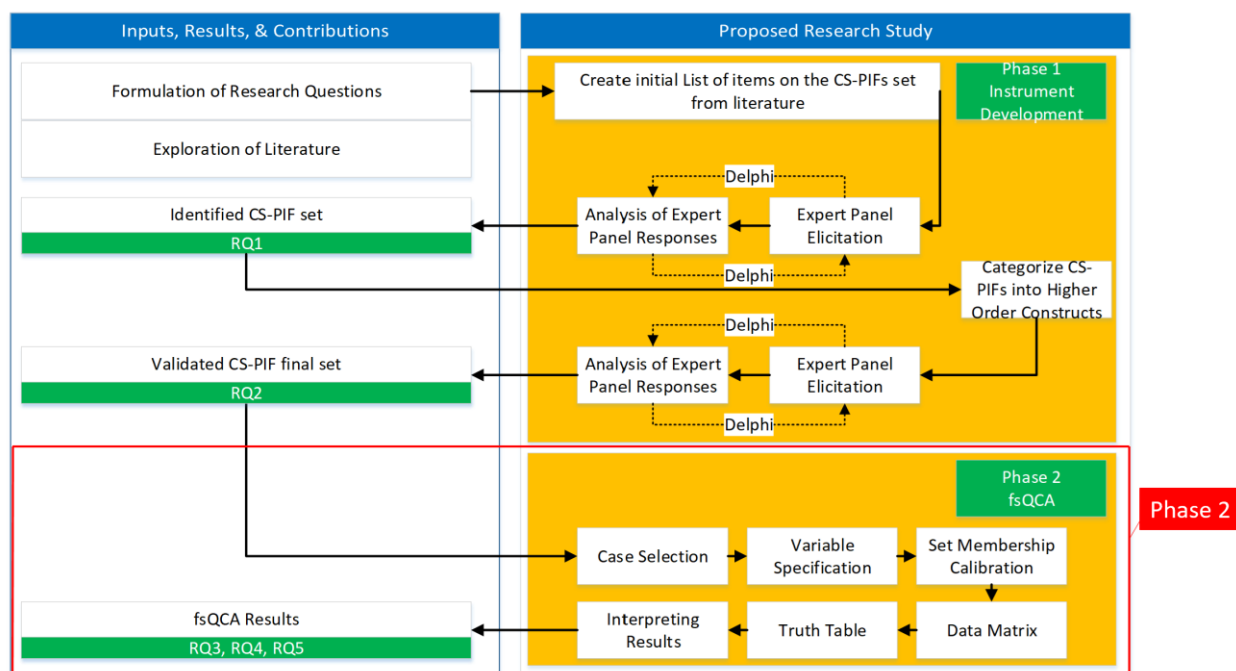


Figure 21: Phase 2 of the Research Design for Empirical Investigation using fsQCA

Case Selection

The Privacy Rights Clearinghouse (PRC) Data Breach Chronology Database was used as the dataset. The database was downloaded on June 1st, 2020. This database contained 9,015 total data breaches entries, of which some are duplicate entries of the same breach. The entries varied with the amount of information provided regarding the cases: some were very detailed, and some were not detailed at all. The earliest breach made public in the database occurred on January 10, 2005.

The database contains eight organization types, as provided previously in Table 11. The top 100 cases (in terms of records breached) were examined for each organization type. Some of the cases were removed from consideration: 13 entries that were not data breaches (e.g. legal disputes), 35 entries did not have enough information to categorize and were not found through internet searches, and 42 duplicate case entries were removed. When a case was removed, the next biggest case in the same organization type was added, to ensure there were 100 cases for each organization type. A total of 800 cases were reviewed and categorized.

The cases were reviewed using information listed in the PRC database, but also corroborated through media reports, to provide initial classification of the data breaches. After the initial review, data breach causes and cause categories began to emerge. With respect to this research, the focus was on whether a data breach was caused by (1) human error (definitely caused by human error), (2) non-conclusive, or (3) not caused by human error (definitely not caused by human error).

The very specific causes of the data breaches (e.g. software bug, phishing attack, etc.) were grouped into higher order categories. Data breaches caused by human error were classified into the Human Error Group, with the following sub-categories: Misconfiguration, Poor Cybersecurity Hygiene, Social Engineering, and Unintended Disclosure. The Non-Conclusive Group have the sub-categories of 3rd Party (Lost IS), 3rd Party (Stolen IS), 3rd Party (Hacked IS), and Hacked-Possible Error. The Not Human Error Group have the categories of Insider Threat, Stolen IS from Secure Area, and Unavoidable Hack. A breakdown the groups and categories are shown in Figure 22.

Human error (Green):
<ul style="list-style-type: none"> • Misconfiguration <ul style="list-style-type: none"> ○ Simple/multiple vulnerabilities ○ Sensitive information made publicly accessible/visible ○ Dangerous software installed ○ System/site not properly tested ○ Employee failed to patch a system or close a known vulnerability • Poor Cybersecurity Hygiene <ul style="list-style-type: none"> ○ Reuse of password ○ Using corporate system on public unsecured WiFi • Social Engineering <ul style="list-style-type: none"> ○ Phishing attack • Unintended Disclosure <ul style="list-style-type: none"> ○ Email to wrong recipient(s) ○ Posting PII online or on unprotected/unauthorized server ○ Forgot to remove PII (digital or print) ○ Loss of information systems – except 3rd party loss ○ IS was stolen outside of organization control (e.g. in car) ○ Improper Disposal
Non-conclusive Human Error / Not Enough Information (Yellow):
<ul style="list-style-type: none"> • 3rd Party – Lost IS <ul style="list-style-type: none"> ○ Information system lost, stolen or compromised by 3rd party, to include mail • 3rd Party – Stolen IS • 3rd Party – Hacked IS • Hacked – Possible Error <ul style="list-style-type: none"> ○ Breach may have been caused by human error, but not enough information to be certain ○ Point of sale system hacked (i.e. physical security / logical controls may or may not prevent breach)
Not Human Error (Red):
<ul style="list-style-type: none"> • Insider Threat <ul style="list-style-type: none"> ○ Malicious insider threat (e.g. current or ex-employee steals information, or trusted 3rd party) • Stolen IS from Secure Area <ul style="list-style-type: none"> ○ Laptop, hard drive, equipment was stolen at an organization site (e.g. break-in) • Unavoidable Hack <ul style="list-style-type: none"> ○ Zero-day vulnerability data breach ○ Due to unknown software bug ○ Nation state or highly sophisticated hackers that compromised a system that was not due to a minor vulnerability. For example, due to APT

Figure 22: Data Breach Cause Groups and Categories

A review of the 800 cases revealed that 36% of the cases were definitively caused by human error, while 17% were definitely not caused by human error. There is a large 47% of the 800 cases that were indeterminate as to if the breach was caused by human error or

not. Of those indeterminate cases, 14% were caused by a 3rd party (lost, stolen or hacked IS). About 86% of the indeterminate cases were caused by hacking, which may have been hacked due to human error (e.g. unpatched server). Appendix D and Appendix E contain the case review categorization results, and Appendix F contains the results breakdown.

Figure 23 below contains a high-level summary.

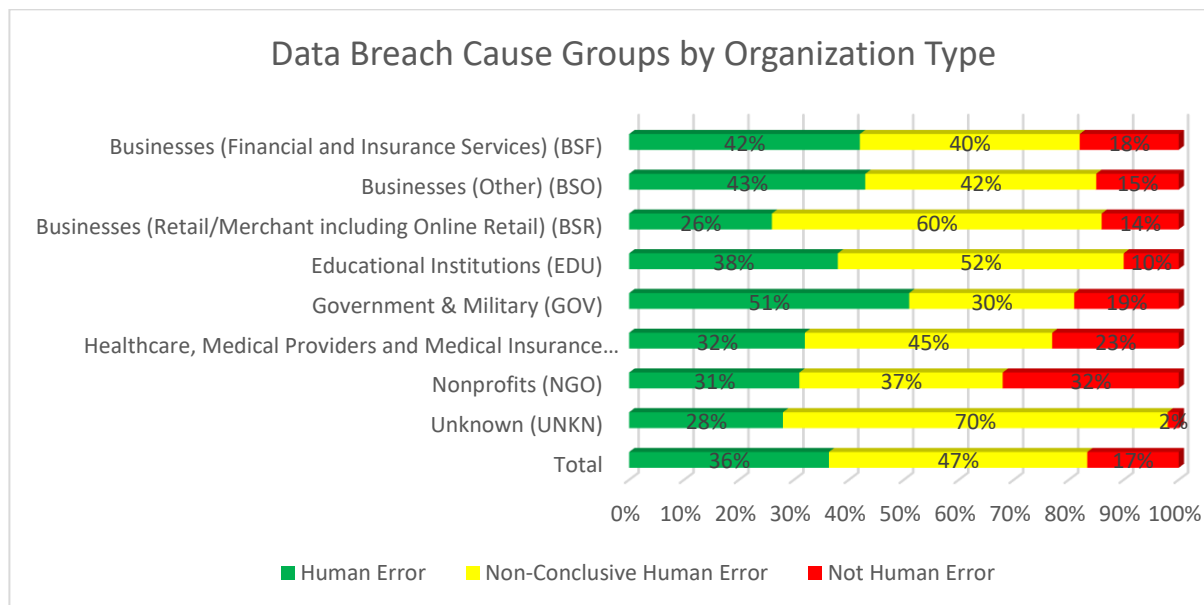


Figure 23: Data Breach Cause Groups by Organization Type

Variable Specification

As described previously throughout this report, there are two axis of variables: Cybersecurity Performance Influencing Factors (CS-PIF) (conditions) and Cybersecurity Human Error (CS-HE) (outcomes). The CS-PIFs were finalized in Phase 1 of this research. The 1st order CS-PIFs are the specific CS-PIFs that were identified in the case review. Presence of 1st order CS-PIFs attribute to 2nd order CS-PIFs. The 2nd order CS-PIFs were used to conduct fsQCA. On the other hand, the CS-HEs were developed throughout the course of the literature review, specifically, based on the works of Rasmussen (1983) and Reason (1990). A summary of the variables is shown in Table 14.

Table 14

Summary of CS-PIFs and CS-HEs

Conditions		Outcomes
I.	Organizational Cybersecurity (ORGC)	I. Skill-Based Error
	a. Cybersecurity Culture	
	b. Organizational Cybersecurity Control	II. Rule-Based Mistake
II.	Cybersecurity Policies and Procedures (CPAP)	
	a. Cybersecurity Policies	III. Knowledge-Based Mistake
	b. Cybersecurity Procedures	
III.	Cybersecurity Education, Training, and Awareness (CETA)	
	a. Cybersecurity Education	
	b. Cybersecurity Training	
	c. Cybersecurity Awareness	
IV.	Ergonomics (ERGO)	
	a. Human-Computer Interaction	
	b. Macro-ergonomics	
V.	Cybersecurity Knowledge, Skills, and Abilities (CKSA)	
	a. Employee Cybersecurity Competency	
	b. Employee Cybersecurity Awareness	
	c. Employee Cybersecurity Skill	
	d. Employee Cybersecurity Self-Efficacy	
VI.	Employee Cybersecurity Fitness for Duty (CFFD)	
	a. Stress	
	b. Fatigue	
	c. Situational Awareness	
	d. Emotions	
	e. Motivations	

Set Membership Calibration

As explained earlier in this research report, the QCA and fsQCA processes require the review of cases, and the identification of the presence or absence of variables (conditions and outcomes) within the cases. This “existence” is called membership. In crisp-set QCA, (or just QCA), membership is defined using Boolean variables: 1 as existing and 0 as not existing. For example, if we were examining the 1st order CS-PIF of fatigue using crisp-set criteria, we could say that the individual that caused the human error was either

fatigued (=1) or not (=0). As the cases were reviewed using publicly available data, there is often ambiguity in membership.

fsQCA uses fuzzy-set logic to allow for partial membership in sets. This logic more accurately relates to the natural world, as societal constructs are not often classified using 1's and 0's. For example, a person may have more democratic or conservative views in politics, but they may fit the entirety of views of a certain political party. The fuzzy-set criteria used in this research is shown in Figure 24. Additionally, a membership calibration rubric was developed using the variables in the preceding section, as shown in Appendix G. Due to fsQCA using log-odds, fsQCA cannot compute exactly 0 or 1 (negative or positive infinity, respectively), so 0 (full non-membership) is adjusted to 0.05, and 1 (full membership) is adjusted to 0.95 (Pappas & Woodside, 2021; Ragin, 2008).

<ul style="list-style-type: none"> • CS-PIFs: 1=Optimal / Desired 0=Not Optimal / Not Desired • CS-HEs: 1=Occurrence 0=No Occurrence 				
0.05	0.33	0.5	.66	.95
Fully Non-Membership	Less out than in	Max Ambiguity	More in than out	Full Membership

Figure 24: Utilized Fuzzy-set Criteria

Data Matrix

Of the 800 data breach cases data set, only 291 (36%) of the data breaches were definitively caused by human error. These breaches were individually reviewed again to assign membership values for conditions (CS-PIFs) and outcomes (CS-HE) using the developed fuzzy-set criteria. Data from the PRC database, other data breach databases, media reports, data breach notification letters, government investigations, legal

documents, and other websites were used to identify and assign fuzzy-set membership scores for each case.

Two unconventional methods were used in the case review: social media and archived websites. For example, the organization LeafFilter had 838 employees listed on LinkedIn, but only one employee was listed as working in security or cybersecurity; this indicated that the organization does not place a high priority in cybersecurity resources and implied a poor cybersecurity culture. The other unconventional method was using the tool Wayback Machine, to either find websites or articles that were once online but no longer accessible via the original URL (companies don't like to keep their dirty laundry online if not necessary), or to find old versions of sites to infer information. For example, Purdue University did not have an IT Security Incident Response procedure posted online in 2017 but did have one following their 2018 data breach.

Unfortunately, provided best efforts, not all the 291 data breach cases that were caused by human error could be used for the final data set. There was simply not enough public information to effectively assign membership values for CS-PIFs and CS-HEs. After several iterations of case review, 102 cases remained. Each case was provided justification for each fuzzy-set assignment and captured in a document, along with links, for documentation and replication purposes. A sample of a case review is shown in Appendix H. The final data matrix is displayed in Appendix I and Appendix J. The CS-PIFs and CS-HEs acronyms were used for the data matrix are presented in Table 15.

Table 15

Conditions and Outcomes Used

Condition or Outcome	Acronym
----------------------	---------

Cybersecurity Performance Influencing	
Organizational Cybersecurity	ORGC
Cybersecurity Policies and Procedures	CPAP
Cybersecurity Education, Training, and Awareness	CETA
Ergonomics	ERGO
Cybersecurity Knowledge, Skills, and Abilities	CKSA
Employee Cybersecurity Fitness for Duty	CFFD
Cybersecurity Human Error Type:	
Skill Based Error	SBE
Role Based Mistake	RBM
Knowledge Based Mistake	KBM

During the case review and data matrix process, it was discovered that ergonomics (human computer interaction and macro-ergonomics) had very minimal mention in the available data. Only 21 of the 102 cases mentioned this condition. Examples of such mention included communication breakdown, manning issues, or changes in processes. For those cases that did not mention this construct, it was difficult to infer if ERGO was present or absent per the fsQCA calibration rubric. For this reason and the effect on the results, ERGO was not included in the remaining steps for fsQCA. This is a known limitation in some fsQCA research studies, and it would be problematic to assume or assign a value to ERGO without sufficient data (de Block & Vis, 2019). Removing conditions from the study is acceptable for the robustness of QCA findings (de Block & Vis, 2019).

What also occurred during the data matrix process, was identification of the size of the organization that was breached. This was accomplished using publicly available data that was closest to the year of the breach (e.g. corporate financial reports). There were five organization size categories, and they were combined into 3, as show in Figure 25.

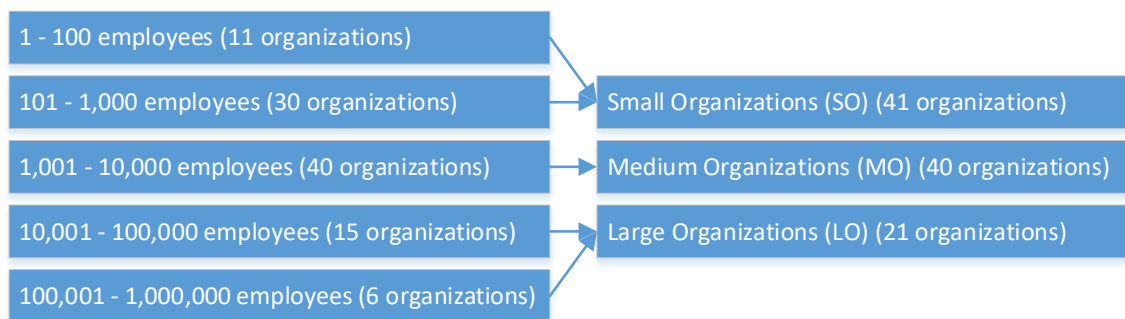


Figure 25: Organization Size Criteria

Analysis of Necessary Conditions

Necessary conditions are conditions that are required for the outcome to occur (Rihoux & Ragin, 2009). Conditions are labeled *necessary* or *almost necessary* if they exceed a consistency threshold of 0.80 or above (Balle et al., 2019; Henriques et al., 2019; Ragin, 2000). Table 16 presents fsQCA results testing necessary conditions for SBE, RBM, and KBM. ~CKSA is a necessary condition for all cybersecurity human error outcomes. In other words, poor cybersecurity knowledge, skills, and abilities is almost always necessary (or present) when cybersecurity human error occurs that leads to data breaches, in cases observed.

Table 16

Necessary Conditions Summary

Conditions	SBE		RBM		KBM	
	Consist.	Coverage	Consist.	Coverage	Consist.	Coverage
ORGC	0.392	0.421	0.461	0.421	0.368	0.465
~ORGC	0.751	0.390	0.707	0.311	0.754	0.460
CPAP	0.415	0.336	0.582	0.400	0.519	0.495
~CPAP	0.728	0.448	0.586	0.307	0.602	0.437
CETA	0.360	0.373	0.491	0.432	0.402	0.491
~CETA	0.783	0.414	0.677	0.304	0.719	0.447
ERGO	0.692	0.400	0.607	0.298	0.694	0.472
~ERGO	0.451	0.400	0.561	0.422	0.428	0.446
CKSA	0.287	0.426	0.366	0.461	0.307	0.536
~CKSA	0.855	0.392	0.802	0.312	0.814	0.439
CFFD	0.369	0.287	0.541	0.356	0.634	0.579
~CFFD	0.774	0.493	0.627	0.339	0.487	0.365

ORGC=Organizational Cybersecurity; CPAP=Cybersecurity Policies and Procedures;
CETA=Cybersecurity Education, Training, and Awareness; ERGO=Ergonomics; CKSA=Cybersecurity
Knowledge, Skills, and Abilities; CFFD=Cybersecurity Fitness for Duty

Truth Table

After the condition and outcome membership assignment for the 102 cases were entered into a data matrix, the next step was to input the data matrix (in CSV format) into fsQCA software. Publicly available fsQCA 3.1b software was used to run data analysis. The truth table transforms the raw data into all logical combinations of the conditions and outcome selected for analysis. For example, for the model “SBE = f(ORGC, CPAP, CETA, ERGO, CKSA, CFFD)”, there are 32 possible configurations of conditions that lead to the outcome SBE. The formula to determine the possible combinations is 2^n where n equals the number of conditions. Since there were only 102 cases, only some configurations were present in the model (some many times), whereas some configurations were not.

When examining the truth table, irrelevant combinations must be removed using frequency and consistency thresholds. The frequency threshold was set to a number that exceeds at least 80% of the cases. The consistency threshold was set to 80% (0.80). A truth table example with researcher’s filter descriptions (in red) is shown in Figure 26. The truth table following setting frequency and consistency thresholds is shown in Figure 27.

ORGC	CPAP	CETA	CKSA	CFFD	number	SBE	cases	raw consist.	PRI consist.	SYM consist
0	0	0	0	0	34 (33%)		cases	0.53437	0.450635	0.450635
0	0	0	0	1	22 (54%)		cases	0.389381	0.261121	0.261121
1	1	1	0	0	10 (64%)		cases	0.514319	0.313916	0.313916
0	1	0	0	0	7 (71%)		cases	0.548268	0.339964	0.339964
0	1	0	0	1	6 (77%)		cases	0.469895	0.241555	0.241554
1	1	1	0	1	4 (81%)		cases	0.421531	0.135659	0.135659
1	1	0	0	0	2 (83%)		cases	0.622849	0.372396	0.372396
0	0	1	0	0	2 (85%)		cases	0.6192	0.356757	0.356757
1	0	1	0	0	2 (87%)		cases	0.648956	0.319853	0.319853
1	1	1	1	0	2 (89%)		cases	0.550225	0.271845	0.271845
0	1	1	0	1	2 (91%)		cases	0.464789	0.109375	0.109375
1	0	0	0	0	1 (92%)		cases	0.67029	0.387206	0.387206
0	1	1	0	0	1 (93%)		cases	0.547138	0.20649	0.20649
0	0	0	1	0	1 (94%)		cases	0.566372	0.304965	0.304965
1	0	1	1	0	1 (95%)		cases	0.706107	0.427509	0.427509
0	1	1	1	0	1 (96%)		cases	0.578067	0.19788	0.19788
1	1	0	0	1	1 (97%)		cases	0.564616	0.283545	0.283545
0	1	0	1	1	1 (98%)		cases	0.563406	0.188553	0.188553
1	0	1	1	1	1 (99%)		cases	0.616183	0.185022	0.185022
1	1	1	1	1	1 (100%)		cases	0.489458	0.171149	0.171149
1	0	0	1	0	0 (100%)		cases			
0	1	0	1	0	0 (100%)		cases			
1	1	0	1	0	0 (100%)		cases			
0	0	1	1	0	0 (100%)		cases			
1	0	0	0	1	0 (100%)		cases			
0	0	1	1	0	0 (100%)		cases			
1	0	1	0	1	0 (100%)		cases			
0	0	0	1	1	0 (100%)		cases			
1	0	0	1	1	0 (100%)		cases			
1	1	0	1	1	0 (100%)		cases			
0	0	1	1	1	0 (100%)		cases			
0	1	1	1	1	0 (100%)		cases			

4 exceeds 80% of configurations in this model. Cases below 4 will be deleted from analysis

Dialog

Delete rows with number less t OK

and set SBE to 1 for rows with consist >= Cancel

.8 sets configurations with 80% or higher under raw Consist. Column to "1" under the Outcome Column. Sets configurations under .80 to "0"

Figure 26: Truth Table Example for $SBE = f(ORGC, CPAP, CETA, CKSA, CFFD)$

ORGC	CPAP	CETA	CKSA	CFFD	number	SBE	cases	raw consist.	PRI consist.	SYM consist
0	1	0	0	0	7	0	cases	0.548268	0.339964	0.339964
0	0	0	0	0	34	0	cases	0.53437	0.450635	0.450635
1	1	1	0	0	10	0	cases	0.514319	0.313916	0.313916
0	1	0	0	1	6	0	cases	0.469895	0.241555	0.241554
1	1	1	0	1	4	0	cases	0.421531	0.135659	0.135659
0	0	0	0	1	22	0	cases	0.389381	0.261121	0.261121

Figure 27: Truth Table Example for $SBE = f(ORGC, CPAP, CETA, CKSA, CFFD)$

following setting frequency and consistency thresholds

Interpreting Results

Fuzzy-set qualitative analysis was conducted using fsQCA 3.1b software. Figure 28 shows the models executed and the resulting intermediate solution consistency, with green representing acceptable solutions as they met the .80 overall solution consistency

requirement (Ragin, 2008). The *Freq Cutoff* row in Figure 28 is the frequency threshold used for the truth table. Only the presence of outcomes were examined, and not the absence (\sim SBE, \sim RBM, and \sim KBM), as these the absence of one type of error equates to the presence of another kind of error, as opposed to a non-error caused data breach. “ \sim ” denotes the absence of a condition or outcome (Fiss, 2007), and “*” denotes the logical operator “AND” (Curado et al., 2016). Seven of the 36 models met the recommended solution consistency requirement of 0.80 (Balle et al., 2019; Henriques et al., 2019; Ragin, 2008).

#	Dataset	Model	SBE	RBM	KBM	Freq Cutoff
RQ3	Entire Dataset	ORGC*CPAP*CETA*CKSA*CFFD	0.421615	0.403207	0.478029	4
RQ4a	Unintended Disclosure	ORGC*CPAP*CETA*CKSA*CFFD	0.506655	0.377107	0.462289	2
RQ4b	System Misconfiguration	ORGC*CPAP*CETA*CKSA*CFFD	0.238095	0.942857	0.238095	1
RQ4c	Social Engineering	ORGC*CPAP*CETA*CKSA*CFFD	0.943074	0.361217	0.361217	1
RQ4d	Poor Cybersecurity Hygiene	ORGC*CPAP*CETA*CKSA*CFFD	0.185784	0.185784	1	1
RQ5a1	Business - Finance/Retail/Other	ORGC*CPAP*CETA*CKSA*CFFD	0.569321	0.569322	0.834808	1
RQ5a2	Education / Non-Profit	ORGC*CPAP*CETA*CKSA*CFFD	0.5311	0.820513	0.442308	1
RQ5a3	Government	ORGC*CPAP*CETA*CKSA*CFFD	0.382765	0.382765	0.884892	1
RQ5a4	Medical	ORGC*CPAP*CETA*CKSA*CFFD	0.509709	0.298544	0.434466	4
RQ5b1	Small Organizations	ORGC*CPAP*CETA*CKSA*CFFD	0.486688	0.522897	0.42705	2
RQ5b2	Medium Organizations	ORGC*CPAP*CETA*CKSA*CFFD	0.399671	0.381579	0.547697	2
RQ5b3	Large Organizations	ORGC*CPAP*CETA*CKSA*CFFD	0.294118	0.45098	0.895227	2

Figure 28: Research Questions fsQCA Results

Table 17 displays a summary of the fsQCA results against the research questions. The cells with checkmarks met the frequency and consistency thresholds revealing sufficient configuration of conditions leading to the outcomes (SBE, RBM, or KBM). The sections that proceed Table 17 provide details and interpretation of the results for the models that met the frequency and consistency thresholds.

Table 17

fsQCA Results Summary

Research Question	Filter	Data Set	Cases	SBE	RBM	KBM
RQ3	None	Entire Dataset	102			
RQ4a	Data Breach Type	Unintended Disclosure	39			
RQ4b	Data Breach Type	System Misconfiguration	21		✓	
RQ4c	Data Breach Type	Social Engineering	19	✓		
RQ4d	Data Breach Type	Poor Cybersecurity Hygiene	23			✓
RQ5a1	Organization Type	Business – Finance/Retail/Other	33			✓
RQ5a2	Organization Type	Education / Non-Profit	22		✓	
RQ5a3	Organization Type	Government	27			✓
RQ5a4	Organization Type	Medical	20			
RQ5b1	Organization Size	Small Organizations	41			
RQ5b2	Organization Size	Medium Organizations	40			
RQ5b3	Organization Size	Large Organizations	21			✓

Solutions of Sufficient Configurations of Conditions

The intermediate and parsimonious solutions are both provided, as recommended in the literature (Fiss, 2011; Henriques et al., 2019; Ragin, 2008). The intermediate solution is used primarily, as it serves as the conservative solution and provides simpler assumptions (Henriques et al., 2019). The parsimonious solution instead only contains conditions highly linked to the outcome (Oliveira, Curado, & Henriques, 2019; Schneider & Wagemann, 2010). Comparing the intermediate and parsimonious solutions allows identification of conditions present in both sets; these conditions present in both intermediate and parsimonious solutions are called *core conditions* whereas those conditions only present in the intermediate solutions are called *peripheral conditions* (Curado et al., 2016; Fiss, 2011).

RQ4b RBM: System Misconfiguration Caused Breaches

Of the 102 total data breaches, 21 of them were caused by system misconfiguration. Examples of this data breach type include website misconfiguration and file server misconfiguration. Understandably, most of the system misconfiguration caused data breaches were a result of a Rule-Based Mistake (RBM). The fsQCA results are displayed in Table 18.

Table 18

RQ4b RBM: System Misconfiguration Caused Breaches Solutions

Model: RBM = f(ORGC, CPAP, CETA, CKSA, CFFD)			
Frequency cutoff: 1.00			
Consistency cutoff: 0.829201			
Intermediate Solution (RBM)			
Causal configuration	Raw coverage	Unique coverage	Cons.
\sim ORGC* \sim CETA* \sim CKSA	0.534	0.376	0.943
CPAP* \sim CKSA*CFFD	0.285	0.054	0.858
ORGC*CETA* \sim CKSA* \sim CFFD	0.241	0.018	1.000
ORGC*CPAP*CETA* \sim CFFD	0.259	0.036	1.000
Solution Coverage: 0.779527			
Solution Consistency: 0.942857			
Parsimonious solution (RBM)			
<i>No parsimonious solutions</i>			

RQ4c SBE: Social Engineering Caused Breaches

Of the 102 total data breaches, 19 of them were caused by social engineering. 18 of the 19 data breaches were caused by phishing via email, categorized under the Skills-Based Error (SBE). One of the 19 data breaches was a more sophisticated attack where an anonymous internet user manipulated an administrator into downloading a malicious web browser extension, categorized as a Knowledge-Based Mistake (KBM). The fsQCA results are displayed in Table 19.

Table 19

RQ4c SBE: Social Engineering Caused Breaches Solutions

Model: SBE = f(ORG, CPAP, CETA, CKSA, CFFD)
 Frequency cutoff: 1.00
 Consistency cutoff: 0.930259

Intermediate Solution (SBE)

Causal configuration	Raw coverage	Unique coverage	Cons.
~ORG*~CETA*~CKSA	0.777	0.571	0.937
ORG*CETA*~CKSA*~CFFD	0.177	0.020	1.000
CPAP*~CETA*~CKSA*~CFFD	0.226	0.000	1.000
ORG*CPAP*~CKSA*~CFFD	0.209	0.000	1.000
Solution Coverage: 0.869388			
Solution Consistency: 0.943074			

Parsimonious solution (SBE)
No parsimonious solutions

RQ4d KBM: Poor Cybersecurity Hygiene Caused Breaches

Of the 102 total data breaches, 23 of them were a result of poor cybersecurity hygiene by the employee or user. These were a result of the intentional disregard for policy—such as leaving a company laptop or drive in their car or other unsecured location, connecting to an unsecured wireless network, sending sensitive files unencrypted, or other intentional decision that ended up being a mistake. All 23 of these data breaches were a result of a Knowledge-Based Mistake (KBM). The fsQCA results are displayed in Table 20.

Table 20

RQ4d KBM: Poor Cybersecurity Hygiene Caused Breaches Solutions

Model: KBM = f(ORG, CPAP, CETA, CKSA, CFFD)
 Frequency cutoff: 1.00
 Consistency cutoff: 1.00

Intermediate Solution (KBM)

Causal configuration	Raw coverage	Unique coverage	Cons.
~ORGC*~CPAP*~CETA*~CKSA	0.777	0.571	0.937
~ORGC*CPAP*~CETA*CFFD	0.177	0.020	1.000
ORGC*CPAP*CETA*~CKSA	0.226	0.000	1.000
ORGC*CETA*CKSA*CFFD	0.209	0.000	1.000
~ORGC*CPAP*CETA*CKSA*~CFFD	0.209	0.000	1.000
Solution Coverage: 0.730892			
Solution Consistency: 1.00			
Parsimonious solution (KBM)			
<i>No parsimonious solutions</i>			

RQ5a1 KBM: All Business Organizations

Research question 5 seeks to identify fsQCA sufficiency among organization types and organization sizes. Cases with organizations categorized under Business-Finance (BSF), Business-Retail (BSR), and Business-Other (BSO) were combined into one data set for fsQCA. The fsQCA results are displayed in Table 21. Note that the parsimonious solution for RQ5a1 did not meet the consistency threshold of 0.80, but is listed here as a limitation.

Table 21

RQ5a1 KBM: All Business Organizations Solutions

Model: KBM = f(ORGC, CPAP, CETA, CKSA, CFFD)			
Frequency cutoff: 1.00			
Consistency cutoff: 0.834808			
Intermediate Solution (KBM)			
Causal configuration	Raw coverage	Unique coverage	Cons.
~ORGC*CPAP*~CETA*CKSA*CFFD	0.227	0.227	0.835
Solution Coverage: 0.227309			
Solution Consistency: 0.834808			
Parsimonious solution (KBM)			
Causal configuration	Raw coverage	Unique coverage	Cons.
CPAP*~CETA*CKSA	0.250	0	0.649
~CETA*CKSA*CFFD	0.317	0	0.738
~ORGC*CKSA*CFFD	0.317	0.02249	0.825
solution coverage: 0.339759			
solution consistency: 0.68336			

RQ5a2 RBM: Education/Non-Profit Organizations

Due to the low number of cases for Education (16) and Non-Profit (NGO) (6), these cases were combined into one data set for fsQCA. These organization types were combined as the potential external threats against these organizations may be similar, as opposed to business or government organizations. The fsQCA results are displayed in Table 22. Note that the parsimonious solution for RQ5a2 did not meet the consistency threshold of 0.80, but is listed here as a limitation.

Table 22

RQ5a2 RBM: Education/Non-Profit Organizations Solutions

Model: RBM = f(ORGC, CPAP, CETA, CKSA, CFFD)			
Frequency cutoff: 1.00			
Consistency cutoff: 0.820513			
Intermediate Solution (RBM)			
Causal configuration	Raw coverage	Unique coverage	Cons.
~ORGC*CPAP*CETA*~CKSA*CFFD	0.253	0.253	0.821
Solution Coverage: 0.253465			
Solution Consistency: 0.820513			
Parsimonious solution (RBM)			
Causal configuration	Raw coverage	Unique coverage	Cons.
~ORGC*CPAP*CETA	0.253	0.000	0.821
~ORGC*CPAP*CFFD	0.281	0.028	0.772
~ORGC*CETA*CFFD	0.253	0.000	0.821
solution coverage: 0.281188			
solution consistency: 0.771739			

RQ5a3 KBM: Government Organizations

Of the 102 cases, 27 of them were data breaches in government organizations. fsQCA was performed on the data set of government organizations. The fsQCA results are displayed in Table 23.

Table 23

RQ5a3 KBM: Government Organizations Solutions

 Model: KBM = f(ORGC, CPAP, CETA, CKSA, CFFD)

Frequency cutoff: 1.00

 Consistency cutoff: 0.866983

 Intermediate Solution (KBM)

Causal configuration	Raw coverage	Unique coverage	Cons.
ORGC*CPAP*~CKSA*~CFFD	0.240	0.020	0.934
~ORGC*CPAP*~CKSA*CFFD	0.348	0.112	0.873
ORGC*~CPAP*CETA*CKSA*CFFD	0.152	0.020	0.900
ORGC*CPAP*CETA*~CKSA	0.294	0.000	0.946
CPAP*CETA*~CKSA*CFFD	0.327	0.000	0.907
Solution Coverage: 0.517117			
Solution Consistency: 0.884892			

 Parsimonious solution (KBM)

Causal configuration	Raw coverage	Unique coverage	Cons.
ORGC*CPAP	0.348	0.037	0.954
CPAP*CFFD	0.473	0.112	0.904
CKSA	0.219	0.017	0.813
ORGC*CETA	0.331	0.017	0.868
ORGC*CFFD	0.311	0.000	0.902
CETA*CFFD	0.365	0.000	0.878
solution coverage: 0.584385			
solution consistency: 0.874214			

RQ5b3 KBM: Large Organizations

Of the 102 cases, 21 of them were data breaches with large organizations (10,001+ employees). fsQCA was performed on the data set of only large organizations. The fsQCA results are displayed in Table 24.

Table 24

RQ5b3 KBM: Large Organizations Solutions

 Model: KBM = f(ORGC, CPAP, CETA, CKSA, CFFD)

Frequency cutoff: 1.00

 Consistency cutoff: 0.808917

 Intermediate Solution (KBM)

Causal configuration	Raw coverage	Unique coverage	Cons.
~ORGC*~CETA*~CKSA*CFFD	0.484	0.185	0.873
~ORGC*CPAP*~CKSA*CFFD	0.369	0.071	0.840
~ORGC*CPAP*CETA*CKSA*~CFFD	0.153	0.049	0.874
Solution Coverage: 0.603137			
Solution Consistency: 0.895227			

 Parsimonious solution (KBM)

Causal configuration	Raw coverage	Unique coverage	Cons.
----------------------	--------------	-----------------	-------

~ORGC*CFFD	0.576	0.336	0.891
~ORGC*CETA	0.224	0.000	0.911
~ORGC*CKSA	0.197	0.000	0.890
solution coverage: 0.603137			
solution consistency: 0.895227			

Solutions Summary

Table 17 displays a summary of the models that exceed the prescribed minimum overall solution consistency (≥ 0.80) requirements. Coverage describes how much of the outcome is explained by the configurations (Pappas & Woodside, 2021; Ragin & Davey, 2017). Overall solution coverage should fall between the .25 and .90 range (Gonçalves et al., 2021; Ragin, 2008). The coverage minimum is not met in RQ5a1 KBM (.22). Several researchers have stressed the importance of high consistency over high coverage, and thus RQ5a1 KBM is presented in Table 25 as acceptable, but as a limitation (Huarng, 2015; Woodside & Zhang, 2013).

Table 25

FsQCA Solutions Summary

Model	Configurations	Solution Coverage	Consist.
System Misconfiguration RBM = f(ORGC, CPAP, CETA, CKSA, CFFD)	~ORGC*~CETA*~CKSA CPAP*~CKSA*CFFD ORGC*CETA*~CKSA*~CFFD ORGC*CPAP*CETA*~CFFD	.779527	.942857
Social Engineering SBE = f(ORGC, CPAP, CETA, CKSA, CFFD)	~ORGC*~CETA*~CKSA ORGC*CETA*~CKSA*~CFFD CPAP*~CETA*~CKSA*~CFFD ORGC*CPAP*~CKSA*~CFFD	.869388	.943074
Poor Cybersecurity Hygiene KBM = f(ORGC, CPAP, CETA, CKSA, CFFD)	~ORGC*~CPAP*~CETA*~CKSA ~ORGC*CPAP*~CETA*CFFD ORGC*CPAP*CETA*~CKSA ORGC*CETA*CKSA*CFFD ~ORGC*CPAP*CETA*CKSA*~CFFD	.730892	1
BSF/BSO/BSR KBM = f(ORGC, CPAP, CETA, CKSA, CFFD)	~ORGC*CPAP*~CETA*CKSA*CFFD	.227309	.834808
EDU/NGO RBM = f(ORGC, CPAP, CETA, CKSA, CFFD)	~ORGC*CPAP*CETA*~CKSA*CFFD	.253465	.820513
GOV KBM = f(ORGC, CPAP, CETA, CKSA, CFFD)	ORGC*CPAP*~CKSA*~CFFD ~ORGC*CPAP*~CKSA*CFFD	.517117	.884892

	ORG*~CPAP*CETA*CKSA*CFFD		
	ORG*CPAP*CETA*~CKSA		
	CPAP*CETA*~CKSA*CFFD		
LO KBM =	~ORG*~CETA*~CKSA*CFFD	.603137	.895227
f(ORG, CPAP, CETA, CKSA, CFFD)	~ORG*CPAP*~CKSA*CFFD		
	~ORG*CPAP*CETA*CKSA*~CFFD		

There were five configurations that fit multiple models. These models require careful consideration as they were responsible for multiple data breach types in the cases reviewed. Table 26 displays common sufficient configurations that fit different models.

Table 26

FsQCA Configurations that Fit Multiple Models

Sufficient Configurations	Models
ORG*CPAP*CETA*~CKSA	Poor Cybersecurity Hygiene KBM = f(ORG, CPAP, CETA, CKSA, CFFD) GOV KBM = f(ORG, CPAP, CETA, CKSA, CFFD)
~ORG*~CETA*~CKSA	System Misconfiguration RBM = f(ORG, CPAP, CETA, CKSA, CFFD) Social Engineering SBE = f(ORG, CPAP, CETA, CKSA, CFFD)
~ORG*CPAP*~CKSA*CFFD	GOV KBM = f(ORG, CPAP, CETA, CKSA, CFFD) LO KBM = f(ORG, CPAP, CETA, CKSA, CFFD)
ORG*CPAP*~CKSA*~CFFD	Social Engineering SBE = f(ORG, CPAP, CETA, CKSA, CFFD) GOV KBM = f(ORG, CPAP, CETA, CKSA, CFFD)
ORG*CETA*~CKSA*~CFFD	System Misconfiguration RBM = f(ORG, CPAP, CETA, CKSA, CFFD) Social Engineering SBE = f(ORG, CPAP, CETA, CKSA, CFFD)

Summary

This chapter covered Phase 1 and Phase 2 of the Research Design (Figure 12). The objective of Phase 1 was the Instrument Development for conditions that were used for fsQCA. Cybersecurity SMEs participated in an online survey to aid with instrument development. Survey demographics of the SMEs were presented and discussed. The cybersecurity SME feedback resulted in the positive identification of 1st order CS-PIFs and validation of 2nd order CS-PIFs, using the Delphi method. As a result, Research Questions 1 and 2 were answered, which presented the CS-PIFs to be used for fsQCA.

Upon completion of Phase 1, Phase 2 progressed through the fsQCA steps: case selection, variable specification, set membership calibration, producing the truth table and interpreting results of the fsQCA solutions. Eight hundred data breach cases were reviewed and categorized. Two hundred and ninety-one data breaches were found to have been caused by human error; these 291 cases were further sub-categorized into four data breach types of unintended disclosure, system misconfiguration, social engineering, and poor cybersecurity hygiene, as well as the organization size. Of those 291 cases, only 102 cases had enough qualitative information for conditions and outcomes to transform into fuzzy-set values. Each of the 102 cases were notated using researcher developed fuzzy-set criteria for the data matrix. The data matrix was transformed into a truth table, cleaned of irrelevant configurations, then fsQCA was executed to produce solutions. Seven specific models produced sufficient configurations of conditions and those were presented and reviewed. Further discussion of the solutions occurs in Chapter 5.

Chapter 5

Conclusions, Discussions, Implications, Recommendations, and Summary

Conclusions

The research problem that this study addressed is that organizational data breaches caused by human error are both costly and have the most significant impact on Personally Identifiable Information (PII) breaches (81.5%) (Greitzer et al., 2014; Evans et al., 2019; Kraemer & Carayon, 2007). Of the 800 data breaches reviewed, 36% were definitively caused by CS-HE and 47% were possibly caused by CS-HE. CS-HE caused data breaches continues to be a prevalent and expensive problem for many organizations around the world. To begin to address this longstanding problem, the main goal of this research study was to employ configurational analysis to empirically assess the conjunctural causal relationship of internal (individual) and external (organizational and contextual) Cybersecurity Performance Influencing Factors (CS-PIFs) leading to Cybersecurity Human Error (CS-HE) (SBE, RBM, and KBM) that resulted in the largest data breaches across multiple organization types from 2007 to 2019 in the US.

This research first needed to identify the factors that led to CS-HE. A thorough exploration and comprehensive understanding of the conditions—cybersecurity performance influencing factors—leading to cybersecurity human error types (skills-based errors, rule-based mistakes, and knowledge-based mistakes) was conducted in this

research. Each case had a unique set of individual and organizational circumstances that led to the data breach. Thus, the first goal of this research study identified, using cybersecurity Subject Matter Experts (SMEs), the most common internal (individual) and external (organizational and contextual) CS-PIFs leading to human error that resulted in data breaches. Eighteen tangible or identifiable internal and external CS-PIFs (i.e. factors) that may attribute to CS-HE were identified (see Figure 16 and 17). The consensus among 25 cybersecurity SMEs for identified 1st order CS-PIFs was 91.1%.

Effective fsQCA practice requires limiting the number of conditions for analysis, with the number of conditions in QCA studies ranging from two to 10 (Douglas et al., 2020; Marx et al., 2013; Schneider & Wagemann, 2010). Due to this, the 18 identified 1st order CS-PIFs were logically organized into higher order (i.e. 2nd order) CS-PIFs, and validated using cybersecurity SMEs. Therefore, the second goal of this research study validated, using cybersecurity SMEs, the higher-order set of the most common internal (individual) and external (organizational and contextual) CS-PIFs leading to human error that resulted in data breaches. Six 2nd order CS-PIFs were proposed: organizational cybersecurity; cybersecurity policy and procedures; cybersecurity education, training, and awareness; cybersecurity knowledge, skills, and abilities; employee cybersecurity fitness for duty; and ergonomics. Twenty five cybersecurity SMEs validated the 2nd order CS-PIFs with a consensus of 94%.

The third specific goal of this study was to assess the alternative configurations of internal (individual) and external (organizational and contextual) CS-PIFs leading to (a) skill-based errors; (b) rule-based mistakes; and (c) knowledge-based mistakes resulting in the largest data breaches across multiple organization types from 2007 to 2019 in the US.

This goal conducted fsQCA against the entire data set of 102 cases of data breaches caused by CS-HE. Thirty-four of the data breaches were caused by skill-based errors, 28 of the data breaches were caused by rule-based mistakes, and 41 of the data breaches were caused by knowledge-based mistakes. There were no alternative configurations or solutions that met the consistency thresholds, to signify sufficiency in combinations of CS-PIFs. In other words, of the 102 total observed human error caused data breaches, there were no solutions of sufficient configurations (CS-PIFs that led to CS-HE).

The fourth specific goal of this study was to assess the alternative configurations of CS-PIFs responsible for CS-HE leading to various data breaches caused by: (a) unintended disclosure; (b) system misconfiguration; (c) social engineering; and (d) poor cybersecurity hygiene in the largest data breaches across multiple organization types from 2007 to 2019 in the US. When dissecting the data, by data breach types, several alternative configurations and solutions did exceed the consistency thresholds: system misconfiguration data breach types caused by rule-based mistakes, social engineering data breach types caused by rule-based mistakes, and poor cybersecurity hygiene data breach types caused by knowledge-based mistakes. These solutions contained alternative sufficient configurations that led to the respective data breaches.

The fifth specific goal of this study was to assess how alternative configurations of CS-PIFs on CS-HE leading to the largest data breaches across multiple organization types from 2007 to 2019 in the US were represented across (a) industry type and (b) company size. These two modified data sets also produced alternative configurations. By organization type, business-type organizations caused by knowledge-based mistakes, education/non-profit type organizations caused by rule-based mistakes, and government-

type organizations caused by knowledge-based mistakes. By size of the organization, only the large organization solution met the consistency thresholds, of those caused by knowledge-based mistakes.

The results of the study are only as accurate as the data, and a weakness in the study is the availability of standardized and detailed data on the data breach cases. Of the 800 cases initially evaluated, only 102 of the cases had enough information to assign membership values for CS-HE and CS-PIFs. Even of these 102 cases, careful interpretation and best judgement for implication was used by the researcher to assign values for fsQCA. Extensive case evaluation across the publicly available data, and documentation of the case review process was conducted to improve internal validity as much as possible. Still, an inherent weakness exists in the research study due to available data.

Discussion

The literature has shown that human error and performance influencing factors vary based on context (Boring, 2010; Gawron et al., 2006; Shappell et al., 2007). This was evident as CS-HEs and CS-PIFs varied widely between the observed cases, data breach types, and organization sizes and types. The context mattered as well when considering that research question 3 (all data breaches) returned no acceptable fsQCA solutions, but research questions 4 and 5 (compartmentalized data sets) did. The one constant is that ~CKSA (the deficiency of cybersecurity knowledge, skills, and abilities) was a *necessary condition* for data breaches caused by skill-based errors (n=0.85), rule-based mistakes (n=0.80), and knowledge-based mistakes (n=0.81). ~CKSA was a condition in 16 of the 23 sufficient configurations listed in Table 17.

At a high level, other patterns were apparent from the dataset of 102 cases. First, and not surprisingly, rule-based mistakes caused 20 of the 21 system misconfiguration data breach types, with one being a knowledge-based mistake where the US Department of Energy employee did not have the expertise to patch commonly known exploits. Similarly, 18 of 19 social engineering data breach types were caused by skills-based error, showing that training alone does not prevent these types of attacks. A potential prevention strategy could be to move the user from skills-based performance to rule-based or knowledge-based performance, by means of having the user perform conscious (instead of sub-conscious) actions (e.g. user confirmation before allowing link from an external email sender to proceed). Finally—and also not surprisingly—knowledge-based mistakes caused 23 of the 23 data breaches of the poor cybersecurity hygiene variety, demonstrating that about a quarter of observed data breaches were intentional but non-malicious.

It must be understood that the findings of this research must not be mistook as evidence of predicting future CS-PIF configurations to CS-HE. fsQCA views causation as conjuncture and context specific (Berg-Schlusser et al., 2009). In other words, the solutions uncovered in this research reflect the cases observed and analyzed, and future data breaches in a different context (time and space) may or may not have the same causal recipes. The solutions do indicate potential causal pathways to consider for the future.

Implications

There had been a major research and knowledge gap in cybersecurity within the context of human factors. Much research and acknowledgement of various factors and

contributions to cybersecurity human errors existed, but a comprehensive review of these factors had yet to be conducted. Additionally, the importance of the interaction between the factors was not realized. A holistic approach to understanding CS-HE as a result, was not readily apparent. This research provided clarity that CS-PIFs and their interaction leads to CS-HE, and there are multiple alternative configurations that lead to different types of CS-HEs. Additionally, there is no magic bullet: the various configurations are dependent on the context (data breach type, industry type, and company size).

Another major contribution is the introduction of QCA to cybersecurity research. Introduced in 1987 by Sociologist Charles Ragin, the research method has quickly spread from sociology research into many other disciplines (Thomann & Maggetti, 2017), to include information systems (Pappas & Woodside, 2021). As a comparative case research method, QCA and the derivative fsQCA, has potential applications in various cybersecurity research streams, to include examples of human-computer interaction and security, user compliance, and security management. The applications are limitless as organizations vary across cultures, geography, industries, and time.

Recommendations

As mentioned in chapter 4, the ergonomics CS-PIF was not included in the data analysis due to uncertainty of presence or absence in the cases, based on the text of available data. Only 21 of the 102 cases mentioned the condition in the available data, and when it was mentioned, it was a factor that contributed to the error. For 81 of the cases, it was ambiguous as to if it was a factor or not. It is possible that the acknowledgement of ergonomics' importance is not realized as it is not regularly documented. Still, 20% of the data breach cases reviewed were at least partly due to

ergonomics, in combination with other factors. Further research may consider further investigating the role of ergonomics in data breaches.

Other possibilities for future research include different datasets. In this research, the Privacy Rights Clearinghouse data breach dataset was used. During the research process, PRC stopped collecting data on data breaches, so the cases were limited from January 2005 to Oct 2019. Other data breach data sets may possibly contain more detailed information or more recent data. It appeared that generally the more recent the data breach, the more detailed the data that are available. This is especially true in the earlier cases (e.g. 2005), where data breach laws were not as prevalent and reporting was generally not required. An example of a potential resource could be the US Department of Health and Human Services, that still investigates and reports data breaches; the inherent limitation is that those organizations more often align with the healthcare industry (reducing generalizability). Last, US based organizations and data breaches were examined. Examining international data breaches, along with international individual and organizational factors may provide different results.

As the applicability of fsQCA is context specific, further research may consider examining more detailed investigation into the relationships between 1st order CS-PIFs, as well as the relationships between 2nd order CS-PIFs. An extensive number of research studies recognized relationships between factors that cause human error, but a comprehensive list that is validated via quantitative research methods has not. It is possible that not every 1st and 2nd order CS-PIF has been identified, and future research may uncover new causes to degraded performance. Finally, future research studies may consider utilizing a mixed-methods approach (e.g. fsQCA and Structured Equation

Modeling) to extend the research presented in this dissertation, as has been done by other researchers (Crespo et al., 2021; Gonçalves et al., 2021; Santos et al., 2021).

Summary

Information systems are critical for most organizations to function and thrive. Data breaches on information systems are inherent risks to organizations of all types and sizes. The perpetual reliance on information systems and increase in data breaches has produced widespread academic and commercial interest in cybersecurity.

Data breaches can be caused by external or internal actors. Internal actors can intentionally or unintentionally cause data breaches. These insider threats that unintentionally cause data breaches commit these actions during periods of degraded performance, namely skill-based performance, rule-based performance, or knowledge-based performance types. These performance failures produce cybersecurity human error: skill-based errors, rule-based mistakes, or knowledge-based mistakes.

Cybersecurity performance influencing factors affect human performance. The effect can be positive or negative, depending on how the CS-PIF influences the individual. Through a review of the literature and during Phase 1 (Instrument Development) in the Research Design of this dissertation, six CS-PIFs emerged. The CS-PIFs are organizational cybersecurity; cybersecurity education, training, and awareness; cybersecurity policies and procedures; ergonomics; cybersecurity knowledge, skills, and abilities; and cybersecurity fitness for duty. Identified in the safety and cybersecurity literature, these CS-PIFs were validated with the assistance of cybersecurity SMEs, as well as recognized in the data breach case review.

Of the 800 data breach cases that were reviewed, 291 of them were caused by CS-HE. Of those, 102 data breaches had enough data to be chosen for content analysis. Due to low mention in the data during the content analysis process, ergonomics–organizational work factors and human-computer interaction–was removed from consideration in the study. The five remaining CS-PIFs were not present (or deficient) on average in 75% of the cases, though no one case had all present (or ideal) CS-PIFs. In other words, it was evident that there was a combination of CS-PIFs that led to a CS-HE, that resulted in the data breach.

fsQCA is a comparative case method that allows a researcher to expose single or multiple sufficient configurations (causal recipes) of conditions that lead to outcomes. In this research, the conditions are the CS-PIFs and the outcomes are the CS-HE types. Fuzzy-set qualitative comparative analysis—Phase 2 of the Research Design—was conducted using a 6-step process: case selection, variable specification, set membership calibration, data matrix, truth table, and interpreting results. The research method requires careful selection of cases and specification of variables, fuzzy-set membership calibration and assignment of values to conditions and outcomes, based on the presence or absence of each. Each of the 102 data breaches (cases) were reviewed several times and tabulated on the presence or absence of CS-PIFs and CS-HE types using the researcher developed fuzzy-set calibration criteria, and input into a data matrix. Followed input of the data matrix in fsQCA software, the truth table was populated. The truth table lists every possible logical combination of conditions and counts the instances of each from the dataset. Executing fsQCA on the truth table using researcher defined frequency and

consistency thresholds produces the fsQCA solutions, which allows interpretation of the results.

On interpreting the results, the main research question was answered, being: What is the conjunctural causal relationship, using configurational analysis, of internal (individual) and external (organizational and contextual) CS-PIFs leading to CS-HE that resulted in the largest data breaches across multiple organization types from 2007 to 2019 in the US? The identification of 1st order and validation of 2nd order CS-PIFS answered research questions 1 and 2. The main research question was addressed by answering research questions 4 and 5.

RQ4. What alternative configurations of CS-PIFs are responsible for CS-HE leading to various data breaches caused by: (a) unintended disclosure; (b) system misconfiguration; (c) social engineering, and (d) poor cybersecurity hygiene, in the largest data breaches across multiple organization types from 2007 to 2019 in the US?

Table 27

RQ4 FsQCA Solutions

Model	Configurations
RQ4b RBM: System Misconfiguration Caused Breaches RBM = f(ORGC, CPAP, CETA, CKSA, CFFD)	~ORGC*~CETA*~CKSA CPAP*~CKSA*CFFD ORGC*CETA*~CKSA*~CFFD ORGC*CPAP*CETA*~CFFD
RQ4c SBE: Social Engineering Caused Breaches SBE = f(ORGC, CPAP, CETA, CKSA, CFFD)	~ORGC*~CETA*~CKSA ORGC*CETA*~CKSA*~CFFD CPAP*~CETA*~CKSA*~CFFD ORGC*CPAP*~CKSA*~CFFD
RQ4d KBM: Poor Cybersecurity Hygiene Caused Breaches KBM = f(ORGC, CPAP, CETA, CKSA, CFFD)	~ORGC*~CPAP*~CETA*~CKSA ~ORGC*CPAP*~CETA*CFFD ORGC*CPAP*CETA*~CKSA ORGC*CETA*CKSA*CFFD ~ORGC*CPAP*CETA*CKSA*~CFFD

RQ5. How are the alternative configurations of CS-PIFs on CS-HE leading to the largest data breaches across multiple organization types from 2007 to 2019 in the US, represented across (a) industry type and (b) company size?

Table 28

RQ5 FsQCA Solutions

Model	Configurations
RQ5a1 KBM: All Business Organizations Solutions KBM = f(ORGC, CPAP, CETA, CKSA, CFFD)	~ORGC*CPAP*~CETA*CKSA*CFFD
RQ5a2 RBM: Education/Non-Profit Organizations Solutions RBM = f(ORGC, CPAP, CETA, CKSA, CFFD)	~ORGC*CPAP*CETA*~CKSA*CFFD
RQ5a3 KBM: Government Organizations Solutions KBM = f(ORGC, CPAP, CETA, CKSA, CFFD)	ORGC*CPAP*~CKSA*~CFFD ~ORGC*CPAP*~CKSA*CFFD ORGC*~CPAP*CETA*CKSA*CFFD ORGC*CPAP*CETA*~CKSA CPAP*CETA*~CKSA*CFFD
RQ5b3 KBM: Large Organizations Solutions KBM = f(ORGC, CPAP, CETA, CKSA, CFFD)	~ORGC*~CETA*~CKSA*CFFD ~ORGC*CPAP*~CKSA*CFFD ~ORGC*CPAP*CETA*CKSA*~CFFD

The main goal of this research study was to employ configurational analysis—specifically, Fuzzy-Set Qualitative Analysis (fsQCA)—to empirically assess the conjunctural causal relationship of internal (individual) and external (organizational and contextual) Cybersecurity Performance Influencing Factors (CS-PIFs) leading to Cybersecurity Human Error (CS-HE) (SBE, RBM, and KBM) that resulted in the largest data breaches across multiple organization types from 2007 to 2019 in the US. Utilizing data collected from 102 data breach cases, this research found that multiple combinations, or causal recipes, of CS-PIFs led to certain CS-HEs, that resulted in data breaches. Specifically, seven of the 36 fsQCA models had solution consistencies that exceeded the minimum threshold of 0.80, thereby providing argument for the contextual nature of CS-PIFs, CS-HE, and data breaches. Two additional findings were also discovered—five sufficient configurations were present in two models, and the absence of strong

cybersecurity knowledge, skills, and abilities is a necessary condition for all cybersecurity human error outcomes in the observed cases.

Appendix A

Expert Panel Recruitment Email

Dear Information Systems and Cybersecurity Expert.

I request your expert feedback in identify and validating instruments for an upcoming doctoral research study. I am a Ph.D. Candidate in Information Systems at the College of Engineering and Computing at Nova Southeastern University (NSU), working under the supervision of Professor Yair Levy (levyy@nova.edu), and a member of the Levy CyLab (<http://CyLab.nova.edu/>). My research study focuses on contributors to human error, which may lead to data breaches.

Completion of the survey takes 20-30 minutes. Information provided in the survey will be used for the research study in aggregated form, and no Personal Identifiable Information (PII) will be collected. By clicking on the link below to access the survey, you consent to participate in this study and agree to keep all information regarding this research confidential.

- Survey: <https://forms.gle/17S2SzQFHe9U7syLA>

Thank you for your time and consideration in participating in this important research. If you would like to receive the findings of this study, please email me with your request and contact information, and I will be happy to provide upon conclusion of the study. Additionally, it would be most appreciated if you would share this survey with your friends and colleagues with Information Technology (IT) and cybersecurity expertise.

Very Respectfully,

Gabriel Cornejo, Ph.D. Candidate
gc721@mynsu.nova.edu

Appendix B

International Review Board Approval Letter



MEMORANDUM

To: **Gabriel Cornejo**

From: **Ling Wang, Ph.D.,
Center Representative, Institutional Review Board**

Date: **December 5, 2019**

Re: **IRB #: 2019-569; Title, "Human Errors in Data Breaches: An Exploratory Configurational Analysis"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Yair Levy, Ph.D.
Ling Wang, Ph.D.

Appendix C

Qualitative Survey: Instrument for Identification of Cybersecurity

Performance Influencing Factors (CS-PIFs) and Validation of Higher-Order
set of Cybersecurity Performance Influencing Factors (CS-PIFs)

Expert Panel Review: Identification of Cybersecurity Performance Influencing Factors (CS-PIFs) and Validation of Higher Order CS-PIF Categorization

Dear Expert,

Thank you for agreeing to participate in this important expert panel survey.

Your opinion will help us to identify factors that contribute to human error, which may lead to data breaches. Additionally, your opinion will help us to validate proposed categories of those same factors. Please review the research overview provided below, then proceed to review the survey instructions, and questions. Below you will find three sections: (1) External CS-PIFs; (2) Internal CS-PIFs; and (3) A bit information about yourself.

All questions are required. Don't forget to hit the 'Submit' button to submit your responses.

I would like to thank YOU again for your time and participation in this important research effort.

Should you have any question, feel free to e-mail me, or Dr. Levy.

Best Regards,

Gabriel Cornejo, Doctoral Candidate (gc721@mynsu.nova.edu)

Yair Levy, Ph.D., Dissertation Advisor (levyy@nova.edu)

Levy CyLab: <http://CyLab.nova.edu/>

OVERVIEW:

~~~~~

Data breaches are problematic for organizations throughout the world. One of the most problematic and least understood causes of data breaches are human error. Employees' human error directly or indirectly leads to data breaches.

In the safety literature, circumstantial contributors to human error are called performance influencing factors (PIF). This research investigates Cybersecurity PIFs (CS-PIFs) and their inter-relationship in influencing human error leading to data breaches.

This study considers Cybersecurity in the broader sense-the protection of information systems from technological, psychological and organizational lenses.

This survey requests for you to identify the applicability of proposed common CS-PIFs. The factors were identified in the cybersecurity literature, safety literature, or both. Additionally, this survey requests your validation of the appropriateness of categorization of proposed CS-PIFs.

\* Required

**SECTION 1: External CS-PIFs**

External Cybersecurity Performance Influencing Factors (CS-PIFs) are organizational and contextual circumstances that directly or indirectly cause an individual to commit a human error that could lead to a data breach. Identifying a CS-PIF as a contributor to human error pertains to either the presence or the absence of the factor, or the quality of the factor.

SECTION 1 has three sub-sections:

SUB-SECTION 1A: Identification of External CS-PIFs (Need feedback)

SUB-SECTION 1B: Validation of Higher Order External CS-PIFs (Need feedback)

SUB-SECTION 1C: External CS-PIF Definitions (For your information only)

**SECTION 1A: Identification of Common External CS-PIFs**

Please provide your expert opinion about the Common External Cybersecurity Performance Influencing Factors (CS-PIFs) by selecting one of the choices below:

1. Keep - the proposed External Factor should be included as is.
2. Adjust- the External Factor should be included but with modifications (Please provide your feedback below on the exact modifications at the short text field at the end in the space provided).
3. Remove - the proposed External Factor should NOT be included (Please recommend reasons below on why not, and propose a replacement if possible at the end in the space provided).

If you feel there are External Factors not covered here that should be included, please include them in the space provided below.

Proposed Common External Cybersecurity Performance Influencing Factors (CS-PIFs) \*

|                                                    | Keep                  | Adjust                | Remove                |
|----------------------------------------------------|-----------------------|-----------------------|-----------------------|
| 1A-EF1.<br>Cybersecurity Culture                   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1A-EF2.<br>Organizational<br>Cybersecurity Control | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1A-EF3.<br>Cybersecurity<br>Policies               | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1A-EF4.<br>Cybersecurity<br>Procedures             | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1A-EF5.<br>Cybersecurity<br>Education              | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1A-EF6.<br>Cybersecurity<br>Training               | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1A-EF7.<br>Cybersecurity<br>Awareness              | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1A-EF8. Human-<br>Computer Interaction             | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1A-EF9.<br>Macroergonomics                         | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

1A-EF10. If you selected "2. Adjust" and/or "3. Remove" to at least one of the items above, please provide your recommended adjustments (or "N/A" if none) \*

Your answer

---

1A-EF11. Please provide additional factors that you see fit to be included as Common External Cybersecurity Performance Influencing Factors (CS-PIFs) beyond those listed above (or "N/A" if none). For additional factors, please provide a short justification as context for the researcher. \*

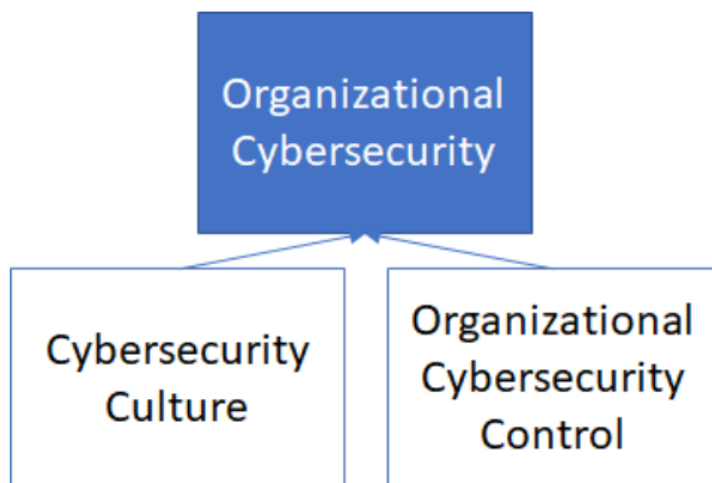
Your answer

---

### SECTION 1B: Validation of Higher Order External CS-PIFs

Based on your expert judgement and experience, please rate the appropriateness of the below categorizations, of factors identified in SECTION 1A being grouped similarly. These groupings of higher-order CS-PIFs are required for causal analysis of this proposed research.

1B-EF1. Organizational Cybersecurity CS-PIF Category



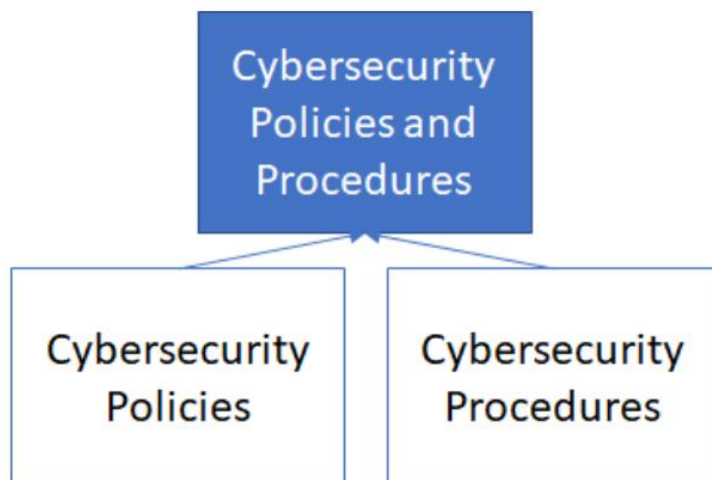
1B-EF1a. Organizational Cybersecurity is an appropriate higher order CS-PIF categorization for factors that could directly or indirectly cause an individual to commit a human error that could lead to a data breach. \*

1B-EF1b. If you selected 1-5 for EF1a, please provide recommended adjustments (or "N/A" if none). \*

Your answer

---

1B-EF2. Cybersecurity Policies and Procedures CS-PIF Category



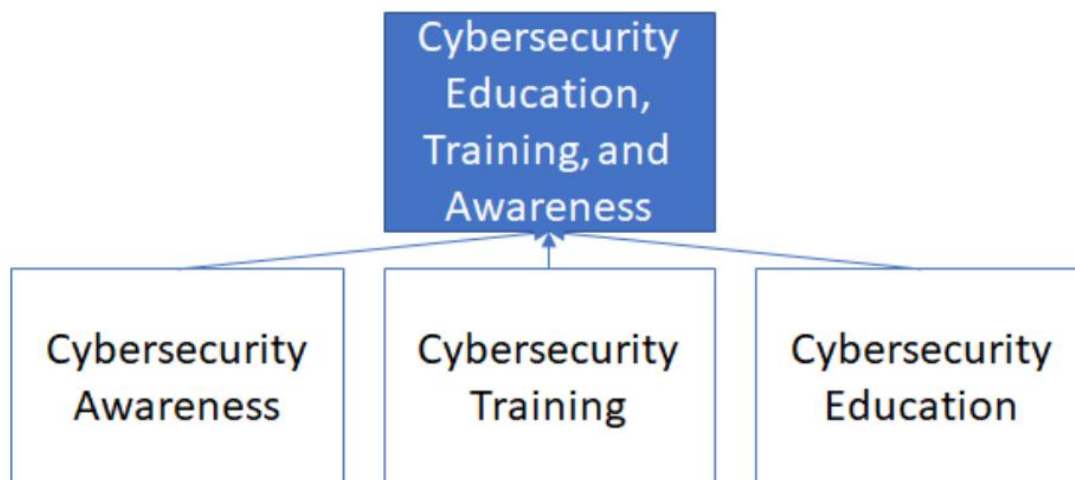
1B-EF2a. Cybersecurity Policies and Procedures is an appropriate higher order CS-PIF categorization for factors that could directly or indirectly cause an individual to commit a human error that could lead to a data breach. \*

1B-EF2b. If you selected 1-5 for EF2a, please provide recommended adjustments (or "N/A" if none). \*

Your answer

---

1B-EF3. Cybersecurity Education, Training, and Awareness CS-PIF Category



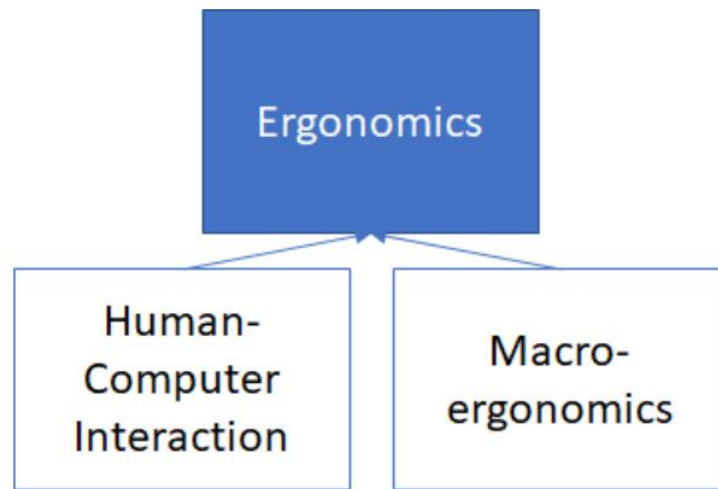
1B-EF3a. Cybersecurity Education, Training, and Awareness is an appropriate higher order CS-PIF categorization for factors that could directly or indirectly cause an individual to commit a human error that could lead to a data breach. \*

1B-EF3b. If you selected 1-5 for EF3a, please provide recommended adjustments (or "N/A" if none). \*

Your answer

---

## 1B-EF4. Ergonomics CS-PIF Category



1B-EF4a. Ergonomics is an appropriate higher order CS-PIF categorization for factors that could directly or indirectly cause an individual to commit a human error that could lead to a data breach. \*

1B-EF4b. If you selected 1-5 for EF4a, please provide recommended adjustments (or "N/A" if none). \*

Your answer

---

**SECTION 1C: Definition of Common External CS-PIFs**

## Definition of External Cybersecurity Performance Influencing Factors

### Cybersecurity Culture

Culture is a unit that resides in individuals and is also a force that drives individuals' behavior inside and outside of an organization (Schein, 2009). The subcultures of cybersecurity culture and security culture, have elements of security awareness (when employees are committed to their security mission) and security ownership (employee responsibility to protect information security) (Alnatheer et al., 2002).

### Organizational Cybersecurity Control

Organizational cybersecurity control is a factor involved with directing and motivating individuals to comply with organizational cybersecurity objectives (Boss et al., 2009).

### Cybersecurity Policies

Cybersecurity policies communicate guidance and procedures for employees to comply with in order to meet the wishes of management (von Solms & von Solms, 2004).

### Cybersecurity Procedures

Cybersecurity procedures provide how employees should comply from a procedural perspective (von Solms & von Solms, 2004).

### Cybersecurity Education

Cybersecurity education are structured programs to educate employees on "why" cybersecurity is important; will impact employees for a longer period than training and awareness programs (Caballero, 2009).

### Cybersecurity Training

Cybersecurity training programs are applied learning techniques designed to develop skills for "how" employees are to comply with security policies and procedures (Puhakainen & Siponen, 2010; Siponen, 2000).

### Cybersecurity Awareness

Cybersecurity awareness programs reinforce the "what" and are short term reminders to security compliance (Caballero, 2009).

### Human-Computer Interaction

Human-Computer Interaction (HCI) is the discipline focused on the design of the interface between humans and computers. In the context of this study, this factor would be how HCI may or may not cause human error.

### Macroergonomics

Macroergonomics is the science and practice which considers the physical, organizational and social contexts in which interventions are implemented (Carayon, 2009). For this research, included in this category are factors such as the quality of the work environment, requisite tools, manning parameters, team communications, and time/task parameters.

## **SECTION 2: Internal CS-PIFs**

Internal Cybersecurity Performance Influencing Factors (CS-PIFs) are an individual's circumstances and characteristics that directly or indirectly cause an individual to commit a human error that could lead to a data breach. Identifying a CS-PIF as a contributor to human error pertains to either the presence or the absence of the factor, or the quality of the factor.

SECTION 2 has three sub-sections:

SUB-SECTION 2A: Identification of Internal CS-PIFs (Need feedback)

SUB-SECTION 2B: Validation of Higher Order Internal CS-PIFs (Need feedback)

SUB-SECTION 2C: Internal CS-PIF Definitions (For your information only)

### **SECTION 2A: Identification of Common Internal CS-PIFs**

Please provide your expert opinion about the Common Internal Cybersecurity Performance Influencing Factors (CS-PIFs) by selecting one of the choices below:

1. Keep - the proposed Internal Factor should be included as is.
2. Adjust- the Internal Factor should be included but with modifications (Please provide your feedback below on the exact modifications at the short text field at the end in the space provided).
3. Remove - the proposed Internal Factor should NOT be included (Please recommend reasons below on why not, and propose a replacement if possible at the end in the space provided).

If you feel there are Internal Factors not covered here that should be included, please include them in the space provided below.



Proposed Common Internal Cybersecurity Performance Influencing Factors (CS-PIFs) \*

|                                              | Keep                  | Adjust                | Remove                |
|----------------------------------------------|-----------------------|-----------------------|-----------------------|
| 2A-IF1. Employee Cybersecurity Competency    | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2A-IF2. Employee Cybersecurity Awareness     | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2A-IF3. Employee Cybersecurity Skill         | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2A-IF4. Employee Cybersecurity Self-Efficacy | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2A-IF5. Stress                               | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2A-IF6. Fatigue                              | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2A-IF7. Situation Awareness                  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2A-IF8. Emotion                              | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2A-IF9. Motivation                           | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

2A-IF10. If you selected "2. Adjust" and/or "3. Remove" to at least one of the items above, please provide your recommended adjustments (or "N/A" if none) \*

Your answer

---

2A-IF11. Please provide additional factors that you see fit to be included as Common Internal Cybersecurity Performance Influencing Factors (CS-PIFs) beyond those listed above (or "N/A" if none). For additional factors, please provide a short justification as context for the researcher. \*

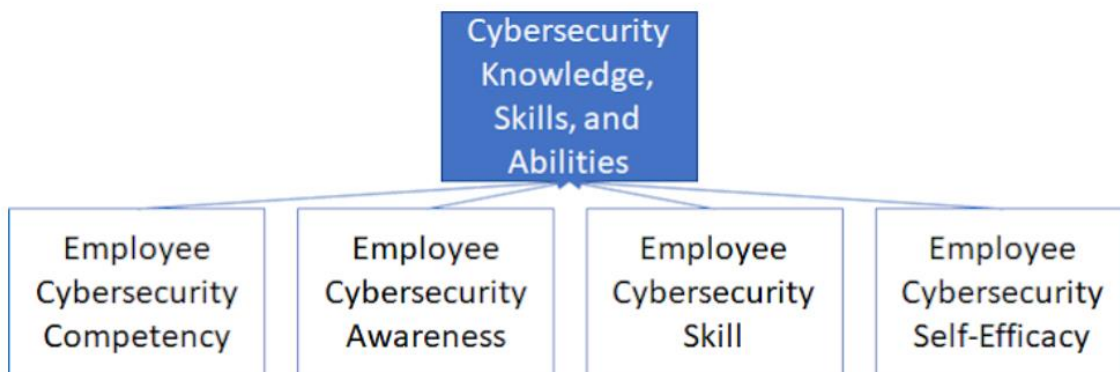
Your answer

---

### SECTION 2B: Validation of Higher Order Internal CS-PIFs

Based on your expert judgement and experience, please rate the appropriateness of the below categorizations, of factors identified in SECTION 2A being grouped similarly. These groupings of higher-order CS-PIFs are required for causal analysis of this proposed research.

2B-IF1. Employee's Cybersecurity KSAs CS-PIF Category



2B-IF1a. Cybersecurity Knowledge, Skills, and Abilities (KSA) is an appropriate higher order CS-PIF categorization for factors that could directly or indirectly cause an individual to commit a human error that could lead to a data breach. \*

2B-IF1b. If you selected 1-5 for IF1a, please provide recommended adjustments (or "N/A" if none). \*

Your answer

---

## 2B-IF2. Employee Cybersecurity Fitness for Duty CS-PIF Category



2B-IF2a. Employee Cybersecurity Fitness for Duty is an appropriate higher order CS-PIF categorization for factors that could directly or indirectly cause an individual to commit a human error that could lead to a data breach. \*

2B-IF2b. If you selected 1-5 for IF2a, please provide recommended adjustments (or "N/A" if none). \*

Your answer

---

## SECTION 2C: Definition of Common Internal CS-PIFs

## Definition of Internal Cybersecurity Performance Influencing Factors

### Employee Cybersecurity Competency

Employee cybersecurity competency is a result of the maturing of an individual's knowledge through improved skills (Carlton & Levy, 2017).

### Employee Cybersecurity Awareness

Employee cybersecurity awareness is "a state where users in an organization are aware of—ideally committed to—their security mission (often expressed in end-user security guidelines)" (Siponen, 2000, p. 31).

### Employee Cybersecurity Skill

Employee cybersecurity skill is the "combination of abilities, knowledge, and experience that enables an individual to complete a task well" (Carlton & Levy, 2017, p. 17).

### Employee Cybersecurity Self-Efficacy

Employee cybersecurity self-efficacy is a form of self-evaluation that is an antecedent to behavior; individuals with high levels of self-efficacy have stronger convictions to utilize their motivation and cognitive resources to successfully execute a task (Rhee et al., 2009).

### Stress

Stress is the human response to a stressor (Swain & Guttman, 1983).

### Fatigue

Fatigue is a suboptimal physical and cognitive state (Gertman et al., 2005).

### Situation Awareness

Situation awareness is the "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 1995, p. 36).

### Emotion

Emotion is phenomena of feelings, behaviors and bodily reactions aroused by external events, and the reactions to those events (Cairns, Pandab, & Power, 2014).

### Motivation

Motivation is the mental and physical effort exerted toward achievement of a goal (Whaley et al., 2016).

## SECTION 3: Please tell us a bit about yourself

3A. What is your gender? \*

Female

Male

3B. What is your age group? \*

- 20-30
- 31-40
- 41-50
- 51-60
- 61-70
- 71-80
- 81 or over

3C. What is your highest level of education? \*

- High School graduate/GED
- Some College
- Associate's degree
- Bachelor's degree
- Master's degree
- Doctoral/Medical/JD degree

3D. What is your main professional role? \*

- Management
- Cybersecurity Professional
- IT Professional
- Other: \_\_\_\_\_

3E. What is your main professional qualification in the role that you hold? \*

- Business Degree
- Business Certificate(s)
- Cybersecurity Degree
- Cybersecurity Certificate(s)
- IT Degree
- IT Certificate(s)
- Other: \_\_\_\_\_

3F. How many years of experience do you have in Cybersecurity? \*

- Under 1 year
- 2 to 5 years
- 6 to 10 years
- 11 to 15 years
- 16 to 20 years
- Over 20 years

3G. How many years have you been using computers? \*

- Under 1 year
- 2 to 5 years
- 6 to 10 years
- 11 to 20 years
- Over 20 years

3H. Have you been in a management role at an organization that has experienced a cybersecurity incident or data breach? \*

- Yes
- No
- Other: \_\_\_\_\_

Submit

## Appendix D

### Case Review Categorization Results 1-50

|    | Businesses (Financial and Insurance Services) (BI) | Businesses (Other) (BSO) | Businesses (Retail/Merchant including Online Retail) (BSR) | Educational Institutions (EDU) | Government & Military (GOV) | Healthcare, Medical Providers and Medical Insurance Services (MED) | Nonprofits (NGC)           | Unknown (UNKN)          |
|----|----------------------------------------------------|--------------------------|------------------------------------------------------------|--------------------------------|-----------------------------|--------------------------------------------------------------------|----------------------------|-------------------------|
| 1  | Misconfiguration                                   | Social Engineering       | Hacked - possible error                                    | Hacked - possible error        | Poor Cybersecurity Hygiene  | Social Engineering                                                 | Misconfiguration           | Hacked - possible error |
| 2  | Hacked - possible error                            | Misconfiguration         | Hacked - possible error                                    | Hacked - possible error        | Misconfiguration            | Social Engineering                                                 | Social Engineering         | 3rd Party - Hacked      |
| 3  | Social Engineering                                 | Social Engineering       | Unavoidable Hack                                           | Unintended Disclosure          | Unintended Disclosure       | Hacked - possible error                                            | Unintended Disclosure      | Hacked - possible error |
| 4  | Hacked - possible error                            | Hacked - possible error  | Misconfiguration                                           | Hacked - possible error        | Social Engineering          | Unintended Disclosure                                              | Hacked - possible error    | Hacked - possible error |
| 5  | Insider Threat                                     | Hacked - possible error  | Hacked - possible error                                    | Hacked - possible error        | Unintended Disclosure       | Hacked - possible error                                            | Hacked - possible error    | Hacked - possible error |
| 6  | Hacked - possible error                            | Misconfiguration         | Misconfiguration                                           | Hacked - possible error        | Hacked - possible error     | Hacked - possible error                                            | Hacked - possible error    | Hacked - possible error |
| 7  | Unintended Disclosure                              | Hacked - possible error  | Misconfiguration                                           | Misconfiguration               | Stolen IS from Secure Area  | Stolen IS from Secure Area                                         | Hacked - possible error    | 3rd Party - Hacked      |
| 8  | Hacked - possible error                            | Misconfiguration         | Poor Cybersecurity Hygiene                                 | Misconfiguration               | Unintended Disclosure       | Stolen IS from Secure Area                                         | Stolen IS from Secure Area | Hacked - possible error |
| 9  | Hacked - possible error                            | Social Engineering       | 3rd Party - Hacked                                         | Hacked - possible error        | Misconfiguration            | 3rd Party - Hacked                                                 | Hacked - possible error    | Hacked - possible error |
| 10 | Insider Threat                                     | Hacked - possible error  | Social Engineering                                         | Hacked - possible error        | 3rd Party - Lost IS         | Hacked - possible error                                            | Stolen IS from Secure Area | Misconfiguration        |
| 11 | Hacked - possible error                            | Hacked - possible error  | Misconfiguration                                           | Hacked - possible error        | Hacked - possible error     | Hacked - possible error                                            | Unintended Disclosure      | Hacked - possible error |
| 12 | Hacked - possible error                            | Misconfiguration         | Hacked - possible error                                    | Hacked - possible error        | Unintended Disclosure       | Hacked - possible error                                            | Unintended Disclosure      | Hacked - possible error |
| 13 | Hacked - possible error                            | Unavoidable Hack         | Hacked - possible error                                    | Misconfiguration               | Insider Threat              | Hacked - possible error                                            | Hacked - possible error    | Hacked - possible error |
| 14 | Hacked - possible error                            | Hacked - possible error  | Hacked - possible error                                    | Hacked - possible error        | Hacked - possible error     | 3rd Party - Stolen IS                                              | Unintended Disclosure      | Unintended Disclosure   |
| 15 | Hacked - possible error                            | Hacked - possible error  | Hacked - possible error                                    | Hacked - possible error        | Unintended Disclosure       | 3rd Party - Stolen IS                                              | Hacked - possible error    | 3rd Party - Hacked      |
| 16 | Stolen IS from Secure Area                         | Unavoidable Hack         | Misconfiguration                                           | Hacked - possible error        | Unintended Disclosure       | Unintended Disclosure                                              | Unintended Disclosure      | Unintended Disclosure   |
| 17 | Insider Threat                                     | Hacked - possible error  | Misconfiguration                                           | Hacked - possible error        | Hacked - possible error     | 3rd Party - Stolen IS                                              | Stolen IS from Secure Area | Hacked - possible error |
| 18 | Hacked - possible error                            | Misconfiguration         | Hacked - possible error                                    | Hacked - possible error        | Unintended Disclosure       | Unintended Disclosure                                              | Hacked - possible error    | Hacked - possible error |
| 19 | Hacked - possible error                            | Hacked - possible error  | Hacked - possible error                                    | Hacked - possible error        | Hacked - possible error     | Unintended Disclosure                                              | Insider Threat             | Hacked - possible error |
| 20 | Misconfiguration                                   | 3rd Party - Hacked       | 3rd Party - Hacked                                         | Misconfiguration               | 3rd Party - Lost IS         | Misconfiguration                                                   | Stolen IS from Secure Area | Hacked - possible error |
| 21 | Insider Threat                                     | Unavoidable Hack         | Hacked - possible error                                    | Misconfiguration               | Misconfiguration            | Stolen IS from Secure Area                                         | Hacked - possible error    | Misconfiguration        |
| 22 | Unintended Disclosure                              | Hacked - possible error  | Hacked - possible error                                    | Misconfiguration               | 3rd Party - Lost IS         | Hacked - possible error                                            | Stolen IS from Secure Area | Hacked - possible error |
| 23 | Stolen IS from Secure Area                         | Hacked - possible error  | Hacked - possible error                                    | Misconfiguration               | Hacked - possible error     | Hacked - possible error                                            | Stolen IS from Secure Area | Unintended Disclosure   |
| 24 | Insider Threat                                     | Hacked - possible error  | Hacked - possible error                                    | Hacked - possible error        | Hacked - possible error     | Unintended Disclosure                                              | Hacked - possible error    | Hacked - possible error |
| 25 | Unintended Disclosure                              | Hacked - possible error  | Hacked - possible error                                    | Hacked - possible error        | Hacked - possible error     | Unintended Disclosure                                              | Hacked - possible error    | Hacked - possible error |
| 26 | Misconfiguration                                   | Hacked - possible error  | Hacked - possible error                                    | Hacked - possible error        | Unintended Disclosure       | Stolen IS from Secure Area                                         | Hacked - possible error    | Unintended Disclosure   |
| 27 | Unintended Disclosure                              | Misconfiguration         | Hacked - possible error                                    | Unintended Disclosure          | Unintended Disclosure       | Hacked - possible error                                            | Hacked - possible error    | Social Engineering      |
| 28 | Hacked - possible error                            | Misconfiguration         | Hacked - possible error                                    | Unintended Disclosure          | Stolen IS from Secure Area  | Stolen IS from Secure Area                                         | Hacked - possible error    | 3rd Party - Hacked      |
| 29 | Insider Threat                                     | Unavoidable Hack         | Hacked - possible error                                    | Unintended Disclosure          | Hacked - possible error     | 3rd party - Lost IS                                                | Hacked - possible error    | 3rd Party - Hacked      |
| 30 | Insider Threat                                     | Unintended Disclosure    | 3rd Party - Hacked                                         | Hacked - possible error        | Unintended Disclosure       | Misconfiguration                                                   | Unintended Disclosure      | Social Engineering      |
| 31 | 3rd Party - Lost IS                                | Hacked - possible error  | Stolen IS from Secure Area                                 | Hacked - possible error        | Unintended Disclosure       | Social Engineering                                                 | Stolen IS from Secure Area | Hacked - possible error |
| 32 | 3rd Party - Lost IS                                | Misconfiguration         | Hacked - possible error                                    | Unintended Disclosure          | Unintended Disclosure       | Stolen IS from Secure Area                                         | Hacked - possible error    | Hacked - possible error |
| 33 | Hacked - possible error                            | Misconfiguration         | Unavoidable Hack                                           | Social Engineering             | Unintended Disclosure       | Insider Threat                                                     | Unavoidable Hack           | Hacked - possible error |
| 34 | Unintended Disclosure                              | Hacked - possible error  | Hacked - possible error                                    | 3rd Party - Stolen IS          | Insider Threat              | Hacked - possible error                                            | Unintended Disclosure      | Hacked - possible error |
| 35 | Misconfiguration                                   | Social Engineering       | Hacked - possible error                                    | Hacked - possible error        | Stolen IS from Secure Area  | Misconfiguration                                                   | Unintended Disclosure      | Misconfiguration        |
| 36 | Hacked - possible error                            | Unavoidable Hack         | Hacked - possible error                                    | Hacked - possible error        | Stolen IS from Secure Area  | Unintended Disclosure                                              | Stolen IS from Secure Area | Hacked - possible error |
| 37 | Social Engineering                                 | Hacked - possible error  | Hacked - possible error                                    | Unintended Disclosure          | Stolen IS from Secure Area  | Stolen IS from Secure Area                                         | Unintended Disclosure      | Social Engineering      |
| 38 | Hacked - possible error                            | Misconfiguration         | Hacked - possible error                                    | Hacked - possible error        | Hacked - possible error     | Hacked - possible error                                            | Hacked - possible error    | Social Engineering      |
| 39 | Unintended Disclosure                              | Misconfiguration         | Hacked - possible error                                    | Hacked - possible error        | Stolen IS from Secure Area  | Hacked - possible error                                            | Stolen IS from Secure Area | Social Engineering      |
| 40 | Unintended Disclosure                              | Unavoidable Hack         | Hacked - possible error                                    | Unintended Disclosure          | Hacked - possible error     | Hacked - possible error                                            | Unintended Disclosure      | Hacked - possible error |
| 41 | Hacked - possible error                            | Misconfiguration         | Hacked - possible error                                    | Unintended Disclosure          | Hacked - possible error     | Hacked - possible error                                            | Stolen IS from Secure Area | Social Engineering      |
| 42 | Hacked - possible error                            | Misconfiguration         | Hacked - possible error                                    | Hacked - possible error        | Unintended Disclosure       | Stolen IS from Secure Area                                         | Hacked - possible error    | Hacked - possible error |
| 43 | Hacked - possible error                            | Misconfiguration         | Stolen IS from Secure Area                                 | Hacked - possible error        | Insider Threat              | Unintended Disclosure                                              | Stolen IS from Secure Area | 3rd Party - Hacked      |
| 44 | Unintended Disclosure                              | Misconfiguration         | Hacked - possible error                                    | Stolen IS from Secure Area     | Unintended Disclosure       | Hacked - possible error                                            | Hacked - possible error    | Hacked - possible error |
| 45 | Unintended Disclosure                              | Hacked - possible error  | Hacked - possible error                                    | Misconfiguration               | Unintended Disclosure       | 3rd party - Lost IS                                                | Hacked - possible error    | 3rd Party - Hacked      |
| 46 | 3rd Party - Hacked                                 | Misconfiguration         | Hacked - possible error                                    | Hacked - possible error        | Unintended Disclosure       | Unavoidable Hack                                                   | Unintended Disclosure      | Misconfiguration        |
| 47 | Misconfiguration                                   | Unavoidable Hack         | Unavoidable Hack                                           | Hacked - possible error        | Hacked - possible error     | Hacked - possible error                                            | Unintended Disclosure      | Hacked - possible error |
| 48 | Unintended Disclosure                              | Misconfiguration         | Misconfiguration                                           | Insider Threat                 | Unintended Disclosure       | Hacked - possible error                                            | Social Engineering         | Hacked - possible error |
| 49 | Stolen IS from Secure Area                         | Hacked - possible error  | Misconfiguration                                           | Hacked - possible error        | Unintended Disclosure       | Unintended Disclosure                                              | Unintended Disclosure      | Hacked - possible error |
| 50 | Hacked - possible error                            | Unintended Disclosure    | Unintended Disclosure                                      | Hacked - possible error        | Unintended Disclosure       | Unintended Disclosure                                              | Insider Threat             | Hacked - possible error |



## Appendix E

## Case Review Categorization Results 51-100

|     | Businesses (Financial and Insurance Services) (BIS) | Businesses (Other) (BSO)   | Businesses (Retail/Merchant including Online Retail) (BSR) | Educational Institutions (EDU) | Government & Military (GOV) | Healthcare, Medical Providers and Medical Insurance Services (MED) | Nonprofits (NGC)           | Unknown (UNKN)             |
|-----|-----------------------------------------------------|----------------------------|------------------------------------------------------------|--------------------------------|-----------------------------|--------------------------------------------------------------------|----------------------------|----------------------------|
| 51  | Social Engineering                                  | Unavoidable Hack           | Hacked - possible error                                    | Hacked - possible error        | Misconfiguration            | 3rd Party - Hacked                                                 | Unintended Disclosure      | Social Engineering         |
| 52  | Hacked - possible error                             | Misconfiguration           | Hacked - possible error                                    | Hacked - possible error        | Unintended Disclosure       | Unintended Disclosure                                              | Hacked - possible error    | Unintended Disclosure      |
| 53  | Unintended Disclosure                               | Misconfiguration           | Unintended Disclosure                                      | Hacked - possible error        | Unintended Disclosure       | Stolen IS from Secure Area                                         | Insider Threat             | 3rd Party - Hacked         |
| 54  | 3rd Party - Hacked                                  | Hacked - possible error    | Poor Cybersecurity Hygiene                                 | Misconfiguration               | Stolen IS from Secure Area  | Stolen IS from Secure Area                                         | Hacked - possible error    | Hacked - possible error    |
| 55  | Social Engineering                                  | Hacked - possible error    | Hacked - possible error                                    | Hacked - possible error        | Misconfiguration            | Unintended Disclosure                                              | Misconfiguration           | Hacked - possible error    |
| 56  | Unintended Disclosure                               | Stolen IS from Secure Area | 3rd Party - Hacked                                         | Misconfiguration               | Unavoidable Hack            | Misconfiguration                                                   | Insider Threat             | Hacked - possible error    |
| 57  | Unintended Disclosure                               | Misconfiguration           | Hacked - possible error                                    | Hacked - possible error        | Stolen IS from Secure Area  | Social Engineering                                                 | Stolen IS from Secure Area | 3rd Party - Hacked         |
| 58  | Unintended Disclosure                               | Misconfiguration           | Hacked - possible error                                    | Stolen IS from Secure Area     | Misconfiguration            | Hacked - possible error                                            | Insider Threat             | Insider Threat             |
| 59  | 3rd Party - Stolen IS                               | 3rd Party - Hacked         | Hacked - possible error                                    | Misconfiguration               | Unintended Disclosure       | Hacked - possible error                                            | Hacked - possible error    | Hacked - possible error    |
| 60  | Insider Threat                                      | Hacked - possible error    | Stolen IS from Secure Area                                 | Social Engineering             | Unintended Disclosure       | Unintended Disclosure                                              | Insider Threat             | Hacked - possible error    |
| 61  | Unintended Disclosure                               | Misconfiguration           | Hacked - possible error                                    | Misconfiguration               | Unintended Disclosure       | Stolen IS from Secure Area                                         | Unintended Disclosure      | Social Engineering         |
| 62  | Social Engineering                                  | Misconfiguration           | Hacked - possible error                                    | Hacked - possible error        | Stolen IS from Secure Area  | Hacked - possible error                                            | Hacked - possible error    | Unintended Disclosure      |
| 63  | Stolen IS from Secure Area                          | Misconfiguration           | Unintended Disclosure                                      | Unintended Disclosure          | Insider Threat              | Social Engineering                                                 | Insider Threat             | Social Engineering         |
| 64  | Unintended Disclosure                               | 3rd Party - Hacked         | Hacked - possible error                                    | Stolen IS from Secure Area     | Hacked - possible error     | 3rd Party - Hacked                                                 | Hacked - possible error    | Hacked - possible error    |
| 65  | Stolen IS from Secure Area                          | Hacked - possible error    | Insider Threat                                             | Insider Threat                 | Hacked - possible error     | 3rd party - Lost IS                                                | Social Engineering         | Hacked - possible error    |
| 66  | Unintended Disclosure                               | Unintended Disclosure      | Hacked - possible error                                    | Stolen IS from Secure Area     | Hacked - possible error     | Stolen IS from Secure Area                                         | Unintended Disclosure      | Social Engineering         |
| 67  | Unintended Disclosure                               | Misconfiguration           | Hacked - possible error                                    | Hacked - possible error        | Insider Threat              | Hacked - possible error                                            | Hacked - possible error    | Hacked - possible error    |
| 68  | Hacked - possible error                             | Misconfiguration           | Unintended Disclosure                                      | Unintended Disclosure          | Misconfiguration            | Hacked - possible error                                            | Unintended Disclosure      | Stolen IS from Secure Area |
| 69  | Hacked - possible error                             | Misconfiguration           | Hacked - possible error                                    | Poor Cybersecurity Hygiene     | Hacked - possible error     | Insider Threat                                                     | Hacked - possible error    | Social Engineering         |
| 70  | Hacked - possible error                             | Hacked - possible error    | Insider Threat                                             | Hacked - possible error        | Hacked - possible error     | Insider Threat                                                     | Hacked - possible error    | Hacked - possible error    |
| 71  | Hacked - possible error                             | Misconfiguration           | Hacked - possible error                                    | Hacked - possible error        | Unintended Disclosure       | Stolen IS from Secure Area                                         | Unintended Disclosure      | 3rd Party - Hacked         |
| 72  | Unintended Disclosure                               | Insider Threat             | Unavoidable Hack                                           | Hacked - possible error        | Poor Cybersecurity Hygiene  | Misconfiguration                                                   | Misconfiguration           | Social Engineering         |
| 73  | Hacked - possible error                             | Hacked - possible error    | Unintended Disclosure                                      | Misconfiguration               | Hacked - possible error     | Hacked - possible error                                            | Social Engineering         | Hacked - possible error    |
| 74  | Misconfiguration                                    | Hacked - possible error    | Hacked - possible error                                    | Hacked - possible error        | Unintended Disclosure       | 3rd party - Lost IS                                                | Hacked - possible error    | Hacked - possible error    |
| 75  | Hacked - possible error                             | Misconfiguration           | Hacked - possible error                                    | Hacked - possible error        | 3rd Party - Lost IS         | Insider Threat                                                     | Unintended Disclosure      | Unintended Disclosure      |
| 76  | Hacked - possible error                             | Unavoidable Hack           | Misconfiguration                                           | Unintended Disclosure          | Unintended Disclosure       | Unintended Disclosure                                              | Hacked - possible error    | Hacked - possible error    |
| 77  | 3rd Party - Stolen IS                               | Stolen IS from Secure Area | Stolen IS from Secure Area                                 | Hacked - possible error        | Hacked - possible error     | Misconfiguration                                                   | Hacked - possible error    | Hacked - possible error    |
| 78  | Unintended Disclosure                               | Hacked - possible error    | Unintended Disclosure                                      | Misconfiguration               | Hacked - possible error     | Unintended Disclosure                                              | Stolen IS from Secure Area | Hacked - possible error    |
| 79  | Misconfiguration                                    | Hacked - possible error    | Stolen IS from Secure Area                                 | Hacked - possible error        | 3rd Party - Lost IS         | Stolen IS from Secure Area                                         | Stolen IS from Secure Area | Hacked - possible error    |
| 80  | Social Engineering                                  | Hacked - possible error    | Hacked - possible error                                    | Unintended Disclosure          | Unintended Disclosure       | Hacked - possible error                                            | Insider Threat             | 3rd Party - Hacked         |
| 81  | Stolen IS from Secure Area                          | 3rd Party - Hacked         | Unintended Disclosure                                      | Hacked - possible error        | Hacked - possible error     | Unintended Disclosure                                              | Unintended Disclosure      | 3rd Party - Hacked         |
| 82  | Insider Threat                                      | Misconfiguration           | Hacked - possible error                                    | 3rd Party - Lost IS            | Hacked - possible error     | Hacked - possible error                                            | Hacked - possible error    | Hacked - possible error    |
| 83  | Unintended Disclosure                               | Hacked - possible error    | Unintended Disclosure                                      | Hacked - possible error        | Poor Cybersecurity Hygiene  | Stolen IS from Secure Area                                         | Stolen IS from Secure Area | Hacked - possible error    |
| 84  | Unintended Disclosure                               | Hacked - possible error    | Hacked - possible error                                    | Hacked - possible error        | Stolen IS from Secure Area  | Insider Threat                                                     | Stolen IS from Secure Area | Hacked - possible error    |
| 85  | Unintended Disclosure                               | Hacked - possible error    | Unintended Disclosure                                      | Unintended Disclosure          | Stolen IS from Secure Area  | 3rd party - Lost IS                                                | Misconfiguration           | Social Engineering         |
| 86  | Insider Threat                                      | Hacked - possible error    | Stolen IS from Secure Area                                 | Unintended Disclosure          | Unintended Disclosure       | Unintended Disclosure                                              | Hacked - possible error    | Social Engineering         |
| 87  | Insider Threat                                      | Hacked - possible error    | Unintended Disclosure                                      | Hacked - possible error        | Unintended Disclosure       | Hacked - possible error                                            | Hacked - possible error    | Hacked - possible error    |
| 88  | Unintended Disclosure                               | Unintended Disclosure      | Hacked - possible error                                    | Unintended Disclosure          | Insider Threat              | Hacked - possible error                                            | Insider Threat             | Social Engineering         |
| 89  | 3rd Party - Stolen IS                               | Unintended Disclosure      | Unavoidable Hack                                           | Stolen IS from Secure Area     | Hacked - possible error     | Hacked - possible error                                            | Stolen IS from Secure Area | Hacked - possible error    |
| 90  | Unintended Disclosure                               | Stolen IS from Secure Area | Unintended Disclosure                                      | Unintended Disclosure          | Unintended Disclosure       | 3rd party - Lost IS                                                | Hacked - possible error    | Hacked - possible error    |
| 91  | Unintended Disclosure                               | Hacked - possible error    | Insider Threat                                             | Stolen IS from Secure Area     | Unintended Disclosure       | Unintended Disclosure                                              | Unintended Disclosure      | Social Engineering         |
| 92  | Hacked - possible error                             | Stolen IS from Secure Area | Unintended Disclosure                                      | Insider Threat                 | Unintended Disclosure       | 3rd party - Lost IS                                                | Insider Threat             | Hacked - possible error    |
| 93  | Hacked - possible error                             | Unintended Disclosure      | Hacked - possible error                                    | Stolen IS from Secure Area     | Insider Threat              | Stolen IS from Secure Area                                         | Stolen IS from Secure Area | Hacked - possible error    |
| 94  | Misconfiguration                                    | Unintended Disclosure      | Hacked - possible error                                    | Misconfiguration               | Unintended Disclosure       | Hacked - possible error                                            | Hacked - possible error    | Hacked - possible error    |
| 95  | Stolen IS from Secure Area                          | Hacked - possible error    | Hacked - possible error                                    | Unintended Disclosure          | Unintended Disclosure       | Hacked - possible error                                            | Hacked - possible error    | Hacked - possible error    |
| 96  | 3rd Party - Stolen IS                               | Misconfiguration           | Unintended Disclosure                                      | Unintended Disclosure          | Misconfiguration            | Unintended Disclosure                                              | Stolen IS from Secure Area | Hacked - possible error    |
| 97  | 3rd Party - Hacked                                  | Unintended Disclosure      | Unintended Disclosure                                      | Unintended Disclosure          | Unintended Disclosure       | Unintended Disclosure                                              | Stolen IS from Secure Area | Hacked - possible error    |
| 98  | Unintended Disclosure                               | Hacked - possible error    | Hacked - possible error                                    | Hacked - possible error        | 3rd Party - Hacked          | Social Engineering                                                 | Unintended Disclosure      | Hacked - possible error    |
| 99  | Hacked - possible error                             | Hacked - possible error    | Hacked - possible error                                    | Unintended Disclosure          | Unintended Disclosure       | Stolen IS from Secure Area                                         | Unintended Disclosure      | Social Engineering         |
| 100 | Unintended Disclosure                               | Unavoidable Hack           | Hacked - possible error                                    | 3rd Party - Hacked             | Unintended Disclosure       | Hacked - possible error                                            | Stolen IS from Secure Area | Hacked - possible error    |



# Appendix G

## Fuzzy-set Qualitative Comparative Analysis

### Membership Calibration Rubric

|                      |                  |               |                  |                 |
|----------------------|------------------|---------------|------------------|-----------------|
| 0.05                 | 0.33             | 0.5           | .66              | .95             |
| Fully Non-Membership | Less out than in | Max Ambiguity | More in than out | Full Membership |

1=Optimal / Desired ||| 0=Not Optimal / Not Desired

| 1. Organizational Cybersecurity (ORGC) |                                                                              |            |
|----------------------------------------|------------------------------------------------------------------------------|------------|
| Cybersecurity Culture                  | Does the organization have a Positive Cybersecurity Culture?                 | Yes = 0.95 |
|                                        | Does the organization have a Negative or non-existent Cybersecurity Culture? | Yes = 0.05 |
| Organizational Cybersecurity Control   | Does the organization have Organizational Cybersecurity Control?             | Yes = 0.95 |
|                                        | Does the organization not have Organizational Cybersecurity Control?         | Yes = 0.05 |

| 2. Cybersecurity Policies and Procedures (CPAP) |                                                                                |            |
|-------------------------------------------------|--------------------------------------------------------------------------------|------------|
| Cybersecurity Policies                          | Does the organization have cybersecurity policies?                             | Yes = 0.95 |
|                                                 | Does the organization lack cybersecurity policies or are they not effective?   | Yes = 0.05 |
| Cybersecurity Procedures                        | Does the organization have cybersecurity procedures?                           | Yes = 0.95 |
|                                                 | Does the organization lack cybersecurity procedures or are they not effective? | Yes = 0.05 |

| 3. Cybersecurity Education, Training, and Awareness (CETA) |                                                                   |            |
|------------------------------------------------------------|-------------------------------------------------------------------|------------|
| Cybersecurity Education                                    | Does the organization have a cybersecurity education program?     | Yes = 0.95 |
|                                                            | Does the organization not have a cybersecurity education program? | Yes = 0.05 |
| Cybersecurity Training                                     | Does the organization have a cybersecurity training program?      | Yes = 0.95 |
|                                                            | Does the organization not have a cybersecurity training program?  | Yes = 0.05 |
| Cybersecurity Awareness                                    | Does the organization have a cybersecurity awareness program?     | Yes = 0.95 |
|                                                            | Does the organization not have a cybersecurity awareness program? | Yes = 0.05 |

| 4. Ergonomics (ERGO)       |                                                                                     |            |
|----------------------------|-------------------------------------------------------------------------------------|------------|
| Human-Computer Interaction | Was HCI NOT a factor in the human error, or not mentioned in the case?              | Yes = 0.95 |
|                            | Was HCI a factor that contributed to the human error?                               | Yes = 0.05 |
| Macro-ergonomics           | Was macro-ergonomics NOT a factor in the human error, or not mentioned in the case? | Yes = 0.95 |
|                            | Was macro-ergonomics a factor that contributed to the human error?                  | Yes = 0.05 |

| 5. Cybersecurity Knowledge, Skills, and Abilities (CKSA) |                                                                           |            |
|----------------------------------------------------------|---------------------------------------------------------------------------|------------|
| Employee Cybersecurity Competency                        | Does the employee have appropriate levels of Cybersecurity Competency?    | Yes = 0.95 |
|                                                          | Does the employee have low levels of Cybersecurity Competency?            | No = 0.05  |
| Employee Cybersecurity Awareness                         | Does the employee have appropriate levels of Cybersecurity Awareness?     | Yes = 0.95 |
|                                                          | Does the employee have low levels of Cybersecurity Awareness?             | No = 0.05  |
| Employee Cybersecurity Skill                             | Does the employee have appropriate levels of Cybersecurity Skill?         | Yes = 0.95 |
|                                                          | Does the employee have low levels of Cybersecurity Skill?                 | No = 0.05  |
| Employee Cybersecurity Self-Efficacy                     | Does the employee have appropriate levels of Cybersecurity Self-Efficacy? | Yes = 0.95 |
|                                                          | Does the employee have low levels of Cybersecurity Self-Efficacy?         | No = 0.05  |

| 6. Employee Cybersecurity Fitness for Duty (CFFD) |                                                                                     |            |
|---------------------------------------------------|-------------------------------------------------------------------------------------|------------|
| Stress                                            | Was the employee NOT stressed when the human error occurred?                        | Yes = 0.95 |
|                                                   | Was the employee stressed when the human error occurred?                            | No = 0.05  |
| Fatigue                                           | Was the employee NOT fatigued when the human error occurred?                        | Yes = 0.95 |
|                                                   | Was the employee fatigued when the human error occurred?                            | No = 0.05  |
| Situational Awareness                             | Was the employee's situational awareness optimal when the human error occurred?     | Yes = 0.95 |
|                                                   | Was the employee's situational awareness NOT optimal when the human error occurred? | No = 0.05  |
| Emotions                                          | Was the employee's emotion optimal when the human error occurred?                   | Yes = 0.95 |
|                                                   | Was the employee's emotion NOT optimal when the human error occurred?               | No = 0.05  |
| Motivations                                       | Was the employee's motivation optimal when the human error occurred?                | Yes = 0.95 |
|                                                   | Was the employee's motivation NOT optimal when the human error occurred?            | No = 0.05  |

1=Occurrence ||| 0=No Occurrence

| 1. Skill Based Error |                                                                                                    |            |
|----------------------|----------------------------------------------------------------------------------------------------|------------|
| Skill Based Error    | The cause of the data breach was caused by a slip (failure of action) or lapse (failure of memory) | Yes = 0.95 |
|                      | The cause of the data breach was NOT caused by an SBE                                              | No = 0.05  |

| 2. Rule Based Mistake |                                                                                                                                 |            |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------|------------|
| Rule Based Mistake    | The cause of the data breach was caused by a misapplication of good rule, application of bad rule, non-application of good rule | Yes = 0.95 |
|                       | The cause of the data breach was NOT caused by an RBM                                                                           | No = 0.05  |

| 3. Knowledge Based Mistake |                                                                                                                         |            |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------|------------|
| Knowledge Based Mistake    | The cause of the data breach was caused during a novel situation that the employee never encountered or was trained for | Yes = 0.95 |
|                            | The cause of the data breach was NOT caused by an KBM                                                                   | No = 0.05  |

| 4. Cybersecurity Human Error |                                                            |            |
|------------------------------|------------------------------------------------------------|------------|
| Cybersecurity Human Error    | The cause of the data breach was caused by human error     | Yes = 0.95 |
|                              | The cause of the data breach was NOT caused by human error | No = 0.05  |

## Appendix H

### Sample Case Review

**2018 – Bezop – 25,000**

BSF – Misconfiguration - [~10 employees](#)

| Abbrev | CS-PIFs and CS-HE Types                          | #   | Note                                                                                                                   |
|--------|--------------------------------------------------|-----|------------------------------------------------------------------------------------------------------------------------|
| CC     | Cybersecurity Culture                            | 0   | As a new company, it is highly likely their security program was not initiated                                         |
| OCC    | Organizational Cybersecurity Control             | 0   |                                                                                                                        |
| OGRC   | Organizational Cybersecurity                     | 0   |                                                                                                                        |
| CPOL   | Cybersecurity Policies                           | 0   | As a new company, it is highly likely their security program was not initiated                                         |
| CPRO   | Cybersecurity Procedures                         |     |                                                                                                                        |
| CPAP   | Cybersecurity Policies and Procedures            |     |                                                                                                                        |
| CE     | Cybersecurity Education                          | 0   | As a new company, it is highly likely their security program was not initiated                                         |
| CT     | Cybersecurity Training                           |     |                                                                                                                        |
| CA     | Cybersecurity Awareness                          |     |                                                                                                                        |
| CETA   | Cybersecurity Education, Training, and Awareness |     |                                                                                                                        |
| HCI    | Human-Computer Interaction                       | 0   | Small company with limited resources                                                                                   |
| ME     | Macro-ergonomics                                 |     |                                                                                                                        |
| ERGO   | Ergonomics                                       |     |                                                                                                                        |
| ECC    | Employee Cybersecurity Competency                | .33 | Mentioned that developers were dealing with DDOS attack at the time and may have not known how to handle               |
| ECA    | Employee Cybersecurity Awareness                 | .33 |                                                                                                                        |
| ECS    | Employee Cybersecurity Skill                     | .33 |                                                                                                                        |
| ECSE   | Employee Cybersecurity Self-Efficacy             | .33 |                                                                                                                        |
| CKSA   | Cybersecurity Knowledge, Skills, and Abilities   | .33 |                                                                                                                        |
| STRE   | Stress                                           | .33 | Limited staffing, multiple roles, handling DDOS attack, starting company up, lot of stress, fatigue is almost apparent |
| FATI   | Fatigue                                          | .33 |                                                                                                                        |
| SA     | Situational Awareness                            | .33 |                                                                                                                        |
| EMOT   | Emotions                                         | .33 |                                                                                                                        |
| MOTI   | Motivations                                      | .33 |                                                                                                                        |
| CFFD   | Employee Cybersecurity Fitness for Duty          | 0   |                                                                                                                        |
| SBE    | Skill-Based Error                                |     | Misconfigured                                                                                                          |
| RBM    | Rule-Based Mistake                               | 1   |                                                                                                                        |
| KBM    | Knowledge-Based Mistake                          |     |                                                                                                                        |

[On Mar 30, researchers](#) at [MacKeeper Security](#) identified a database open to the public containing full names, addresses, email addresses, encrypted passwords, wallet information, along with links to scanned passports, driver's licenses, and other IDs for over 25,000 investors of the newly created Bezop. The information was found within a MongoDB database without any security. In fact, it's a little difficult to grasp how it could happen, even if by mistake. Given the changes to MongoDB, it would have to have been deliberately configured (RBM=1) to be public, a configuration which should not even be risked internally.

[Data security wasn't](#) the first issue to strike the Bezop ICO. In response to scores of complaints from investors and bounty program participants, they issued a statement in which they announced "We clearly got caught with our pants down around our ankles during the ICO. What you need to understand is that we were a very small company at the time with very limited resources."

[If you remember, we reported](#) a DDoS attack and a couple of security holes that unintentionally exposed user data such as name, wallet addresses, address on file, copies of identification documents, etc., and that they could possibly be in the public domain. That database has since been closed and [secured](#)

[A company representative](#) has already admitted to this data breach, explaining that the MongoDB database was negligently exposed online [in the midst](#) of a DDoS attack its developers were dealing with (CFFD=0, ECS=0). The DDoS attack took place on January 8, and it proves how devastating these attacks are to businesses.

[Because we still hadn't](#) gotten things fixed and staff were performing 2 and 3 jobs at once.

## Appendix I

## Final Data Matrix

## Cases 1-50

| Company                                                        | SBE  | RBM  | KBM  | CSHE | ORGC | CPAP | CETA | ERGO | CKSA | CFFD |
|----------------------------------------------------------------|------|------|------|------|------|------|------|------|------|------|
| YMCA of San Diego                                              | 0.95 | 0.05 | 0.05 | 0.95 | 0.33 | 0.05 | 0.67 | 0.67 | 0.33 | 0.05 |
| SEIU 32BJ                                                      | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.33 | 0.33 |
| Hampton Redevelopment and Housing Authority                    | 0.95 | 0.05 | 0.05 | 0.95 | 0.33 | 0.33 | 0.33 | 0.67 | 0.33 | 0.33 |
| Allconnect                                                     | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.05 | 0.05 |
| Leaf filter north llc                                          | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.05 | 0.33 |
| Corporate Employment Resources, Inc.                           | 0.95 | 0.05 | 0.05 | 0.95 | 0.33 | 0.33 | 0.33 | 0.67 | 0.95 | 0.05 |
| Coty inc                                                       | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.67 |
| Oldcastle APG, Inc.                                            | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.05 | 0.33 | 0.95 | 0.33 | 0.67 |
| Sunspire health                                                | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.95 | 0.05 | 0.67 |
| TCM Bank                                                       | 0.05 | 0.95 | 0.05 | 0.95 | 0.33 | 0.05 | 0.05 | 0.67 | 0.05 | 0.67 |
| Home Depot                                                     | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.67 | 0.05 | 0.95 | 0.05 | 0.95 |
| Teensafe                                                       | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.33 | 0.33 | 0.67 | 0.05 | 0.67 |
| Transamerica retirement solutions llc                          | 0.95 | 0.05 | 0.05 | 0.95 | 0.95 | 0.95 | 0.67 | 0.67 | 0.33 | 0.33 |
| Qualified plans llc                                            | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.95 | 0.05 | 0.67 |
| Aetna                                                          | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.33 | 0.05 | 0.95 | 0.05 | 0.33 |
| Belmont Savings Bank (BSB)                                     | 0.95 | 0.05 | 0.05 | 0.95 | 0.33 | 0.95 | 0.05 | 0.95 | 0.05 | 0.33 |
| Feinstein Institute for Medical Research                       | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 | 0.95 | 0.05 | 0.67 |
| Stanford Federal Credit Union                                  | 0.95 | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.67 | 0.05 | 0.95 | 0.05 |
| Blue Shield of California/Department of Managed Healthcare     | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.33 | 0.67 | 0.05 | 0.33 |
| University of Virginia, Aetna Health Care                      | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.67 | 0.05 | 0.33 |
| Flexible Benefit Service Corporation                           | 0.95 | 0.05 | 0.05 | 0.95 | 0.33 | 0.95 | 0.33 | 0.67 | 0.33 | 0.33 |
| Bezop                                                          | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.05 | 0.33 | 0.05 |
| Purdue university                                              | 0.95 | 0.05 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.95 | 0.33 | 0.05 |
| 211 L.A. County                                                | 0.05 | 0.95 | 0.05 | 0.95 | 0.67 | 0.33 | 0.67 | 0.67 | 0.33 | 0.33 |
| National Finance Center                                        | 0.05 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.33 | 0.67 | 0.05 | 0.33 |
| NJ Department of Labor and Workforce Development               | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.33 | 0.33 | 0.05 | 0.05 | 0.05 |
| Oklahoma University                                            | 0.05 | 0.95 | 0.05 | 0.95 | 0.95 | 0.67 | 0.33 | 0.67 | 0.33 | 0.67 |
| Anthem Blue Cross                                              | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.33 | 0.67 |
| First Advantage Tax Consulting Services (TCS)                  | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.33 | 0.05 | 0.33 |
| Renaissance philanthropic solutions group                      | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.05 | 0.95 |
| Arkansas Army National Guard                                   | 0.95 | 0.05 | 0.05 | 0.95 | 0.33 | 0.05 | 0.95 | 0.33 | 0.33 | 0.05 |
| Victoria independent school district                           | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.33 | 0.33 | 0.95 | 0.05 | 0.67 |
| Riverside Community College                                    | 0.95 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 | 0.33 | 0.05 | 0.05 |
| U.S. Agriculture Department                                    | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.05 | 0.95 |
| Massachusetts Department of Revenue                            | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.05 | 0.05 | 0.67 |
| University of Hawai'i West O'ahu (UHWO)                        | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 | 0.33 | 0.05 | 0.95 |
| Clinical pathology laboratories southeast inc                  | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.33 | 0.67 | 0.33 | 0.67 |
| Yale University                                                | 0.05 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.67 | 0.95 | 0.33 | 0.95 |
| FDIC                                                           | 0.05 | 0.05 | 0.95 | 0.95 | 0.95 | 0.33 | 0.95 | 0.67 | 0.67 | 0.67 |
| University of Colorado, Boulder                                | 0.05 | 0.95 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 |
| Wells Fargo                                                    | 0.05 | 0.95 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.05 | 0.33 | 0.33 |
| Orrstown bank                                                  | 0.95 | 0.05 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.67 | 0.05 | 0.05 |
| American esoteric laboratories                                 | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.33 | 0.33 | 0.95 | 0.05 | 0.33 |
| Poway Unified School District                                  | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.05 | 0.33 | 0.33 |
| Robeson County Board of Elections                              | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.33 | 0.33 | 0.67 | 0.33 | 0.67 |
| Stanford University                                            | 0.05 | 0.95 | 0.05 | 0.95 | 0.33 | 0.95 | 0.33 | 0.33 | 0.33 | 0.33 |
| Aimbridge hospitality holdings llc                             | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.05 | 0.33 |
| Louisiana Board of Regents                                     | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.05 | 0.67 |
| Medassets Inc., Saint Barnabas Health Care System, Cook County | 0.05 | 0.05 | 0.95 | 0.95 | 0.67 | 0.95 | 0.95 | 0.95 | 0.33 | 0.33 |

## Appendix J

## Final Data Matrix

## Cases 51-102

| Company                                                             | SBE  | RBM  | KBM  | CSHE | ORGC | CPAP | CETA | ERGO | CKSA | CFFD |
|---------------------------------------------------------------------|------|------|------|------|------|------|------|------|------|------|
| Housatonic Community College                                        | 0.95 | 0.05 | 0.05 | 0.95 | 0.33 | 0.33 | 0.05 | 0.67 | 0.05 | 0.33 |
| Washington State Health Authority (HCA)                             | 0.05 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.95 | 0.95 | 0.05 | 0.95 |
| Lincoln Financial Group, Lincoln National Life Insurance Company    | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.33 | 0.33 | 0.67 | 0.33 | 0.67 |
| Franklin's Budget Car Sales, Inc.                                   | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 | 0.05 | 0.05 | 0.33 |
| Transportation Security Administration (TSA)                        | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.95 | 0.95 | 0.67 | 0.05 | 0.67 |
| Virginia Department of Education                                    | 0.95 | 0.05 | 0.05 | 0.95 | 0.95 | 0.95 | 0.67 | 0.67 | 0.33 | 0.33 |
| U.S. Department of Energy                                           | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.95 | 0.33 | 0.05 | 0.05 | 0.95 |
| Connecticut Department of Revenue Services                          | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.33 | 0.95 | 0.05 | 0.05 |
| The Princeton Review                                                | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.33 | 0.33 | 0.67 | 0.33 | 0.67 |
| Wisconsin Department of Revenue                                     | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.95 | 0.95 | 0.67 | 0.33 | 0.33 |
| Centerstone Insurance and Financial Services (d/b/a BenefitMall)    | 0.95 | 0.05 | 0.05 | 0.95 | 0.33 | 0.33 | 0.05 | 0.67 | 0.05 | 0.33 |
| Community Mercy Health Partners                                     | 0.05 | 0.95 | 0.05 | 0.95 | 0.33 | 0.05 | 0.33 | 0.67 | 0.33 | 0.33 |
| Lifeline (Federal Communications Commission), TerraCom Inc., Y      | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.33 | 0.67 |
| Oklahoma State Department of Health                                 | 0.05 | 0.05 | 0.95 | 0.95 | 0.67 | 0.95 | 0.67 | 0.95 | 0.33 | 0.33 |
| Massachusetts Secretary of State Office                             | 0.05 | 0.95 | 0.05 | 0.95 | 0.33 | 0.33 | 0.33 | 0.67 | 0.05 | 0.33 |
| Georgia Division of Public Health                                   | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 |
| Virginia Polytechnic Institute and State University (Virginia Tech) | 0.05 | 0.95 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.67 | 0.33 | 0.33 |
| Health equity inc                                                   | 0.95 | 0.05 | 0.05 | 0.95 | 0.67 | 0.33 | 0.67 | 0.67 | 0.33 | 0.33 |
| Mesa County, Western Colorado Drug Task Force                       | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.33 | 0.33 | 0.67 | 0.33 | 0.95 |
| Blue Cross and Blue Shield of Georgia                               | 0.05 | 0.95 | 0.05 | 0.95 | 0.33 | 0.33 | 0.33 | 0.67 | 0.33 | 0.67 |
| Davidson Companies                                                  | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.05 | 0.67 |
| Western Connecticut State University                                | 0.05 | 0.95 | 0.05 | 0.95 | 0.33 | 0.67 | 0.67 | 0.67 | 0.33 | 0.95 |
| National Archives and Records Administration                        | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 | 0.33 | 0.05 | 0.33 |
| Florida Agency for Workforce Innovation                             | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.33 | 0.33 | 0.67 | 0.33 | 0.33 |
| Urology Austin, PLLC                                                | 0.95 | 0.05 | 0.05 | 0.95 | 0.67 | 0.95 | 0.33 | 0.67 | 0.05 | 0.05 |
| Southern California Medical-Legal Consultants, Inc. (SCMLC)         | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.67 | 0.33 | 0.67 | 0.33 | 0.33 |
| Cord Blood Registry                                                 | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.05 | 0.33 | 0.67 | 0.05 | 0.05 |
| Beacon Health System                                                | 0.95 | 0.05 | 0.05 | 0.95 | 0.33 | 0.05 | 0.05 | 0.67 | 0.05 | 0.33 |
| Touchstone Medical Imaging, LLC                                     | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.33 | 0.33 |
| Emory Healthcare                                                    | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.95 | 0.33 | 0.67 | 0.33 | 0.67 |
| University of Florida College of Dentistry                          | 0.05 | 0.95 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.67 | 0.33 | 0.67 |
| Affinity Health Plan, Inc.                                          | 0.05 | 0.95 | 0.05 | 0.95 | 0.33 | 0.67 | 0.33 | 0.67 | 0.33 | 0.33 |
| California Correctional Health Care Services                        | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.33 | 0.05 | 0.95 | 0.33 | 0.33 |
| California Public Employees' Retirement System (CalPERS)            | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.33 | 0.33 |
| JPMorgan Chase                                                      | 0.05 | 0.95 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.05 | 0.67 | 0.33 |
| County of Los Angeles Departments of Health and Mental Health       | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.33 | 0.05 | 0.67 | 0.05 | 0.33 |
| Utah Department of Technology Services                              | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.67 | 0.05 | 0.33 |
| Science Applications International Corp. (SAIC)                     | 0.05 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.67 | 0.67 | 0.33 | 0.33 |
| Ohio state workers                                                  | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.05 | 0.05 |
| Health Net                                                          | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.33 | 0.33 |
| Cloudflare                                                          | 0.05 | 0.95 | 0.05 | 0.95 | 0.95 | 0.95 | 0.67 | 0.67 | 0.67 | 0.33 |
| Secretary of State Brian Kemp                                       | 0.05 | 0.05 | 0.95 | 0.95 | 0.67 | 0.95 | 0.95 | 0.05 | 0.33 | 0.95 |
| South Carolina Department of Revenue                                | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.05 | 0.33 |
| Office of the Texas Attorney General                                | 0.95 | 0.05 | 0.05 | 0.95 | 0.67 | 0.05 | 0.33 | 0.05 | 0.33 | 0.33 |
| ClixSense                                                           | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.05 | 0.33 |
| Premera Blue Cross                                                  | 0.95 | 0.05 | 0.05 | 0.95 | 0.05 | 0.33 | 0.05 | 0.67 | 0.33 | 0.33 |
| Bank of New York Mellon                                             | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.33 | 0.33 |
| Office of Personnel Management (OPM)                                | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.33 | 0.05 | 0.67 | 0.05 | 0.95 |
| IRS                                                                 | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.67 | 0.05 | 0.67 | 0.05 | 0.95 |
| Panera Bread                                                        | 0.05 | 0.05 | 0.95 | 0.95 | 0.33 | 0.67 | 0.67 | 0.67 | 0.95 | 0.33 |
| TJ stores (TJX), including TJMaxx, Marshalls, Winners, HomeSense    | 0.05 | 0.05 | 0.95 | 0.95 | 0.95 | 0.95 | 0.95 | 0.05 | 0.67 | 0.95 |
| Equifax Corporation                                                 | 0.05 | 0.05 | 0.95 | 0.95 | 0.05 | 0.95 | 0.33 | 0.05 | 0.95 | 0.67 |
| Deep Root Analytics                                                 | 0.05 | 0.95 | 0.05 | 0.95 | 0.05 | 0.05 | 0.05 | 0.67 | 0.33 | 0.33 |

## References

- Abdolrahmani, A., Easley, W., Williams, M., Branham, S., & Hurst, A. (2017, May). Embracing errors: Examining how context of use impacts blind individuals' acceptance of navigation aid errors. *Proceedings from 2017 CHI Conference on Human Factors in Computing Systems* (pp. 4158–4169). Denver, CO. <https://doi.org/10.1145/3025453.3025528>
- Agarwal, R., Sambamurthy, V., & Stair, R. M. (2000). The evolving relationship between general and specific computer self-efficacy—An empirical assessment. *Information Systems Research, 11*(4), 418–430. <https://doi.org/10.1287/isre.11.4.418.11876>
- Ahmed, M., Sharif, L., Kabir, M., & Al-Maimani, M. (2012). Human errors in information security. *International Journal of Advanced Trends in Computer Science and Engineering, 1*(3), 82–87.
- Alavi, R., Islam, S., & Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. *Information & Computer Security, 24*(2). <https://doi.org/10.1108/ICS-01-2016-0006>
- Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and measuring information security culture. *Proceedings of the Pacific Asia Conference on Information Systems* (pp. 1–16). Retrieved from <https://aisel.aisnet.org/pacis2012/144>
- Alonso, I. J., & Broadribb, M. (2018). Human error: A myth eclipsing real causes. *Process Safety Progress, 37*(2), 145–149. <https://doi.org/10.1002/prs.11936>
- Alshboul, Y., & Streff, K. (2017). Beyond cybersecurity awareness: Antecedents and satisfaction. In *Proceedings of the 2017 International Conference on Software and e-Business* (pp. 85–91). ACM. <https://doi.org/10.1145/3178212.3178218>
- Amenta, E., & Poulsen, J. D. (1994). Where to begin: A survey of five approaches to selecting independent variables for qualitative comparative analysis. *Sociological Methods & Research, 23*(1), 22–53. <https://doi.org/10.1177/0049124194023001002>
- American Society of Safety Professionals (2012). Proposed rule to strengthen railroad training programs. *Professional Safety, 57*(4), 24.
- Anderson, J. R. (1982). Acquisition of cognitive skill. *Psychological Review, 89*(4), 369–406. <https://doi.org/10.1037/0033-295X.89.4.369>



- Angst, C. M., Block, E. S., D'arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, 41(3), 893-916. <https://doi.org/10.25300/MISQ/2017/41.3.10>
- Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005–2011: Trends and insights. *Journal of Information Privacy and Security*, 8(2), 33–56. <https://doi.org/10.1080/15536548.2012.10845654>
- Balle, A. C., Curado, C., & Oliveira, M. (2018). Knowledge donation and knowledge collection patterns in a free software community. *Online Journal of Applied Knowledge Management*, 6(2), 23–36. [https://doi.org/10.36965/OJAKM.2018.6\(2\)23-36](https://doi.org/10.36965/OJAKM.2018.6(2)23-36)
- Balle, A., Steffen, M. O., Curado, C. and Oliveira, M. (2019). Interorganizational knowledge sharing in a science and technology park: The use of knowledge sharing mechanisms. *Journal of Knowledge Management*, 23(10), 2016-2038. <https://doi.org/10.1108/JKM-05-2018-0328>
- Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, 39, 145–159. <https://doi.org/10.1016/j.cose.2013.05.006>
- Basurto, X., & Speer, J. (2012). Structuring the calibration of qualitative data as sets for qualitative comparative analysis (QCA). *Field Methods*, 24(2), 155–174. <https://doi.org/10.1177/1525822X11433998>
- Baxter, G. D., & Bass, E. J. (1998, March). Human error revisited: Some lessons for situation awareness. In *Proceedings Fourth Annual Symposium on Human Interaction with Complex Systems* (pp. 81–87). IEEE. <https://doi.org/10.1109/HUICS.1998.659960>
- Berg-Schlosser, D. De Meur, G., Rihoux, B., & Ragin, C. C. (2009). Qualitative comparative analysis (QCA) as an approach. In B. Rihoux & C. C. Ragin (Eds.), *Configurational comparative methods: Qualitative comparative analysis (QCA) and related techniques* (pp. 1–18). Thousand Oaks, CA: Sage Publications.
- Bernardino, G. and Curado, C. (2020). Training evaluation: Causal conditions for success and failure of trainers and trainees. *European Journal of Training and Development*, 44(4/5), 531-546. <https://doi.org/10.1108/EJTD-10-2019-0177>
- Bolton, M. L. (2017). A task-based taxonomy of erroneous human behavior. *International Journal of Human-Computer Studies*, 108, 105–121. <https://doi.org/10.1016/j.ijhcs.2017.06.006>



- Boring, R. L. (2007). Dynamic human reliability analysis: Benefits and challenges of simulating human performance. *In Proceedings of the 2007 European Safety and Reliability Conference* (pp. 1-8). Idaho National Laboratory (INL).
- Boring, R. L. (2010). How many performance shaping factors are necessary for human reliability analysis? *INL/CON-10-18620*. Idaho Falls, ID: Idaho National Laboratory (INL).
- Boring, R. L., Gertman, D. I., & Ulrich, T. A. (2019, July). Human reliability research needs for long-duration spaceflight. *In International Conference on Applied Human Factors and Ergonomics* (pp. 289-297). [https://doi.org/10.1007/978-3-030-20037-4\\_26](https://doi.org/10.1007/978-3-030-20037-4_26)
- Boring, R. L., Griffith, C. D., & Joe, J. C. (2007). The measure of human error: Direct and indirect performance shaping factors. *In 2007 IEEE 8th Human Factors and Power Plants and HPRCT 13th Annual Meeting* (pp. 170–176). IEEE. <https://doi.org/10.1109/HFPP.2007.4413201>
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864. <https://www.jstor.org/stable/26628654>
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151–164. <https://doi.org/10.1057/ejis.2009.8>
- Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011, September). Human performance in cybersecurity: A research agenda. *Proceedings of the Human Factors and Ergonomics Society*, 55(1) (pp. 1115–1119). <https://doi.org/10.1177/1071181311551233>
- Bratus, S., Masone, C., & Smith, S. W. (2008). Why do street-smart people do stupid things online? *IEEE Security & Privacy*, 6(3), 71–74. <https://doi.org/10.1109/MSP.2008.79>
- Buckley, O., Nurse, J. R., Legg, P. A., Goldsmith, M., & Creese, S. (2014, July). Reflecting on the ability of enterprise security policy to address accidental insider threat. *In 2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 8–15). IEEE. <https://doi.org/10.1109/STAST.2014.10>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523–548. <https://doi.org/10.2307/25750690>

- Burley, D. L., Bishop, M., Buck, S., Ekstrom, J. J., Fatcher, L., Gibson, D.,... Parrish, A. (2017). Curriculum guidelines for post-secondary degree programs in cybersecurity. *Cybersecurity Curricula 2017*. Retrieved from [https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover\\_csec2017.pdf](https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf)
- Caballero, A. (2009). Information security essentials for IT managers: Protecting mission-critical systems. In J. R. Vacca (Ed.). *Computer and Information Security Handbook* (pp. 225–254). Burlington, MA: Morgan Kaufman.
- Cairns, P., Pandab, P., & Power, C. (2014). The influence of emotion on number entry errors. In *Proceedings of the 32nd annual ACM conference on human factors in computing systems* (pp. 2293–2296). ACM. <https://doi.org/10.1145/2556288.2557065>
- Carayon, P. (2009). The balance theory and the work system model... Twenty years later. *International Journal of Human–Computer Interaction*, 25(5), 313–327. <https://doi.org/10.1080/10447310902864928>
- Carayon, P., & Smith, M. J. (2000). Work organization and ergonomics. *Applied Ergonomics*, 31(6), 649–662. [https://doi.org/10.1016/S0003-6870\(00\)00040-5](https://doi.org/10.1016/S0003-6870(00)00040-5)
- Carre, J. R., Curtis, S. R., & Jones, D. N. (2018). Ascribing responsibility for online security and data breaches. *Managerial Auditing Journal*, 33(4). <https://doi.org/10.1108/MAJ-11-2017-1693>
- Carlton, M., & Levy, Y. (2017). Cybersecurity skills: The cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management*, 5(2), 16–28. [https://doi.org/10.36965/OJAKM.2017.5\(2\)16-28](https://doi.org/10.36965/OJAKM.2017.5(2)16-28)
- CERT Insider Threat Team (2013). *Unintentional insider threats: A foundational study*. Retrieved from <https://www.sei.cmu.edu/reports/13tn022.pdf>
- Chang, E. S., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, 107(3), 438–458. <https://doi.org/10.1108/02635570710734316>
- Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5), 1–14. <https://doi.org/10.1002/widm.1211>
- Cheng, X. Y., Wang, Y. M., & Xu, Z. L. (2006, August). Risk assessment of human error in information security. *Proceedings from 2006 International Conference on Machine Learning and Cybernetics* (pp. 3573–3578). Dalian, China. <https://doi.org/10.1109/ICMLC.2006.258573>

- Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. *Journal of Medical Systems*, 43(1), 1-12. <https://doi.org/10.1007/s10916-018-1123-2>
- Choi, M., Levy, Y., & Hovav, A. (2013, December). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. In *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC–Workshop on Information Security and Privacy (WISP)* (pp. 1–19).
- Clarke, K., & Levy, Y. (2017). Cybersecurity vital signs: The role of anomaly detection on insider threat triage. *Proceeding of the Knowledge Management (KM) 2017 Conference* (pp. 79–89).
- Cram, W. A., Proudfoot, J. G., & D’arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, 26(6), 605-641. <https://doi.org/10.1057/s41303-017-0059-9>
- Crespo, N., Curado, C., Oliveira, M., Muñoz-Pascual, L. (2021). Entrepreneurial capital leveraging innovation in micro firms: A mixed methods perspective. *Journal of Business Research*, 123, 333-342. <https://doi.org/10.1016/j.jbusres.2020.10.001>
- Cress, D. M., & Snow, D. A. (2000). The outcomes of homeless mobilization: The influence of organization, disruption, political mediation, and framing. *American Journal of Sociology*, 105(4), 1063–1104. <https://doi.org/10.1086/210399>
- Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the ChoicePoint and TJX data breaches. *MIS Quarterly*, 33(4), 673–687. <https://doi.org/10.2307/20650322>
- Curado, C. (2017). Human resource management contribution to innovation in small and medium-sized enterprises: A mixed methods approach. *Creativity and Innovation Management*, 27, 79–90. <https://doi.org/10.1111/caim.12251>
- Curado, C., Henriques, P., Oliveira, M. and Martins, R. (2021). Organisational culture as an antecedent of knowledge sharing in NGOs. *Knowledge Management Research & Practice*, 1-13. <https://doi.org/10.1080/14778238.2021.1908864>
- Curado, C., Henriques, P. L., Oliveira, M., & Matos, P. V. (2016). A fuzzy-set analysis of hard and soft sciences publication performance. *Journal of Business Research*, 69(11), 5348–5353. <https://doi.org/10.1016/j.jbusres.2016.04.136>
- Curado, C., Muñoz-Pascual, L., & Galende, J. (2018). Antecedents to innovation performance in SMEs: A mixed methods approach. *Journal of Business Research*, 18, 206–215. <https://doi.org/10.1016/j.jbusres.2017.12.056>

- Curado, C. & Sousa, I. (2021). Training evaluation of a sales programme in a Portuguese cosmetics SME. *Industrial and Commercial Training*, 53(3), 283-293. <https://doi.org/10.1108/ICT-12-2019-0107>
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79–98. <https://doi.org/10.1287/isre.1070.0160>
- D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), 43-69. <https://doi.org/10.1111/isj.12173>
- Da Veiga, A. (2016, July). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *2016 SAI Computing Conference (SAI)* (pp. 1006-1015). IEEE. <https://doi.org/10.1109/SAI.2016.7556102>
- da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, 162–176. <https://doi.org/10.1016/j.cose.2014.12.006>
- da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70, 72–94. <https://doi.org/10.1016/j.cose.2017.05.002>
- de Block, D., & Vis, B. (2019). Addressing the challenges related to transforming qualitative into quantitative data in qualitative comparative analysis. *Journal of Mixed Methods Research*, 13(4), 503-535. <https://doi.org/10.1177/1558689818770061>
- Deal, T. E., & Kennedy, A. A. (1982). *Corporate cultures: The rites and rituals of organizational life*. Reading: MA: Addison-Wesley.
- Dekker, S. (2006). *The field guide to understanding human error*. Surrey: Ashgate Publishing, Ltd.
- Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal*, 18(4), 326–342. <https://doi.org/10.4018/irmj.2005100102>
- Dormann, T., & Frese, M. (1994). Error training: Replication and the function of exploratory behavior. *International Journal of Human Computer Interaction*, 6(4), 365–372. <https://doi.org/10.1080/10447319409526101>
- Douglas, E. J., Shepherd, D. A., & Prentice, C. (2020). Using fuzzy-set qualitative comparative analysis for a finer-grained understanding of entrepreneurship.

*Journal of Business Venturing*, 35(1), 105970.  
<https://doi.org/10.1016/j.jbusvent.2019.105970>

- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science & Information Technology*, 6, 323–337. <https://doi.org/10.28945/1062>
- Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human factors*, 37(1), 32–64. <https://doi.org/10.1518/001872095779049543>
- Endsley, M. R. (2015). Situation awareness misconceptions and misunderstandings. *Journal of Cognitive Engineering and Decision Making*, 9(1), 4–32. <https://doi.org/10.1177/1555343415572631>
- Enrici, I., Ancilli, M., & Liroy, A. (2010, May). A psychological approach to information technology security. *Proceedings from 2010 IEEE 3<sup>rd</sup> Conference on Human System Interactions (HSI)* (pp. 459–466). <https://doi.org/10.1109/HSI.2010.5514528>
- Evans, M. G., He, Y., Yevseyeva, I., & Janicke, H. (2019). Published incidents and their proportions of human error. *Information & Computer Security*, 27(3). <https://doi.org/10.1108/ICS-12-2018-0147>
- Fiss, P. C. (2007). A set-theoretic approach to organizational configurations. *Academy of Management Review*, 32(4), 1180–1198. <https://doi.org/10.5465/amr.2007.26586092>
- Fiss, P. C. (2011). Building better causal theories: A fuzzy set approach to typologies in organization research. *Academy of Management Journal*, 54(2), 393–420. <https://doi.org/10.5465/amj.2011.60263120>
- Forester, J., Kolaczowski, A., Lois, E., & Kelly, D. (2006). Evaluation of human reliability analysis methods against good practices: Final report. NUREG-1842. Washington, DC: US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.
- Franciosi, C., Di Pasquale, V., Iannone, R., & Miranda, S. (2019). A taxonomy of performance shaping factors for human reliability analysis in industrial maintenance. *Journal of Industrial Engineering and Management*, 12(1), 115–132. <http://dx.doi.org/10.3926/jiem.2702>
- French, S., Bedford, T., Pollard, S. J., & Soane, E. (2011). Human reliability analysis: A critique and review for managers. *Safety Science*, 49(6), 753–763. <https://doi.org/10.1016/j.ssci.2011.02.008>
- Friedlander, M. A., & Evans, S. A. (1997, June). Influence of organizational culture on human error. *In Proceedings of the 1997 IEEE Sixth Conference on Human*

- Factors and Power Plants, 1997.*'Global Perspectives of Human Factors in Power Generation' (pp. 12–19). IEEE. <https://doi.org/10.1109/HFPP.1997.624870>
- Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change, 10*(1), 2. <https://doi.org/10.5590/JOSC.2018.10.1.02>
- Garrison, C., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security, 19*(4), 216–230. <https://doi.org/10.1108/09685221111173049>
- Gaur, A., & Kumar, M. (2018). A systematic approach to conducting review studies: An assessment of content analysis in 25 years of IB research. *Journal of World Business, 53*(2), 280-289. <https://doi.org/10.1016/j.jwb.2017.11.003>
- Gawron, V. J., Drury, C. G., Fairbanks, R. J., & Berger, R. C. (2006). Medical error and human factors engineering: Where are we now? *American Journal of Medical Quality, 21*(1), 57–67. <https://doi.org/10.1177%2F1062860605283932>
- Gcaza, N., & von Solms, R. (2017). Cybersecurity culture: An ill-defined problem. *Proceedings from IFIP World Conference on Information Security Education* (pp. 98-109). [https://doi.org/10.1007/978-3-319-58553-6\\_9](https://doi.org/10.1007/978-3-319-58553-6_9)
- Gcaza, N., von Solms, R., Grobler, M. M., & van Vuuren, J. J. (2017). A general morphological analysis: Delineating a cyber-security culture. *Information & Computer Security, 25*(3), 259-278. <https://doi.org/10.1108/ICS-12-2015-0046>
- Gertman, D., Blackman, H., Marble, J., Byers, J., & Smith, C. (2005). The SPAR-H human reliability analysis method. *NUREG/CR-6883, INL/EXT-05-00509*. Washington, DC: US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.
- Gonçalves, T., Curado, C. and Balle, A. (2021). Psychosocial antecedents of knowledge sharing in healthcare research centers: A mixed methods approach. *Journal of Health Organization and Management, Vol. ahead-of-print No. ahead-of-print*. <https://doi.org/10.1108/JHOM-12-2020-0463>
- Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *Online Journal of Applied Knowledge Management, 6*(1), 67–80. [https://doi.org/10.36965/OJAKM.2018.6\(1\)67-80](https://doi.org/10.36965/OJAKM.2018.6(1)67-80)
- Greitzer, F. L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A., & Mundie, D. (2014, January). Unintentional insider threat: Contributing factors, observables, and mitigation strategies. *Proceedings from 2014 47th Hawaii International Conference on System Sciences (HICSS)* (pp. 2025–2034). IEEE. <https://doi.org/10.1109/HICSS.2014.256>

- Groth, K. M. (2009). A data-informed model of performance shaping factors for use in human reliability analysis (Doctoral dissertation). Retrieved from <https://drum.lib.umd.edu/bitstream/handle/1903/9975/G?sequence=1>. University of Maryland, College Park.
- Hallbert, B., Boring, R., German, D., Dudenhoefter, D., Whaley, A., Marble, J., ... Lois, E. (2006). Human event repository and analysis (HERA) system, overview. *NUREG/CR-6093, Vol. 1, INL/EXT-06-11528*. Washington, DC: US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.
- Henriques, P. L., Curado, C., Oliveira, M., & Maçada, A. C. G. (2019). Publishing? You can count on knowledge, experience, and expectations. *Quality & Quantity*, 53(3), 1301-1324. <https://doi.org/10.1007/s11135-018-0816-4>
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. <https://doi.org/10.1057/ejis.2009.6>
- Holland, K., Sun, S., Gackle, M., Goldring, C., & Osmar, K. (2019). A qualitative analysis of human error during the DIBH procedure. *Journal of Medical Imaging and Radiation Sciences*, 50(3), 369-377. <https://doi.org/10.1016/j.jmir.2019.06.048>
- Holroyd, C. B., & Coles, M. G. (2002). The neural basis of human error processing: reinforcement learning, dopamine, and the error-related negativity. *Psychological Review*, 109(4), 679–709. <https://doi.org/10.1037//0033-295X.109.4.679>
- Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, 22(2), 242–260. <https://doi.org/10.1108/JFC-09-2013-0055>
- Hua, J., & Bapna, S. (2013). Who can we trust? The economic impact of insider threats. *Journal of Global Information Technology Management*, 16(4), 47–67. <https://doi.org/10.1080/1097198X.2013.10845648>
- Huang, K., & Pearlson, K. (2019, January). For what technology can't fix: Building a model of organizational cybersecurity culture. *In Proceedings of the 52nd Hawaii International Conference on System Sciences*. <http://hdl.handle.net/10125/60074>
- Huang, K. H. (2015, July). Re-examining the consistency in fsQCA. *In Annual Conference of the Global Innovation and Knowledge Academy* (pp. 102-109). [https://doi.org/10.1007/978-3-319-22204-2\\_10](https://doi.org/10.1007/978-3-319-22204-2_10)
- IBM Security (2017). IBM x-force threat intelligence index 2017. Retrieved from <https://www.ibm.com/security/data-breach/threat-intelligence>
- Identity Theft Resource Center (2018). *2017 annual data breach year-end review*. Retrieved from

<https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf>

- Identity Theft Resource Center (2021). Notified. Retrieved from <https://notified.idtheftcenter.org/s/>
- International Information System Security Certification Consortium (2020). Cybersecurity professionals stand up to a pandemic. Retrieved from <https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.as>
- Jensen, B. K., Bailey, J. L., & Baar, S. (2014). Making security policies memorable: The first line of defense. *International Journal of Business, Humanities and Technology*, 4(2), 28–36.
- Kalaian, S., & Kasim, R. M. (2012). Terminating sequential Delphi survey data collection. *Practical Assessment, Research, and Evaluation*, 17(1), 5. <https://doi.org/10.7275/g48q-je05>
- Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, 12(8), 518–555. <https://doi.org/10.17705/1jais.00274>
- Kennedy, S. E. (2016). The pathway to security—mitigating user negligence. *Information & Computer Security*, 24(3), 255–264. <https://doi.org/10.1108/ICS-10-2014-0065>
- Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, 5(26), 10862–10868. <https://doi.org/10.5897/AJBM11.067>
- Klehe, U. C., & Anderson, N. (2007). Working hard and working smart: Motivation and ability during typical and maximum performance. *Journal of Applied Psychology*, 92(4), 978–992. <https://doi.org/10.1037/0021-9010.92.4.978>
- Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38(2), 143–154. <https://doi.org/10.1016/j.apergo.2006.03.010>
- Kraus, S., Ribeiro-Soriano, D., & Schüssler, M. (2017). Fuzzy-set qualitative comparative analysis (fsQCA) in entrepreneurship and innovation research—the rise of a method. *International Entrepreneurship and Management Journal*, 14(1), 15–33. <https://doi.org/10.1007/s11365-017-0461-8>
- Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, April). Protecting people from phishing: The design and evaluation of an embedded training email system. *In Proceedings of the SIGCHI conference on*



*Human factors in computing systems* (pp. 905–914). ACM.  
<https://doi.org/10.1145/1240624.1240760>

- Levine, H. G., & Rossmore, D. (1993, January). Understanding barriers to IT implementation: A case study of rationality, human error, and undiscussable issues. *Proceedings from 1993 Twenty-Sixth Hawaii International Conference on System Sciences*, 4 (pp. 850–859). IEEE.  
<https://doi.org/10.1109/HICSS.1993.284273>
- Levy, Y. (2003). A study of learners' perceived value and satisfaction for implied effectiveness of online learning systems (Doctoral dissertation). Retrieved from <http://digitalcommons.fiu.edu/dissertations/AAI3126765/>. Florida International University.
- Levy, Y., Ramim, M. M., Furnell, S. M., & Clarke, N. L. (2011). Comparing intentions to use university-provided vs vendor-provided multibiometric authentication in online exams. *Campus-Wide Information Systems*, 28(2), 102–113.  
<https://doi.org/10.1108/10650741111117806>
- LexisNexus (2021). LexisNexus. Retrieved from <https://www.lexisnexis.com/en-us/home.page>
- Li, Y., Pan, T., & Zhang, N. (2019). Examining the boundary effect of information systems security behavior under different usage purposes. *IEEE Access*, 7, 156544–156554. <https://doi.org/10.1109/ACCESS.2019.2949079>
- Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, 28(3), 215–228.  
<https://doi.org/10.1016/j.cose.2008.11.003>
- Liu, L., & Guo, C. (2016, July). Research on the improvement of human error in the process of production operation—Taking the fatigue operation in the production as the object of study. In *2016 International Conference on Logistics, Informatics and Service Sciences (LISS)* (pp. 1–6). IEEE.  
<https://doi.org/10.1109/LISS.2016.7854481>
- Luciano, E. M., Mahmood, M. A., & Maçada, A. C. G. (2010). The influence of human factors on vulnerability to information security breaches. In *Proceedings of the Sixteenth Americas Conference on Information Systems* (pp. 12–15).
- Maluf, D. A., Gawdiak, Y., & Bell, D. G. (2005). On space exploration and human error: A paper on reliability and safety. *Proceedings of the 38<sup>th</sup> Hawaii International Conference on System Sciences* (pp. 1–6). IEEE.  
<https://doi.org/10.1109/HICSS.2005.466>

- Marcolin, B. L., Compeau, D. R., Munro, M. C., & Huff, S. L. (2000). Assessing user competence: Conceptualization and measurement. *Information Systems Research*, *11*(1), 37–60. <https://doi.org/10.1287/isre.11.1.37.11782>
- Marx, A., Rihoux, B., & Ragin, C. (2013). The origins, development, and application of qualitative comparative analysis: The first 25 years. *European Political Science Review*, *6*(1), 1–28. <https://doi.org/10.1017/S1755773912000318>
- Maxion, R. A., & Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. *International Journal of Human-Computer Studies*, *63*(1–2), 25–50. <https://doi.org/10.1016/j.ijhcs.2005.04.009>
- Melati, C., Janissek-Muniz, R. and Curado, C. (2021). Decision-making quality of public managers: Contributions from intelligence and knowledge management. *Journal of Contemporary Administration*, *25*(2), 1-17. <https://doi.org/10.1590/1982-7849rac2021190044.en>
- Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, *147*, 424–428. <https://doi.org/10.1016/j.sbspro.2014.07.133>
- Miller, C. O. (1976). The design-induced part of the human error problem in aviation. *Journal of Air Law and Commerce*, *42*, 119–131.
- Miranda, A. T. (2018). Understanding human error in naval aviation mishaps. *Human Factors*, *60*(6), 763-777. <https://doi.org/10.1177/0018720818771904>
- Moody, G. D., Siponen, M., & Pahlila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285–311. <https://doi.org/10.25300/MISQ/2018/13853>
- National Highway Traffic Safety Administration (2018). 2017 fatal motor vehicle crashes: overview. Retrieved from <https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812603>
- Nielen, A., Költer, D., Mütze-Niewöhner, S., & Schlick, C. M. (2011, December). Identification and classification of human error in process model development. *Proceedings from 2011 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)* (pp. 1633–1637). <https://doi.org/10.1109/IEEM.2011.6118193>
- Norman, D. A. (1981). Categorization of action slips. *Psychological Review*, *88*(1), 1–15. <https://doi.org/10.1037//0033-295X.88.1.1>
- Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014). Understanding insider threat: A framework for characterising

- attacks. *Proceedings from 2014 IEEE Security and Privacy Workshops (SPW)*, (pp. 214–228). <https://doi.org/10.1109/SPW.2014.38>
- Oliveira, M., Curado, C., & Henriques, P. L. (2019). Knowledge sharing among scientists: A causal configuration analysis. *Journal of Business Research*, *101*, 777-782. <https://doi.org/10.1016/j.jbusres.2018.12.044>
- Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 156–166). IEEE. <https://doi.org/10.1109/HICSS.2007.206>
- Pappas, I. O., & Woodside, A. G. (2021). Fuzzy-set Qualitative Comparative Analysis (fsQCA): Guidelines for research practice in Information Systems and marketing. *International Journal of Information Management*, *58*, 1-23. <https://doi.org/10.1016/j.ijinfomgt.2021.102310>
- Park, S. (2019). Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics*, *58*, 132-145. <https://doi.org/10.1016/j.irl.2019.03.007>
- Parker, D., Manstead, A. S., Stradling, S. G., Reason, J. T., & Baxter, J. S. (1992). Intention to commit driving violations: An application of the theory of planned behavior. *Journal of Applied Psychology*, *77*(1), 94–101. <https://doi.org/10.1037//0021-9010.77.1.94>
- Paul, C. L., & Dykstra, J. (2017). Understanding operator fatigue, frustration, and cognitive workload in tactical cybersecurity operations. *Journal of Information Warfare*, *16*(2), 1-11.
- Pena, N., & Curado, C. (2007). Uncovering the pathways to e-learning success: A qualitative approach. *Online Journal of Applied Knowledge Management*, *5*(1), 42–56. [https://doi.org/10.36965/OJAKM.2017.5\(1\)42-56](https://doi.org/10.36965/OJAKM.2017.5(1)42-56)
- Pigni, F., Bartosiak, M., Piccoli, G., & Ives, B. (2018). Targeting Target with a 100 million dollar data breach. *Journal of Information Technology Teaching Cases*, *8*(1), 9-23. <https://doi.org/10.1057%2Fs41266-017-0028-0>
- Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, 1-20. <https://doi.org/10.1007/s10111-021-00683-y>
- Ponemon Institute (2017). *2017 cost of data breach study: Global overview*. Retrieved from [https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-15763&S\\_PKG=ov58441](https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-15763&S_PKG=ov58441)

- Ponemon Institute (2021). *Cost of a data breach report 2021*. Retrieved from <https://www.ibm.com/security/data-breach>
- Privacy Rights Clearinghouse (2019). *PRC Data Breach Chronology*. Retrieved from <https://privacyrights.org/sites/default/files/2020-01/PRC%20Data%20Breach%20Chronology%20-%201.13.20.csv>
- Privacy Rights Clearinghouse (2021). *Data breaches*. Retrieved from <https://www.privacyrights.org/data-breaches>
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757–778. <https://doi.org/10.2307/25750704>
- Ragin, C. C. (1987). *The comparative method: Moving beyond qualitative and quantitative strategies*. Oakland, CA: University of California Press.
- Ragin, C. C. (1999). Using qualitative comparative analysis to study causal complexity. *Health Services Research*, 34(5), 1225–1239.
- Ragin, C. C. (2008). *Redesigning social inquiry: Fuzzy sets and beyond*. Chicago, IL: University of Chicago Press.
- Ragin, C. C. (2009). Qualitative comparative analysis using fuzzy sets (fsQCA). In B. Rihoux & C. C. Ragin (Eds.), *Configurational comparative methods: Qualitative comparative analysis (QCA) and related techniques* (pp. 87–121). Thousand Oaks, CA: Sage Publications.
- Ragin, C. C. & Davey, S. (2017). User's guide to fuzzy-set / qualitative comparative analysis. Retrieved from <http://www.socsci.uci.edu/~cragin/fsQCA/download/fsQCAManual.pdf>
- Rahulamathavan, Y., Rajarajan, M., Rana, O. F., Awan, M. S., Burnap, P., & Das, S. K. (2015). Assessing data breach risk in cloud systems. In *2015 IEEE 7th International Conference on Cloud Computing Technology and Science* (pp. 363–370). IEEE. <https://doi.org/10.1109/CloudCom.2015.58>
- Raju, A. D., AbuAlhaol, I., Giagone, R. S., Zhou, Y., & Shengqiang, H. (2021). A survey on cross-architectural IoT malware threat hunting. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2021.3091427>
- Ramim, M. M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology*, 8(4), 24–34. <https://doi.org/10.4018/jcit.2006100103>
- Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, 2(1), 122–136.

- Rasmussen, J. (1983). Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. *IEEE transactions on systems, man, and cybernetics*, 3, 257–266. <https://doi.org/10.1109/TSMC.1983.6313160>
- Reason, J. (1990). *Human error*. Cambridge, UK: Cambridge University Press.
- Reason, J. (1995). Understanding adverse events: Human factors. *Quality in Health Care*, 4(2), 80–89.
- Reason, J. (2000). Human error: Models and management. *BMJ: British Medical Journal*, 320, 768–770. <https://doi.org/10.1136/bmj.320.7237.768>
- Reason, J., Manstead, A., Stradling, S., Baxter, J., & Campbell, K. (1990). Errors and violations on the roads: A real distinction? *Ergonomics*, 33(10-11), 1315–1332. <https://doi.org/10.1080/00140139008925335>
- Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. *Proceedings of the 29th european safety and reliability conference*, 4036-4043. [http://dx.doi.org/10.3850/978-981-11-2724-3\\_0761-cd](http://dx.doi.org/10.3850/978-981-11-2724-3_0761-cd)
- Renaud, K., & Flowerday, S. (2017). Contemplating human-centred security & privacy research: Suggesting future directions. *Journal of Information Security and Applications*, 34, 76-81. <http://dx.doi.org/10.1016/j.jisa.2017.05.006>
- Rhee H., Kim C., & Ryu Y. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28, 816–826. <https://doi.org/10.1016/j.cose.2009.05.008>
- Rihoux, B. (2006). Qualitative comparative analysis (QCA) and related systematic comparative methods: Recent advances and remaining challenges for social science research. *International Sociology*, 21(5), 679–706. <https://doi.org/10.1177%2F0268580906067836>
- Rihoux, B., & De Meur, G. (2009). Crisp-set qualitative comparative analysis (csQCA). In B. Rihoux & C. C. Ragin (Eds.), *Configurational comparative methods: Qualitative comparative analysis (QCA) and related techniques* (pp. 33–68). Thousand Oaks, CA: Sage Publications.
- Rihoux, B., & Ragin, C. C. (Eds.) (2009). *Configurational comparative methods: Qualitative comparative analysis (QCA) and related techniques*. Thousand Oaks, CA: Sage Publications.
- Rihoux, B., Álamos-Concha, P., Bol, D., Marx, A., & Rezsöhazy, I. (2013). From niche to mainstream method? A comprehensive mapping of QCA applications in journal articles from 1984 to 2011. *Political Research Quarterly*, 66(1), 175–184.

- Rizzo, A., Parlangeli, O., Marchigiani, E., & Bagnara, S. (1996). The management of human errors in user-centered design. *ACM SIGCHI Bulletin*, 28(3), 114–118. <https://doi.org/10.1145/231132.231155>
- Rosati, P., & Lynn, T. (2021). A dataset for accounting, finance and economics research on US data breaches. *Data in Brief*, 35, 1-6. <https://doi.org/10.1016/j.dib.2021.106924>
- Rouse, W. B. (1985). Optimal allocation of system development resources to reduce and/or tolerate human error. *IEEE Transactions on Systems, Man, and Cybernetics*, 5, 620–630.
- Saarelainen, K., & Jäntti, M. (2015, November). Quality and human errors in IT service infrastructures: Human error based root causes of incidents and their categorization. In *proceeding from 2015 11th International Conference on Innovations in Information Technology (IIT)* (pp. 207–212). <https://doi.org/10.1109/INNOVATIONS.2015.7381541>
- Sabherwal, R., Sabherwal, S., Havakhor, T., & Steelman, Z. (2019). How does strategic alignment affect firm performance? The roles of information technology investment and environmental uncertainty. *MIS Quarterly*, 43(2), 453-474. <https://doi.org/10.25300/MISQ/2019/13626>
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70–82. <https://doi.org/10.1016/j.cose.2015.10.006>
- Sands, R. G., & Roer-Strier, D. (2006). Using data triangulation of mother and daughter interviews to enhance research about families. *Qualitative Social Work*, 5(2), 237–260. <https://doi.org/10.1177/1473325006064260>
- Santos, R. F., Oliveira, M. and Curado, C. (2021). The effects of the relational dimension of social capital on tacit and explicit knowledge sharing: A mixed-methods approach. *VINE Journal of Information and Knowledge Management Systems*, Vol. ahead-of-print No. ahead-of-print <https://doi.org/10.1108/VJIKMS-05-2020-0094>
- Schein, E. H. (2009). *The corporate culture survival guide*. San Francisco: John Wiley & Sons.
- Schneider, C. Q., & Wagemann, C. (2010). Standards of good practice in qualitative comparative analysis (QCA) and fuzzy-sets. *Comparative Sociology*, 9(3), 1–22. <https://doi.org/10.1163/156913210X12493538729793>
- Schneider, C. Q., & Rohlfing, I. (2016). Case studies nested in fuzzy-set QCA on sufficiency: Formalizing case selection and causal inference. *Sociological*

- Methods & Research*, 45(3), 526-568.  
<https://doi.org/10.1177%2F0049124114532446>
- Schultz, E. (2005). The human factor in security. *Computers & Security*, 6(24), 425–426.  
<https://doi.org/10.1016/j.cose.2005.07.002>
- Senders, J. W., & Moray, N. P. (1991). *Human error: Cause, prediction, and reduction*. Hillsdale, NJ: L. Erlbaum Associates.
- Shappell, S., Detwiler, C., Holcomb, K., Hackworth, C., Boquet, A., & Wiegmann, D. A. (2007). Human error and commercial aviation accidents: An analysis using the human factors analysis and classification system. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 49(2), 227–242.  
<https://doi.org/10.1518/001872007X312469>
- Shwartz, L., Rosu, D., Loewenstern, D., Bucu, M. J., Guo, S., Lavrado, R., Gupta, M., De, V., Madduri, V., & Singh, J. K. (2010, December). Quality of IT service delivery—analysis and framework for human error prevention. *Proceedings from 2010 IEEE International Conference on Service-Oriented Computing and Applications* (pp. 1–8). <https://doi.org/10.1109/SOCA.2010.5707161>
- Singh, S. (2018, March). Critical reasons for crashes investigated in the National Motor Vehicle Crash Causation Survey. (Traffic Safety Facts Crash•Stats. Report No. DOT HS 812 506). Washington, DC: National Highway Traffic Safety Administration. Retrieved from <https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115>
- Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31–41.  
<https://doi.org/10.1108/09685220010371394>
- Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 487–502. <https://doi.org/10.2307/25750688>
- Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, 24(2), 124–133.  
<https://doi.org/10.1016/j.cose.2004.07.001>
- Stanton, N. (2009). Human-error identification in human-computer interaction. In Sears, A. & Jacko, J. A. (Eds.). *The Human-Computer Interaction Fundamentals* (pp. 123–133). Boca Raton, FL: CRC Press.
- Stephoe & Johnson LLP (2018). *Comparison of US state and federal security breach notification laws*. Retrieved from <https://www.stephoe.com/images/content/1/7/v2/175438/Comparison-of-Security-Breach-Notification-Laws-Updated-6-1-201.pdf>

- Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security*, 25(5), 494–534. <https://doi.org/10.1108/ICS-07-2016-0054>
- Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255–276. <https://doi.org/10.1287/isre.1.3.255>
- Swain, A.D., & Guttman, H.E. (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications: Final report. *NREG/CR-1278*. Washington, DC: US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.
- Taylor, R. G., & Robinson, S. L. (2015). An information system security breach at First Freedom Credit Union 1: What goes in must come out. *Journal of the International Academy for Case Studies*, 21(1), 131.
- Thiem, A. (2017). Conducting configurational comparative research with qualitative comparative analysis: A hands-on tutorial for applied evaluation scholars and practitioners. *American Journal of Evaluation*, 38(3), 420–433. <https://doi.org/10.1177/1098214016673902>
- Thiem, A., & Duşa, A. (2013). QCA: A package for qualitative comparative analysis. *The R Journal*, 5(1), 87–97. <https://doi.org/10.32614/RJ-2013-009>
- Thomann, E., & Maggetti, M. (2017). Designing research with qualitative comparative analysis (QCA): Approaches, challenges, and tools. *Sociological Methods & Research*, 49(2), 1–31. <https://doi.org/10.1177/0049124117729700>
- Thomson, M. E., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, 6(4), 167–173. <https://doi.org/10.1108/09685229810227649>
- Thomson, K. L., & von Solms, R. (2005). Information security obedience: A definition. *Computers & Security*, 24(1), 69–75. <https://doi.org/10.1016/j.cose.2004.10.005>
- Ung, S. T., & Shen, W. M. (2011). A novel human error probability assessment using fuzzy modeling. *Risk Analysis: An International Journal*, 31(5), 745–757. <https://doi.org/10.1111/j.1539-6924.2010.01536.x>
- US Congress (2014). Federal information security modernization act of 2014. 113th Congress (2013–2015). Retrieved from <https://www.congress.gov/bill/113th-congress/senate-bill/2521/text>
- US Department of Health and Human Services Office for Civil Rights (2020). *Breach portal: Notice to the secretary of HHS breach of unsecure protected health information*. Retrieved from [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)



- Vance, A., & Siponen, M. T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing*, 24(1), 21–41. <https://doi.org/10.4018/joeuc.2012010102>
- Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management*, 57(4), 103212. <https://doi.org/10.1016/j.im.2019.103212>
- Verizon (2017). *2017 data breach investigations report: 10<sup>th</sup> edition*. Retrieved from <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>
- Verizon (2021). *2021 data breach investigations report*. Retrieved from <https://www.verizon.com/business/resources/reports/dbir/>
- Von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security*, 23(4), 275–279. <https://doi.org/10.1016/j.cose.2004.01.013>
- Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23(3), 191–198. <https://doi.org/10.1016/j.cose.2004.01.012>
- Whaley, A.M., Xing, J., Boring, R.L., Hendrickson, S.M., Joe, J.C., Le Blanc, K.L., & Morrow, S.L. (2016). Cognitive basis for human reliability analysis. *NUREG-2114*. Washington, DC: US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.
- Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security*, 88, 1-8. <https://doi.org/10.1016/j.cose.2019.101640>
- Wood, C. C., & Banks, W. W. (1993). Human error: An overlooked but significant information security problem. *Computers & Security*, 12(1), 51–60. [https://doi.org/10.1016/0167-4048\(93\)90012-T](https://doi.org/10.1016/0167-4048(93)90012-T)
- Woodside, A. G., & Zhang, M. (2013). Cultural diversity and marketing transactions: Are market integration, large community size, and world religions necessary for fairness in ephemeral exchanges? *Psychology & Marketing*, 30(3), 263-276. <https://doi.org/10.1002/mar.20603>
- Xing, J., Parry, G., Presley, M., Forester, J., Hendrickson, S., & Dang, V. (2017). An integrated human event analysis system (IDHEAS) for nuclear power plant internal events at-power application. *NUREG-2199, Vol. 1*. Washington, DC: US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.
- Yayla, A. A. (2011, October). Controlling insider threats with information security policies. In *European Conference on Information Systems (ECIS)* (pp. 1–13). Retrieved from <http://aisel.aisnet.org/ecis2011/242>

- Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, 8(3), 338–353.
- Zamosky, L. (2014). Avoid the breach: Put data security measures in place. *Physician Executive*, 40(4), 82–84.
- Zimmermann, V., & Renaud, K. (2019). Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187. <https://doi.org/10.1016/j.ijhcs.2019.05.005>