

2023

## **An Empirical Assessment of the Use of Password Workarounds and the Cybersecurity Risk of Data Breaches**

Michael Joseph Rooney

Follow this and additional works at: [https://nsuworks.nova.edu/gscis\\_etd](https://nsuworks.nova.edu/gscis_etd)

 Part of the [Databases and Information Systems Commons](#), and the [Information Security Commons](#)

All rights reserved. This publication is intended for use solely by faculty, students, and staff of Nova Southeastern University. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, now known or later developed, including but not limited to photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the author or the publisher.

---

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](mailto:nsuworks@nova.edu).

An Empirical Assessment of the Use of Password Workarounds and the  
Cybersecurity Risk of Data Breaches

by

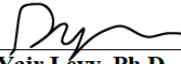
Michael Joseph Rooney

A dissertation report submitted in partial fulfillment of the requirements  
for the degree of Doctor of Philosophy  
in  
Cybersecurity Management

College of Computing and Engineering  
Nova Southeastern University

2023


**We hereby certify that this dissertation, submitted by Michael Rooney 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

12/8/23  
Date

  
\_\_\_\_\_  
Wei Li, Ph.D.  
Dissertation Committee Member

12/8/23  
Date

  
\_\_\_\_\_  
Ajoy Kumar, Ph.D.  
Dissertation Committee Member

12/8/23  
Date

Approved:

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

12/8/23  
Date

College of Computing and Engineering  
Nova Southeastern University

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

An Empirical Assessment of the Use of Password Workarounds and the  
Cybersecurity Risk of Data Breaches

By  
Michael Joseph Rooney  
December 2023

Passwords have been used for a long time to grant controlled access to classified spaces, electronics, networks, and more. However, the dramatic increase in user accounts over the past few decades has exposed the realization that technological measures alone cannot ensure a high level of IS security; this leaves the end-users holding a critical role in protecting their organization and personal information. The increased use of IS as a working tool for employees increases the number of accounts and passwords required. Despite being more aware of password entropy, users still often participate in deviant password behaviors, known as ‘password workarounds’ or ‘shadow security.’ These deviant password behaviors can put individuals and organizations at risk, resulting in data privacy. This study, engaging 303 IS users and 27 Subject Matter Experts (SMEs), focused on designing, developing, and empirically validating Password Workaround Cybersecurity Risk Taxonomy (PaWoCyRiT)—a model supported on perceived cybersecurity risks from Password Workarounds (PWWA) techniques and their usage frequency. A panel of SMEs validated the PWWA list from existing literature with recommended adjustments. Additionally, the perception level of the cybersecurity risks of each technique was measured from the 27 SMEs and 303 IS users. They also provided their self-reported and reported on coworkers' engagement frequencies related to the PWWA list. Noteworthy, significant differences were found between SMEs and IS users in their aggregated perceptions of cybersecurity risks of the PWWAs, with IS users perceiving higher risks. Engagement patterns varied between the groups, as well as factors like years of IS experience, gender, and job level had significant differences among groups. The PaWoCyRiT was developed to provide insights into password-related risks and behaviors.

## Acknowledgments

First and foremost, I express my profound gratitude to God for the strength, wisdom, and serenity bestowed upon me during this research journey.

To my late father, John, who always believed in me and instilled in me the value of hard work and perseverance, I dedicate this work to your loving memory. Your influence continues to guide me in all my endeavors.

I extend my deepest gratitude to my advisor, Dr. Yair Levy, who challenged and motivated me throughout this extremely rewarding journey from the beginning of the program and to your invaluable guidance, patience, and expertise that greatly contributed to my research.

Thank you to the best chair, Dr. Wei Li and Dr. Ajoy Kumar, for their invaluable feedback and patience, which has been instrumental in shaping this dissertation and my academic journey.

My heartfelt appreciation goes to my mother, Cindy, my stepfather, Lane, and my brother, Ric. Your unwavering support, love, and belief in me have been my greatest strength. Thank you for being my constant source of motivation and for standing by me through all the highs and lows.

A special thank you to my academic support team and friends, Ariel and Maria, as we share our journey to this amazing milestone and continue to support each other and assist with endless encouragement, thoughtful insights, and countless moments of support.

I am deeply grateful to my friends Joe, Phae, and Alex, whose friendship has been an invaluable and cherished part of my journey. Thank you for always being there and for your endless support.

I want to thank the Promoting Postbaccalaureate Opportunities for Hispanic Americans (PPOHA) for providing the financial support that made my studies possible.

Lastly, I want to thank all those who have directly or indirectly contributed to my academic journey. Your support has been significant in completing this dissertation, whether big or small.

Thank you all for being a part of this journey.

## Table of Contents

**Abstract iii**

**List of Tables vii**

**List of Figures ix**

### **Chapter**

#### **1. Introduction 1**

Background 1  
Problem Statement 2  
Research Goals 7  
Research Questions 10  
Relevance and Significance 11  
Barriers and Issues 13  
Assumptions, Limitations, and Delimitations 14  
Definition of Terms 15  
Summary 17

#### **2. Review of the Literature 19**

Introduction 19  
Data Breaches 20  
    Impact 21  
    Current trends 26  
    Human Factor in Data Breach 27  
Cybersecurity Risk 32  
    Risk 34  
    Risk Management 36  
    Cybersecurity Risk Management 38  
Authentication 41  
    Overview of Authentication Methods 42  
    Passwords 44  
    Common Password Attacks 49  
    Password Workarounds 52  
Summary of What is Known and Unknown 57

#### **3. Methodology 59**

Overview of Research Design 59  
Phase One 60  
Phase Two 62  
Phase Three 62  
Sample 62  
Survey Tool 63  
Resources 65  
Summary 65

#### **4. Results 67**

Overview 67

Data Analysis 67

Results Phase I-Subject Matter Expert (SME) Panel Round 1 67

Phase I-Subject Matter Expert (SME) Panel Round 2 70

SMEs Results from Delphi 72

Phase 2 – Pilot Test 78

Phase 3 – Main Data Collection 81

Main Data Collection- Research Questions 82

Summary 100

#### **5. Conclusions, Discussions, Implications, Recommendations, and Summary 102**

Conclusions 102

Discussions 103

Implications 105

Recommendations 107

Summary 107

#### **Appendices**

**A.** Institutional Review Board Approval Letter 111

**B.** Subject Matter Expert Recruitment Letter 113

**C.** Information Users Recruitment Letter 114

**D.** Subject Matter Expert Survey- Round 1 115

**E.** Subject Matter Expert Survey- Round 2 123

**F.** Information Systems Users Survey 132

#### **References 138**

## List of Tables

### Tables

1. Summary of Data Breach Impact From Literature 24
2. Summary of Human Behavior From Literature 30
3. Summary of Risk From Literature 35
4. Summary of Cybersecurity Risk Management From Literature 40
5. Summary of Passwords From Literature 47
6. Summary of PWWA From Literature 55
7. PWWA From Literature 60
8. Delphi Round 2 Adjusted PWWAs List 69
9. Descriptive SMEs Criteria (N=27) 71
10. PWWAs Validation Percentage of Agreement (N=27) 73
11. SMEs Identified Measure of Perceived Risk of Data Breach on Validated PWWAs (N=27) 75
12. Finalized SME Validated Adjusted PWWA List 80
13. ANOVA Differences in Perceived Cybersecurity Risk of Data Breaches (N=330) 84
14. ANOVA Analysis of SMEs and IS Users Self-reported PWWA Usage Frequency Differences (N=330) 89
15. ANOVA Analysis of Co-worker PWWA Usage Reported Frequency Differences (N=330) 90
16. Descriptive Statistics of the IS Users (N=303) 90
17. Descriptive Statistics of the SMEs (N=27) 92



18. ANCOVA Results for SMEs Perceived Cybersecurity Risk Based on  
Demographics (N=27) 93

19. ANCOVA Results for IS Users Perceived Cybersecurity Risk Based on  
Demographics (N=303) 94

## List of Figures

### Figures

1. The Proposed Password Workaround Cybersecurity Risk Taxonomy (PaWoCyRiT) 10
2. An Overview of the Research Design Process to Develop and Validate the PaWoCyRiT 59
3. SMES Reported Frequency of Co-worker's Engagement in PWWAs Ranking (N=27) 78
4. IS Users and SMEs Aggregated Perceptions of PWWAs Will Lead to Data Breach (N=330) 83
5. SMEs and IS Users Self-reported Frequency Use of PWWAs (N=330) 86
6. SMEs and IS Users Reported Frequency of Co-worker Engagement in PWWAs (N=330) 88
7. PaWoCyRiT IS Users' Perceived Cybersecurity Risk and Reported Co-workers' Frequency 96
8. PaWoCyRiT IS Users Perceived Cybersecurity Risk and Self-reported Frequency 97
9. PaWoCyRiT SMEs Perceived Cybersecurity Risk and Reported Co-workers Frequency 98
10. PaWoCyRiT SMEs Perceived Cybersecurity Risk and Self-reported Frequency 99
11. PaWoCyRiT 100

## Chapter 1

### Introduction

#### **Background**

Cybersecurity involves a broad range of techniques, from physical to technical, and authentication provides a layer of protection for Information Systems (IS) against data breaches (Siponen et al., 2020). Cybersecurity involves various techniques, including cyber-physical, managerial, and technical, while authentication protects Information Systems (IS) against data breaches (Liginlal et al., 2009). Authentication protects IS against unauthorized access utilizing various defense techniques, with the most popular and frequently used technique being alphanumeric passwords (Zimmermann & Gerber, 2020). Passwords have been used for a long time to grant controlled access to classified spaces, electronics, IS, and various other resources (Chanda, 2016). However, the dramatic increase in IS accounts over the past few decades has exposed the realization that technological measures alone cannot wholly secure IS, leaving the end users holding a critical role (Dang-Pham et al., 2017). The increased use of IS as a working tool for employees increases the number of accounts and passwords required; despite users being more aware of password security, users still often participate in deviant password behaviors (Woods & Siponen, 2019). These deviant password behaviors can put individuals and organizations at risk, resulting in data privacy issues, data loss, and, ultimately, a data breach incident (Wibisono et al., 2020). Deviant password behaviors, or insecure password practices, occur when users deliberately circumvent organizational password policies to make passwords more memorable and manageable (Woods & Siponen, 2019). These deviant password behaviors the users exhibit can be known as Password Workarounds (PWWA).

The European Union Agency for Cybersecurity (ENISA; 2020) identified that data breaches have increased by 54% from 2018 to mid-2019, with over 3800 breaches reported, exposing 4.1 billion records. About 64% of those data breaches were password data exposure, which increased 25% from previous years (ENISA, 2020). Joseph (2018) defined a data breach as disclosing an organization's protected confidential data through unauthorized access. According to the Ponemon Institute (2020), the global average cost of data breaches was \$3.86 million in 2019, and malicious attacks were responsible for 52% of those data breaches, with compromised credentials making up 19% of the malicious attacks. Data breaches are pivotal in cybersecurity research, but independent empirical studies focusing on this subject are limited. Existing research predominantly revolves around data breaches after they have occurred, which introduces various biases into the analyses (Goode et al., 2017). The scarcity of research studies focusing on individual aspects of data breaches, such as the examination of PWWAs and their potential cybersecurity risks, emphasizes the significance of contributing to the collective understanding of this subject matter. The goal of this research is to empirically assess if there is a significant mean difference between the *perceived cybersecurity risk of data breaches* resulting from PWWAs and the frequency of PWWA usage, using inputs from Subject Matter Experts (SMEs) and employees. This study aimed to develop a taxonomy to identify the risks associated with each PWWA technique based on the constructs of users' perceived cybersecurity risk of data breaches resulting from PWWA techniques and the frequency of PWWA techniques usage.

### **Problem Statement**

The research problem that this study addressed is the use of PWWA techniques by employees in organizations that may pose a significant cybersecurity risk of data

breaches and financial damages (Wibisono et al., 2020). Davis et al. (2018) defined cybersecurity by using the Joint Task Force on Cybersecurity Education (2017) definition:

Computing-based discipline involving technology, people, information, and processes to enable assured operations. 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 in the context of adversaries. (p. 16)

In their work, Davis et al. (2018) define cybersecurity as a discipline that spans technology, law, ethics, and risk management, which is crucial for addressing challenges like data breaches. Information security risk is defined by Kissel (2013) as:

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring. (p. 161)

A workaround is when employees use deviated actions from those enforced by their organizational policies and procedures (Patterson, 2018). Unfortunately, some employees perceive their organizational password policies and procedures as barriers and, therefore, engage in PWWAs to achieve a faster result or make a task easier (Patterson, 2018).

These actions of creating PWWAs fall into a category of security behavior coined as "shadow security" or "shadow Information Technology," where employees feel they cannot comply or are unacquainted with organizational policies and procedures put in

place to protect information assets, resulting in the use of non-compliant alternative mechanisms (Kirlappos et al., 2015; Sillic, 2019).

Passwords are used as an access control mechanism providing user authentication, which is usually the first line of defense, to access IS resources and services (Wang et al., 2017). Previous research has suggested the following techniques are considered insecure password techniques: reusing passwords, creating weak passwords, writing passwords down, and sharing passwords (Chanda, 2016; Chowdhury et al., 2020; Dang-Pham et al., 2017; Kaleta et al., 2019; Kirlappos et al., 2015; Woods & Siponen, 2019). Ives et al. (2004) described the severity of these techniques, such as the reuse of passwords, suggesting they can result in the domino effect. One example is when a user has multiple password-protected accounts, including one for the organization they work for, and they reuse the same weak password for all those accounts. In that case, all their accounts will be at risk if just one of those account passwords is compromised (Ives et al., 2004). These poor practices have had detrimental consequences, not only in the past but also recently, as they have been highlighted in the news with data breaches compromising user accounts: "Adobe (150 million), Evernote (50 million), Anthem (40 million), Rockyou (32 million), Tianya (30 million), Dodonew (16 million), 000webhost (15 million), Gmail (4.9 million), and Phpbb (255 K)" (Wang & Wang, 2018, p. 708). Although there are several disadvantages of using passwords, and much research has gone into finding new alternatives, it has been shown that the "password scored highest in terms of preference, usability, and intention to use, and lowest in terms of perceived effort and expected problems" (Zimmermann & Gerber, 2020, p. 6).

The basic types of authentication techniques include token-based, "something you have," biometric-based, "something you are," and knowledge-based, "something you know" (Bhanushali et al., 2015). The increasing requirement for individuals to have various accounts for work and personal matters results in more passwords they need to manage, leading to increased cybersecurity risks (Woods & Siponen, 2018). According to AlFayyadh et al. (2012), previous research suggested that individuals mentally classify accounts based on their perceived importance. They would practice PWWAs, such as reusing passwords, for accounts perceived as low importance. As defined by Shay et al. (2010), password entropy refers to the difficulty in predicting a variable's value, or in the context of password security, it pertains to the complexity of cracking a password. The greater difficulty of cracking a password depends on the size of the password's entropy values, which would determine the number of guesses and time it would take to identify the set password (Shen et al., 2016). Many tools and techniques exist for stealing or cracking passwords, such as brute-force attacks, dictionary attacks, spyware attacks, shoulder surfing, and other social engineering techniques (Bhanushali et al., 2015). Most organizations will implement a password policy to enforce password complexity for strength to prevent individuals from becoming victims of these attacks. However, users will use PWWAs to remember these passwords, such as creating weak passwords or passphrases to meet the minimum requirements (Wang et al., 2017). Research has shown that when password entropy is too complicated, employees may forget their set passwords, which costs time and resources to reset them (Mujeye et al., 2016).

The National Institute of Standards and Technology (NIST) has made some significant updates to its password policy guidelines in their Special Publication (SP; NIST SP 800-

63-B), which marks the second update within three years (Grassi et al., 2017). The differences eased enforcement of password requirements by recommending the following changes: removal of the password expiration, removal of the requirement for special characters, allowing all characters to be used (including spaces), allowing the copying and pasting of passwords, and increasing the allowed number of characters. According to Topper (2018), NIST initially made these changes in 2017 based on the suggestions that traditional password security encouraged the use of deviant security behavior, such as the identified PWWAs. The use of PWWAs has been heavily researched (Lin et al., 2013; Safa et al., 2015; Siponen et al., 2020; Stanton et al., 2005; Sun et al., 2012; Whitty et al., 2015; Woods & Siponen, 2018; Woods & Siponen, 2019) in different capacities to identify solutions on how to prevent employees from using such techniques. Despite this past work on password security, recent research by Brason (2020) highlighted that 42% of IT and Security Managers identified user password compromise as the leading cause of data breaches. Memorization of passwords is a well-researched topic in password security due to most research identifying IS users as frequently using weak passwords that are easy to remember and reusing passwords across multiple accounts (Sun et al., 2012). According to the 2020 Verizon Data Breach Investigations Report, 45% of breaches featured hacking, and 80% of those hacking breaches utilized lost/stolen or brute-forced credentials. A brute-force attack uses every combination of letters and numbers to crack the original password; the weaker the combination, the faster the password will be cracked (Chanda, 2016). Stolen credentials, generally for sale on the black market, are a cybersecurity risk for organizations whose employees reuse passwords; this warrants some organizations to monitor these black-market sites and send



notifications to users who may be victims (Golla et al., 2018). Research by Thomas et al. (2017) has identified "1.9 billion usernames and passwords exposed via data breaches and traded on blackmarket forums" (p. 1433). Users were unaware of how frequently these poor password techniques were used by others (Ur et al., 2016). Thus, empirical research is needed to determine employee's perceptions of the likelihood and impact of data breaches (i.e., risk) resulting from the frequency use of PWWA.

### **Research Goals**

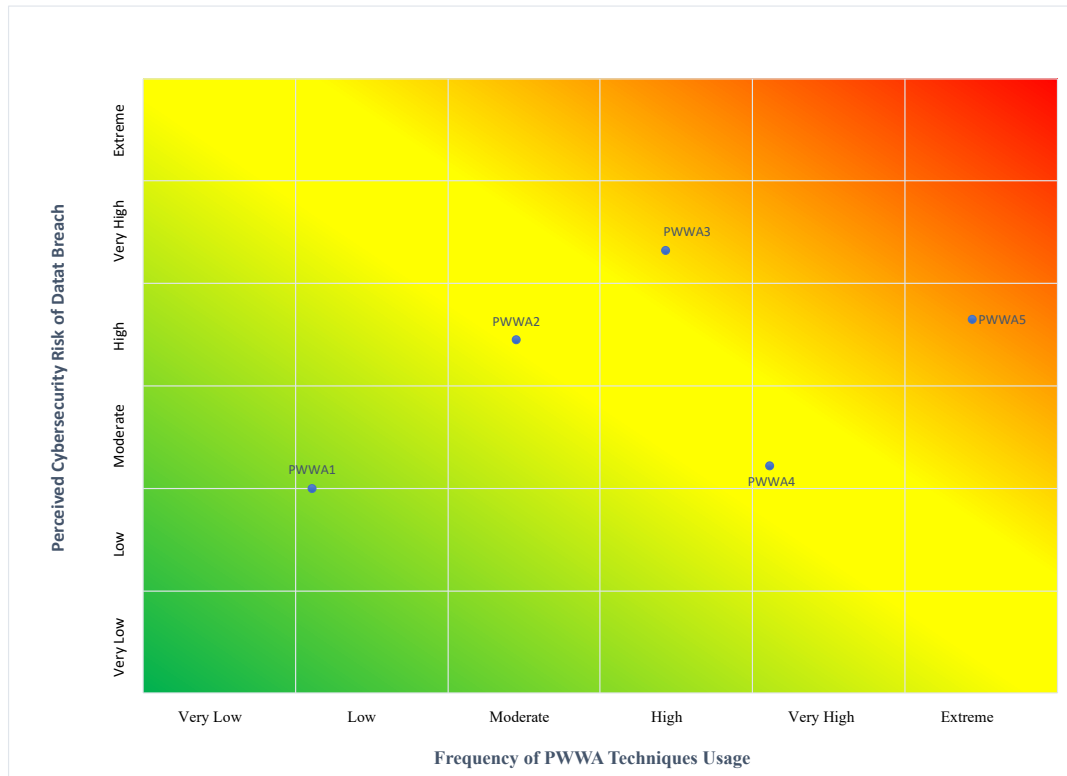
The main goal of this research study aimed to design, develop, and empirically validate the Password Workaround Cybersecurity Risk Taxonomy (PaWoCyRiT), using the constructs of users' perceived cybersecurity risk of data breaches resulting from PWWA techniques and frequency of PWWA techniques usage. This study included employees who used IS daily for work and personal use as the unit of analysis. Additionally, this study establishes various PWWA perceptions, with the level of perceived risk for a data breach being dependent upon the specific PWWA technique employed. Kirlappos et al. (2015) demonstrated the need for this work, which pointed out that non-compliance to security policies was not just a binary decision, comply or not, but introduced a third option: shadow security. Kirlappos et al. (2015) conducted interviews and analyzed the results to understand how employees utilized shadow security practices in response to what the employees felt were unworkable security policies. Their work identified self-made security measures created by employees who felt the organization's existing security policies impeded how they could accomplish their work. Kirlappos et al. (2015) suggested that organizations should recognize shadow security by receiving employee feedback to align security with employees' work requirements better.

To accomplish the main goal, this study addressed 10 specific goals. The first goal of this research was to validate, using SMEs, an initial list of PWWA techniques identified in literature. The outcome from the first goal was used to determine the SMEs' validated list of the top PWWA techniques first identified in literature; this list was used to associate a level of perceived cybersecurity risk for the second goal. The second goal of this study was to develop and validate, using the same SMEs from the first goal, a measure for the perceived cybersecurity risk of data breaches resulting from each validated PWWA technique. The application of SMEs as experts to validate the PWWA techniques and perceived cybersecurity risk of data breaches resulting from each PWWA technique used a method developed by Dalkey and Helmer (1963) known as the Delphi method. The third goal of this study was to identify the most frequently reported used PWWA techniques indicated by SMEs about employees, using a survey tool and a 7-point Likert scale for different types of PWWAs witnessed. The fourth goal of this study was to identify, using employees, aggregated perceived cybersecurity risk of data breaches resulting from each validated PWWA technique. The fifth goal of this study was to identify any statistically significant mean differences in employees' aggregated perceived level of cybersecurity risk of data breaches as a result of each of the validated PWWA techniques compared to those indicated by SMEs. This goal was used to compare results from the SMEs to those from the employees. The sixth goal of this study was to identify the most frequently self-reported used PWWA techniques indicated by SMEs and employees. The seventh goal of this study was to identify the most frequently reported used PWWA techniques indicated by employees about their co-workers. For comparison with SMEs reporting of employee's actions from the third goal, employees

were asked to report their co-workers' use of PWWA techniques. The eighth goal of this study was to determine if there were any statistically mean differences in SMEs' and employees' reports on themselves and co-workers' use of PWWA techniques. Thus, the outcome of this goal was expected to provide data to be examined and compared with the perceived cybersecurity risk of data breaches resulting from the PWWA techniques of SMEs' and employees' responses. The ninth goal of this study was to identify statistically significant differences in the perceived level of cybersecurity risk of data breaches as a result of each of the validated PWWA techniques based on (a) age, (b) gender, (c) years of computer experience, (d) years of cyber awareness training, and (e) job level. The final and 10th goal of this research was to position the PWWA techniques on the PaWoCyRiT based on the aggregated scores of perceived cybersecurity risk of data breaches resulting from each PWWA technique and the frequency of PWWA techniques usage reported by SMEs and employees about themselves and their co-workers. This goal's outcome was to develop the PaWoCyRiT that positions PWWA techniques and their perceived cybersecurity risk of data breaches based on input from the SMEs and employees about themselves and their co-workers. The proposed PaWoCyRiT is shown in Figure 1, with examples of how the techniques were placed based on the results of the data analysis from the received responses from SMEs and employees. The techniques in the PaWoCyRiT were identified through the literature review and validated by SMEs.

**Figure 1**

*The Proposed Password Workaround Cybersecurity Risk Taxonomy (PaWoCyRiT)*



### Research Questions

The main research question that this study addressed was: What are the differences among SMEs and users regarding the cybersecurity risk of data breaches as a result of the frequency of PWWA techniques usage reported by employees about themselves and their co-workers? The 10 research questions that this study addressed are:

RQ1. What are the SMEs' validated PWWA techniques that were identified in literature?

RQ2. What are the SMEs' identified measures for perceived cybersecurity risk of data breaches resulting from each validated PWWA technique?

RQ3. What are the SMEs' reported most frequently observed PWWA techniques co-workers use?

RQ4. What are the employees' aggregated perceived cybersecurity risks of data breaches as a result of each validated PWWA technique?

RQ5. Are there any statistically significant mean differences in employees' aggregated perceived level of cybersecurity risk of data breaches as a result of each validated PWWA technique compared to those indicated by SMEs?

RQ6. What are the most frequently self-reported used PWWA techniques indicated by SMEs and employees' engagement in PWWA techniques?

RQ7. What are the most frequently reported PWWA techniques indicated by employees' reported frequency of co-workers' engagement in PWWA techniques?

RQ8. Are there any statistically significant mean differences between SMEs' and employees' self-reported and reported frequency of co-workers' engagement in PWWA?

RQ9. Do statistically significant differences exist in the perceived level of cybersecurity risk of data breaches as a result of each of the validated PWWA techniques based on (a) age, (b) gender, (c) years of computer experience, (d) years of cyber awareness training, and (e) job level?

RQ10. How are the PWWA techniques positioned on the proposed Password Workaround Cybersecurity Risk Taxonomy (PaWoCyRiT) using the aggregated score of perceived cybersecurity risk of data breaches resulting from the PWWA techniques VS. frequency of PWWA techniques usage?

### **Relevance and Significance**

Data breaches in the United States continue to be the highest average cost out of all countries, totaling \$8.64 million for the year, and compromised credentials were the most expensive initial cause of malicious breaches (Ponemon Institute, 2020). This research

study is relevant because textual passwords remain the primary authentication technique for access control for users' professional and personal accounts (Han et al., 2021). Research in data breaches is mainly conducted during or after an incident but rarely before an occurrence, and data breaches are central to cybersecurity research (Goode et al., 2017). The use of PWWAs increases as users attempt ways to ease password requirements; this is a consequence of acquiring more accounts with password authentication requirements, leading to increased cybersecurity risks (Woods & Siponen, 2018). The increased use of PWWAs has been recognized as shown by the updates made by NIST SP 800-63-B, in which, along with the newly mentioned approaches to password enforcement, it was recommended to compare user passwords against a compiled list of weak and identified compromised passwords (Topper, 2018).

While extensive research advocates for alternative authentication methods to mitigate the cybersecurity risks associated with PWWAs, transitioning away from alphanumeric passwords remains impractical, given their inherent usability, deployability, and security advantages (Guo et al., 2020). Therefore, the significance of this research is to provide a taxonomy showing the perceived cybersecurity risk of data breaches resulting from each validated PWWA technique and the frequency of the use of the validated PWWA techniques. Furthermore, the developed taxonomy may assist organizations in determining user groups that could present heightened risks. It can be employed as an effective tool to categorize employees into specific subgroups, guiding decisions about who requires training or further training. It can also highlight the PWWAs that organizations should prioritize, drawing insights from the research on "the frequency of use of the validated PWWA techniques."

## **Barriers and Issues**

This research study had several potential barriers and issues that needed to be addressed. The first barrier was obtaining an Institutional Review Board (IRB) approval due to conducting a survey involving human participants. Human participation was a vital part of this research study; thus, IRB approval was critical to conducting this study. The second barrier was developing a valid survey instrument that would be used to measure the perceived cybersecurity risk of data breaches based on the frequency of use of PWWAs. The acceptable development of a survey tool and utilization of the instrument is vital to acquiring valid results (Ellis & Levy, 2010). This research study used SMEs to establish internal validity. The Delphi method has been researched and suggested to be a valid instrument for predicting and supplementing decision-making (Landeta, 2006; Lund, 2019). In ancient Greece, experts known as oracles were frequently consulted for their advice and opinions when crucial decisions were needed; this practice is still used in modern research methods (Hohmann et al., 2017). The Delphi method is a technique that is employed to obtain the consensus of SMEs who are seen as specialists in their fields (Dalkey & Helmer, 1963). The first phase of this research relied on SMEs to provide input to validate a list of PWWAs from literature and align their perceived cybersecurity risk of data breaches for each validated PWWA.

The third barrier was verifying the SMEs' experience, as they must be chosen appropriately. The selection of SMEs required the participants to meet specific criteria to be considered a SME regarding this research and be eligible to take the survey. The selection criteria included an appropriate level of cybersecurity experience, industry IT cybersecurity certifications, or education relating to cybersecurity. The fourth barrier was the possibility of a low response rate from all participants, which was considered when

designing the survey to make it as appealing and easy as possible. A SME panel has no actual requirements or limitations on numbers, but it has been suggested that an ideal number is between 10 to 30 experts (Skinner et al., 2015). Since the reliability of self-reporting is debatable due to people not wanting to be honest about actions they feel will implicate them, reporting co-worker's activities was used for comparison (Alkaldi et al., 2019).

### **Assumptions, Limitations, and Delimitations**

According to Ellis and Levy (2009), "assumptions can be viewed as something the researcher accepts as true without a concrete proof" (p. 331). In this research study, the assumption was that the feedback received from the SMEs would be based on their expertise. Another assumption was that SMEs and employees would be truthful about witnessing their co-workers' use of PWWA since this is not self-incriminating. A limitation of this research study was obtaining enough SMEs interested in taking the survey and providing valuable feedback. Another limitation was the proficiency of the survey tool, and diversifying the panels will be important to have the study universally accepted (Ellis & Levy, 2009). A delimitation of this research was the reliability of the demographic selection of all participants and ensuring specific criteria were maintained and validated to increase accuracy. Another delimitation was that since this is a developmental design research, advancements in newer authentication technologies are continuously being researched (Ellis & Levy, 2010). Recent research continues to theorize that textual passwords will continue to be one of the primary authentication methods due to their perceived reliability and ease of use (Zimmermann & Gerber, 2020).



## **Definition of Terms**

**Authentication** – "Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources" (Grassi et al., 2017, p. 41).

**Black Market** – "Market based production of goods and services, whether legal or illegal, that escapes detection in the official estimates of gross domestic product" (Me & Pasticcio, 2018, p. 119).

**Brute Force Attack** – "A computationally intensive technique that generates a series of passwords using character combinations" (Farik & Ali, 2015, p. 342).

**Compliance** - "Refers to a particular kind of response-acquiescence-to a particular kind of communication-a request" (Cialdini & Trost, 1998, p. 168).

**Cybersecurity** – "Computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems" (Joint Task Force on Cybersecurity Education, 2017, p. 16).

**Data Breach** – "The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information" (National Initiative for Cybersecurity Careers and Study Cybersecurity Glossary, 2021).

**Dictionary Attack**- "A list of words called an attack dictionary (or just dictionary) is used along with different mangling rules to create password guesses" (Houshmand et al., 2015, p. 1786).

**Domino Effect** – "Result as one site's password file falls prey to a hacker who then uses it to infiltrate other systems, potentially revealing additional password files that could lead to the failure of other systems" (Ives et al., 2004, p. 76).

**Impact** – "The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability" (Swanson et al., 2010, p. G-2).

**Information Security Risk** – A level of effect "on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring" (Kissel, 2013, p. 161).

**Information Systems** – "Information systems (IS) involve a variety of information technologies (IT) such as computers, software, databases, communication systems, the Internet, mobile devices and much more, to perform specific tasks" (Boell & Cecez-Kecmanovic, 2015, p. 4959).

**Likelihood** – "A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability" (Boyens et al., 2015, p. 3).

**Password** – "A group of characters, symbols and numbers used for authentication, to gain access to a source or prove the identity of oneself" (Rajah et al., 2020, p. 6950).

**Password Entropy** – "A measure of how hard it is to predict the value of a variable. More specifically, entropy can be considered a measure of the difficulty of guessing a password" (Shay et al., 2010, p. 9).

**Shoulder Surfing** – "An adversary tries to guess the password by keenly looking at the user login their screens" (Irfan et al., 2018, p. 422).

**Social Engineering** – "A skill set utilized by an unknown individual to obtain trust and access to an organization via someone in the organization and consequently guides them to alter IT system rights or access that ultimately grants the individual access rights" (Ghafir et al., 2016, p. 145).

**Spyware Attack** – "Software that is secretly or surreptitiously installed onto an information system to gather information on individuals or organizations without their knowledge; a type of malicious code" (Joint Task Force Transformation Initiative, 2013, p. B-24).

**Subject Matter Expert** – "An individual who, by virtue of position, education, training, or experience, is expected to have greater-than-normal expertise or insight relative to a particular technical or operational discipline, system, or process" (Pace & Sheehan, 2002, pp. 3-4).

**Threat** – "Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service" (NIST, 2012, p. 8).

**Workaround** – "Deviation from an intended work process, which is used to overcome an obstacle, by a practitioner responsible for meeting a work demand; the deviation is likely an active adaptation to the process that is documented in policies and procedures" (Patterson, 2018, p. 1).

## **Summary**

This chapter presented the background, problem statement, research goals, research questions, barriers and issues, assumptions, limitations, delimitations, approach, and definition of terms of this research study. This research study was used to develop a list

of PWWAs, validated by SMEs, and measure the perceived cybersecurity risk of data breaches associated with each PWWA technique, along with self-reported and reported co-worker engagement in each PWWA technique. The data was collected using the Delphi method, with a panel of SMEs, and employees from web-based survey responses and data analysis. The main data collection and analysis were used to empirically test and validate the data to design and develop the PaWoCyRiT. The development of the PaWoCyRiT addressed the main research question: What are the differences among SMEs and users regarding the cybersecurity risk of data breaches as a result of the frequency of PWWA Techniques Usage reported by employees about themselves and their co-workers?

## Chapter 2

### Review of the Literature

#### **Introduction**

In this chapter, topics related to this research are presented. The main areas include data breaches, cybersecurity risk, and authentication. This literature review aims to support a developmental study using constructs of password security and employees' and SMEs' perceived risk of data breach. The analysis of this literature led to a comprehensive discussion on data breaches, expanding into the impact, current trends, and human factors in data breaches. Data breaches and ransomware incidents are documented daily in the news media, while a tsunami of such incidents have been observed in the United States (US) both for organizations as well as individuals, mainly because of the recent COVID-19 pandemic (Levy & Gafni, 2021). The most recent yearly report by the Federal Bureau of Investigation (FBI) 's Internet Crime Complaint Center (IC3) (2020) indicated that "a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding \$4.1 billion. This represents a 69% increase in total complaints from 2019" (p. 3). Following is a review of cybersecurity risk, including risk, risk management, and cybersecurity risk management. A review of authentication, an overview of authentication methods, passwords, common password attacks, and password workarounds led to the development of the first construct of the list of PWWAs. To establish the expected outcomes of this research, this chapter concludes with a summary section on the known and unknown as identified in literature.

## **Data Breaches**

Data breaches result from unauthorized access to IS and generally result in data being replicated, modified, stolen, and released in one way or another (Gilbert, 1992). When an organization has a data breach, more are affected than just the organization, including the individual customers, stakeholders, and the business (Seh et al., 2020). Data breaches have been well documented and evaluated in literature. For example, Gilbert (1992) surveyed multiple laws that would penalize those who enact a data breach, state and federal, in the United States to distinguish gaps in those laws and recommend actions to be taken by organizations as preventive measures. Many preventive measures presented back then are still standard protections suggested today, including security audits, awareness training, classification of systems and data, physical controls, contract agreements, policies, anti-virus protection, and staying informed (Gilbert, 1992). Even with the same measures being suggested for over two decades, data breaches continue to occur; protection from data breaches is becoming more prominent due to the increased technological advances in how much more data organizations store and process.

Research by Mayer et al. (2021) was conducted at the individual level of data breaches to identify individuals' awareness, perception, and response to data breaches that have affected them. The research presented findings that individuals were unaware of breaches that affected them and had misconstrued ideas about the causes and impacts of the data breach (Mayer et al., 2021). The lack of awareness of the causes of data breaches can include password security and compromised credentials, which are significant factors in data breaches and increased the average total cost of data breaches for companies from \$1 million to \$ 4.77 million (Ponemon Institute, 2020). Romanoskey et al. (2014) reviewed

data breaches over 10 years from a legal aspect, which exemplifies that data breaches go beyond just loss of data but can also be loss of monetary value and harmful to reputation.

Data breaches are an essential matter for organizations. Although they are treacherous to a business, little research has gone into the impact on individuals and insights into their reactions (Goode et al., 2017). Mobile users were more motivated to take the proper security measures to protect themselves and secure their devices once they understood the threat level and were confident that the security controls effectively mitigate the threat (Giwah et al., 2020). Therefore, it is significant to focus on the individual users and their perceptions of the likelihood and impact of cybersecurity risk of data breaches for PWWA and correlate it with their understanding of the threat level.

### *Impact*

Data breaches will always result in a negative impact. They can affect an organization's financial, legal, technical, and managerial aspects, leading to immediate loss or damage, legal and regulatory costs, and other costs to the whole organization (Furnell et al., 2020). To obtain a more substantial idea of cyber threats and identify how much worse cyber hacking incidents lead to data breaches, Xu et al. (2018) analyzed a set of cyber incidents over 12 years. They suggested that data breaches caused by cyber hacking seemed to have increased in frequency, but the level of damage is not worse. According to Chen and Jai (2021), for organizations with loyalty programs, the impact after a data breach is that those customers lose their trust in the organization and have high privacy concerns, which could lead to a decrease in membership after a data breach. However, research shows that organizations can rebuild those relationships by notifying customers of the occurrence with a robust apology approach (Chen & Jai, 2021).

An industry that is the biggest target of data breaches incurring the highest costs is the healthcare industry, which cost an average of \$7.13 million in 2020 (Ponemon Institute, 2020). The volume of medical accounts required due to the services provided by healthcare providers increases the healthcare industry's threat platform, ultimately contributing to data breaches being the focal occurrence in healthcare information systems (Luna et al., 2016). Reputation is essential to companies, especially those that trade publicly, particularly in the age of social media, which contributes a lot to the reputation of organizations (Rosati et al., 2018). An analysis of the impact on the US stock price of a company following the announcement of a data breach suggested that social media exposure had an increasingly negative impact on the stock price and how a company makes the announcement was also found to be of significance (Rosati et al., 2018). In Europe, Spain was the only country that showed a significant impact on share price following data breach announcements, but not as much data is available for European data breaches as there is in the US, with databases available such as the Privacy Rights Clearinghouse (Ford et al., 2021).

An organization's reputation is significantly negatively impacted after a data breach, and protecting and repairing its reputation is vital (Gwebu et al., 2019). However, those larger reputation organizations suffer more negligible impacts than those with smaller reputations. Mainly because organizations with smaller reputations react better with their response strategies, Campbell et al. (2003) suggested the type of data breach can negatively impact an organization's stock price in the US stock market; when comparing a data breach that involves the loss of confidential information to those that do not, the market reaction is significantly higher. Besides having a financial impact on an



organization, data breaches impacted customers' and investors' behaviors, and both reactions were different when the breaches were framed as minor. In contrast, investors responded negatively, while customers were more accepting of an apology (Masuch et al., 2022).

The economic impact of data breaches on organizations varies based on the size of an organization and the type of data breach, but a negative financial impact is still significant. The type of data that is compromised in a data breach varies; hence does the impact; the comprised data can involve customer personally identifiable information (PII) and non-personally identifiable information (NPII) (Labrecque et al., 2021). Although the frequency of data breaches continues to increase, seldomly does research study the user's perceptions of the impact of data breaches or potential actions (Labrecque et al., 2021). Chua et al. (2021) suggested that users with knowledge or experience with past data breach occurrences had a higher information security awareness, which developed a stronger sense of safeguarding against data breach impact. The impact of a data breach must be determined by the total cost, both direct and indirect, and the damage could range from short-term, medium-term, or long-term impact (Furnell et al., 2020). Unfortunately, organizations still grapple with being able to quantify the impact of a data breach involving the loss of customer information due to many factors that further complicate the business of justifying cybersecurity risk management resolutions (Poyraz et al., 2020).

**Table 1***Summary of Data Breach Impact From Literature*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Campbell et al., 2003	Literature review and event study	Information security breaches between January 1995 through December 2000	Ordinary Least Squares and seemingly unrelated regression	Disclosure of confidential information in a data breach resulted in a negative reaction
Chen & Jai, 2021	Empirical survey	255 hotel customers	Perceived vulnerability and severity to a hotel data breach	Loyalty program customers lost their trust after a data breach
Ford et al., 2021	Literature review and event study	45 data breach disclosures Between 2017 and 2019	The impact of a data breach announcement for European publicly traded companies	Spain was the only EU country where a data breach impacted price
Gwebu et al., 2019	Event study	303 breach announcements	Efficacy of reputation and organizational response to data breaches	Organizational reputation is vital to protecting the firm value
Labrecque et al., 2021	Experimental survey	203 respondents	Impact of stress and perceptions of a social contract violation	Remote work adoption directly affects remote worker's collaboration network

**Table 1***Summary of Data Breach Impact from Literature (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Luna et al., 2016	Literature review and synthesis	19 articles	Identify patterns and impact of cybercrimes in the	Healthcare technology has increased and requires more attention to cybersecurity
Masuch et al., 2022	Event study	141 data breach announcements	Analyzing the impact an organization's response has on stock value	Response actions and a data breach involving customer data negatively impact the stock
Poyraz et al., 2020	Stepwise regression	133 data breach incidents	Identify the effects of data breaches involving PII	The model was developed to estimate the financial impact of data breaches classified by PII/SPII
Rosati et al., 2018	Event study	74 data breach incidents	Investigate the impact of data breaches on market activity	Data breach announcements have a positive short-term effect
Xu et al., 2018	Trend analysis	280 data breach incidents	Identify the evolution of data breach threats	A method developed to improve data breach insights and prediction accuracies

### *Current trends*

Comparing trends of previous data breaches of information systems is an integral part of the analysis to try and determine factors that lead to data breaches and research ways to mitigate the threat based on the causes (Joseph, 2018). The type, financial damage, frequency, and cause of data breaches are all critical data, but identifying the trends between IS security investments and the probabilities of data breaches is also vital (Angst et al., 2017). For example, hospitals classified as symbolic adopters, compared to substantive adopters over time, showed that increased IS security investments were ineffective in decreasing the likelihood of data breaches (Angst et al., 2018). Data breach trends seem to differ in frequency patterns based on the incident of interests and the industry; over time, more robust security controls may be the reason for some decline in several patterns (Africk & Levy, 2021).

Fritz et al. (2017) suggested that records lost have increased, although data breaches have declined from past attacks. Due to modern technological advances and increased use of digital data, the threats still exist. Previous data breach trends consisted of exfiltrating data, such as the Target incident and Equifax hack, which were mainly successful due to a lack of solid incident response; however, current trends show data breaches are destroying data integrity (Shinde & Kulkarni, 2021). The benefit of organizations learning from past trends leads them to improve their cybersecurity defense by understanding how to utilize more than a single framework to improve their incident management (Shinde & Kulkarni, 2021). Holtfreter and Harrington (2015) developed a model to classify data breaches into two categories, external and internal, to assist organizations in making more workable security strategies for protecting data.

### *Human Factor in Data Breach*

Employees, mainly insider threats, have always been the biggest threat to security and continue to be the biggest unresolved threat, which has increased due to many organizations evolving into the data age and utilizing more technology platforms for their processes (Fielding, 2020). Exploring end-user security behaviors, Stanton et al. (2005) identified password behaviors as a significant problem and focused their research on password management. Over half of the users did not create strong passwords, did not change their passwords frequently, write their passwords down, and even share their passwords with other users inside and outside the organization (Stanton et al., 2005). Siponen et al. (2020) explored neutralization techniques derived from criminology to explore the relationship between human behaviors and violating information security policies. Using neutralization techniques has shown that users rationalize when violating information security policies (Siponen et al., 2020). Security Education, Training, and Awareness (SETA) programs are the most recommended way to improve human behavior. However, research has shown that these programs can be ineffective, and employees disengage when this training tends to be boring, unclear, or receive contradicting information from what the employees believe to be true (Reeves et al., 2021). Siponen et al. (2020) suggested that effective education training can positively impact employees' behaviors, significantly improving safe password practices and mitigating the use of neutralization techniques to violate information security policies.

Techniques exist to measure the reliability of humans in fields such as aviation and medicine and have recently been applied to information security in the form of the Human Error Assessment and Reduction Technique of Information Security (HEART-IS)

(Evans et al., 2019). Applying HEART-IS has rendered significant initial results in enhancing comprehension of human factors resulting from human errors with information security incidents (Evans et al., 2019). As much as an unintentional human error can occur, malicious intentions can also be true when discussing insider threats (Elmrabit et al., 2020). An organization can deploy all the technical controls in the world. However, they will be neglecting one vulnerability that could make all those controls ineffective: the human factor and the threat most used to exploit that vulnerability is social engineering (Luo et al., 2011). Social engineering exploits human factors such as human error and social psychology, employing manipulation techniques to access systems and data (Luo et al., 2011).

Technical security controls are more effective in a defense-in-depth model, joined by managerial, technological (software and hardware), and user training (Liginlal et al., 2009). Liginlal et al. (2009) explored privacy breaches and categorized human errors based on the origin of the breach, the type of errors that resulted in a data breach, and the impact to better understand the essential mechanisms and consequences of human errors. Liginlal et al. (2009) suggested that managing human factors, specifically human errors, should be the highest priority in an organization. Their findings show an increase in human errors resulting in malicious attacks. One human behavior that continues to pose a significant threat to an organization is the broad technique of shadow IT (Silic & Back, 2014). Due to naivety, employees utilize shadow IT techniques, such as using unauthorized software to improve their work productivity while putting the organization at risk (Silic & Back, 2014). Organizations are increasing the use of mobile devices with Bring Your Own Device (BYOD) policies, which were suggested to increase shadow IT

and become a more significant threat to an organization, requiring more focus on different layers of organizational security (Silic & Back, 2014).

When the human factor is discussed in information security, the first measure mentioned is passwords, as they are the first line of defense in authenticating and accessing an organization's IS. Chua et al. (2021) explored the effects of data breach publicity on user information security awareness and whether it was significant. Chua et al. (2021) work on previous research showed that individuals' perceptions of risk of data breaches were more prominent when they were subjected to news regarding data breaches and risks. This research suggested that data breach publicity significantly impacted and improved users' information security awareness, and organizations should strategize their programs to include this knowledge (Chua et al., 2021). It emphasizes the importance of the government and traditional news to provide publicity on data breaches but suggested that social media substantially influences an individual's awareness (Chua et al., 2021).

Since it has been theorized that human factors are predominantly seen as the rudimentary cause of most cyber breaches, Neigel et al. (2020) explored cyber hygiene to understand better users' attitudes and behaviors and specific individual factors that affect cyber hygiene. Women's attitudes towards cyber hygiene suggested that intrinsic motivation was vital; men's results showed that computer self-efficacy and trust in technology were more of a factor (Neigel et al., 2020). Although the research was conducted primarily with undergraduate students, it still shows the necessity to research further human factors in cybersecurity and the gap in knowledge on why humans seem to be the weakest link and where the most significant vulnerabilities exist in users (Neigel et

al., 2020). Hibbeln et al. (2017) conducted a research study on human-computer interaction and the impact of negative emotions. Hibbeln et al. (2017) drew on the Attentional Control Theory (ACT) to explore negative emotions in humans and their effects on their behavior. They measured user cursor movements based on distance and speed by manipulating webpage delays (loading speed) and error messages when simulating an online purchase (Hibbeln et al., 2017). The research results suggested that negative emotions can be detected, and it may be beneficial for systems designers to detect negative emotions during live systems use to assist with building more accessible to deploy and more adaptive systems (Hibbeln et al. (2017). The benefit of this knowledge can also be used in cybersecurity technical and managerial policies to detect if users are experiencing negative emotions when following organizational policies, which may lead them to utilize IT shadow security techniques.

**Table 2**

*Summary of Human Behavior From Literature*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Chua et al., 2021	Empirical survey	529 respondents	Hierarchy regression	Publicity of data breaches improves information security awareness
Elmrabit et al., 2020	Empirical study	70 employees	Bayesian network to model and predict	Spain was the only EU country where a data breach impacted stocks
Evans et al., 2019	Case study	183 information security incidents	Implemented Human Reliability Analysis (HRA)	Developed Human Error Assessment and Reduction Technique of Information Security



**Table 2***Summary of Human Behavior From Literature (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Hibbeln et al., 2017	Experimental and observational study	65 employees and 206 university students	Attention control theory to identify negative emotions	Mouse cursor distance and speed can be used to detect negative emotions
Liginlal et al., 2009	Experimental survey	203 respondents	GEMS error typology to analyze publicly reported privacy breach incidents	Defense-in-depth solution strategy founded on error avoidance, interception, and correction
Neigel et al., 2020	Empirical survey	173 university students	Measures of trust, motivation, computer self-efficacy, and cyber hygiene	Information handling, incident reporting, password management, email use, and Internet use were predictive of cyber hygiene behaviors
Reeves et al., 2021	Contextualist personal construct	20 employees	In-depth interviews to understand negative perceptions of SETA programs	The content and behavior of those around employees influence their beliefs in SETA programs

**Table 2***Summary of Human Behavior from Literature (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Silic & Back, 2014	Case study and literature analysis	10 organizations	Triangulation approach to investigate the Shadow IT phenomena	Employees bypassed organizational policies to accomplish tasks when not provided with the right tools
Siponen et al., 2020	Experimental and survey	98 employees	Using a quasi-experimental design	Training based on cognitive dissonance theory can reduce the use of neutralization techniques when the training is designed that way
Stanton et al., 2005	Empirical survey	110 individuals interviewed/49 IT SMEs/1167 survey participants	Interviews and surveys	Developed a taxonomy of security-related behavior

### **Cybersecurity Risk**

Cybersecurity risk of data breaches has been widely researched in IS since the 1970s, with a more limited platform and physical access ultimately advancing to larger platforms when Internet access became widely available (Goode et al., 2017). Although data breaches are more frequent and becoming more severe, organizations and individuals do not perceive the severity of the risk (D'Arcy et al., 2020). Passwords that are lost or stolen pose problems beyond just password resets, such as a risk of a data breach due to users

practicing PWWA, reusing passwords, or creating weak passphrases (Thomas et al., 2017). Risk management has been applied in many aspects of most organizations' information security programs to mitigate the chance of data breaches, from instilling it in software development to handling security incidents to contain adversarial attacks (Khan et al., 2021). Unfortunately, when estimating information security risk, individuals and organizations underestimate the likelihood of a data breach and its massive impact. Academic research continues to work on isolating certain factors that play a significant part in the risk or impact and likelihood an organization will experience leading to a data breach since this continues to be a significant problem (D'Arcy et al., 2020). Elmrabbit et al. (2020) explored a way to predict an insider threat's risk to a data breach before an occurrence, claiming that insider threat is a significant risk to an organization due to its familiarity and authorized access.

Previous research lacks deeper insight into how to handle data breaches effectively and adequately, and there is a significant need to understand better the risks of data breaches (Khan et al., 2021). No computer operating is entirely safe from all cybersecurity risks because even those not connected and considered stand-alone systems require updates; even if loading them from an external device connected to the computer, they still come from the Internet (Garfinkel, 2012). Multiple compliance and security organizations have been established that continually assist with mitigating cyber security risks by developing frameworks and guidelines (Perakslis & Stanley, 2016). Some well-known ones are the Organisation for Economic Co-operation and Development (OECD), International Organization for Standardization (ISO) 27000, NIST, and some US federal

laws, including the Health Insurance Portability and Accountability Act and Federal Information Security Management Act of 2002 (Perakslis & Stanley, 2016).

### *Risk*

When combined, risk consists of several components that can result in a negative impact that harms an organization (Matulevicius et al., 2008). Risk is ultimately when a vulnerability, which is a weakness, and the potential attack or threat that can expose the vulnerability is conducted, causing an impact that results in damage and exposure (Matulevicius et al., 2008). Ways to treat risks are with security controls, which are countermeasures, but unfortunately, there is no way to eliminate risk. However, the alternative is to mitigate as low as possible to an acceptable level for the organization, with the left-over risk being a residual risk (Matulevicius et al., 2008). Risk is a ubiquitous concept not limited to IS but can apply to any situation or organization. Privacy risk has been a substantial part of protecting PII and user data and has become even more important as the increased use of cloud computing becomes more dominant in most organizations for many of the benefits (Theoharidou et al., 2013). Although migrating data to the cloud may alleviate some of the risk requirements for an organization by transferring them to the Cloud Service Provider (CSP) through contractual obligations such as Service Level Agreements (SLA), they are still ultimately accountable (Theoharidou et al., 2013).

Risk analysis is a process or technique that can assist organizations with identifying and managing risk by assessing certain factors and providing estimations to help support decision-making efforts (Alali et al., 2018). A risk model is predominant in risk analysis and provides efficient feedback on identifying risk and prioritizing an approach (Alali et

al., 2018). Alali et al. (2018) developed a risk assessment model utilizing the Mamdani Fuzzy inference system and compared it with the Sugeno-type evaluating 25 conditions. Alali et al. (2018) suggested that organizations must stay active with the current environment, and components should work under controlled risk to avoid asset and data failure. Human errors play a huge part in an organization's information security risk posture and can be identified as the most considerable risk. Human errors can include negligence by leaking confidential information, misconfigured systems, and not using the correct protocols to protect organizational data (Blackwood-Brown et al., 2019).

**Table 3**

*Summary of Risk From Literature*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Alalili et al., 2018	Developmental study	NA	Fuzzy Inference System approach for utilizing Mamdani Fuzzy model	The Fuzzy Inference Model (FIS) produced risk assessment results based on the four risk factors: vulnerability, threat, likelihood, and impact to specify the range of risks
Blackwood-Brown et al., 2019	Developmental study	173 non-IT employees	Scenario-based demonstration of skills	Prototype of the cybersecurity skills measurement tool
Matulevicius et al., 2008	Developmental study	NA	Misuse case meta-model and textual explanations	Strengthens process guidelines for misuse case applications and suggests improvements

**Table 3***Summary of Risk From Literature (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Matulevicius et al., 2008	Developmental study	NA	Misuse case meta-model and textual explanations	Strengthens process guidelines for misuse case applications and suggests improvements
Theoharidou et al., 2013	Empirical study	NA	Examined privacy risks and when migrating services to the cloud	Provided insight on how impact should be assessed before the migration

*Risk Management*

A digital transformation has taken place over time. Most organizational assets have increased integration with IS and digital systems in cyberspace, requiring a specific risk management model exclusive to cybersecurity risk management (Katsumata & Gavins, 2010). Managing risk is an extensive matter. It first requires defining risk to narrow down ways to mitigate it to an acceptable level. Most organizations currently use standard metrics such as estimated impact if an event were to occur (Bodin et al., 2008). A risk management program aims to minimize or mitigate the likelihood and impact of a negative result through risk analysis and obtain enough information to make informed business decisions (Rees et al., 2011).

Risk management is not limited to one industry or organization but is universal and can involve politicians, executives, security and safety officers, and workers by enforcing

laws, regulations, and directives (Rasmussen, 1997). One of the earliest instances of risk management recorded in history was around 3200 BC in the Tigris-Euphrates Valley when a group known as the Asipu would be consulted for risk analysis (Covello & Mumpower, 1984). The Asipu would collect data and analyze it to present possible outcomes and alternatives for everything from marriages to possible building sites and provide a conclusive analysis on a clay tablet (Covello & Mumpower, 1984). As risk identification capabilities increase, research improves ways to control and reduce risk scientifically and technically and improve risk management capabilities (Covello & Mumpower, 1984).

An organization's use of risk management for IS involves implementing security controls to protect the confidentiality, integrity, and availability of organizational assets (Webb et al., 2014). Information security risk management can be used by organizations to identify whether they have adequate controls in place to effectively protect their information assets while using cost-efficient means (Webb et al., 2014). Webb et al. (2014) proposed enhancing information security risk management by developing a model that used an intelligent-driven process to provide accurate situational awareness information for decision-making. Fenz et al. (2013) investigated challenges in information security risk management. They found several factors that hindered most organizations, including asset identification and valuation, the overconfidence effect, trade-offs between cost-effective controls and risk, and lack of knowledge sharing and predicting risk (Fenz et al., 2013). According to NIST (2012), the "risk management processes include (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk" (p.4). NIST (2012) recommended that organizations not stick to just one

fixed risk model but should use a diverse combination of different factors that apply to the specific organization.

### *Cybersecurity Risk Management*

Cybersecurity continues to gain attention and has done so since the 1970s with the introduction of microcomputers, which eventually led to the current-day need for cybersecurity risk management frameworks (Lee, 2021). Many organizations have started to require a standardized and customizable framework (Lee, 2021). Over the past decades, organizations have experienced a digital transformation that has increased the need for enterprise risk management as data has become easily accessible through mobile devices and stored off-premises on cloud services (Lee, 2021). Cybersecurity risk management needs to address technical aspects and the human factor aspect of cybersecurity, and many frameworks have been developed to do so, including ISO/IEC 27001, NIST Cybersecurity Framework, and Control Objectives for Information and Related Technology (COBIT) (Lee, 2021). Lee (2021) developed a four-layer cybersecurity risk management framework that provides feedback from each layer: cyber ecosystem, cyberinfrastructure layer, cyber risk assessment, and cyber performance (Lee, 2021). One mistake many organizations make is defining cybersecurity risk as only an economic crisis or holistically but should address both non-technical and technical factors (Garfinkel, 2012). Currently, there is no recognizable solution to address all cybersecurity risks. However, with culture becoming more reliable in an information society, the risk grows and requires adopting ways to manage the growing cybersecurity risk (Garfinkel, 2012).



The most basic steps of any cybersecurity risk management process are identified by Eling et al. (2021) as "Environmental scanning, risk identification, risk analysis, risk treatment (risk avoidance, risk mitigation, risk transfer, risk retention risk exploitation), risk monitoring and process review" (p. 96). Eling et al. (2021) argued that traditional cybersecurity risk management addresses known threats that have been identified, but this is useless since most environments involve "rapidly evolving and unknown threats" (p. 118). Instead, they suggested that resilience management would be much more effective in surviving and facing the unexpected and go beyond just computer science and incorporate more behavioral sciences involving human behavior in a resilience approach (Eling et al., 2021). To further complicate cybersecurity risk management, IS has evolved into more complex systems by introducing infrastructure like mobile, cloud, and Internet of Things (IoT), where existing frameworks need to be revised to adapt to these environments (Kandasamy et al., 2020). Kandasamy et al. (2020) reviewed and ranked four popular risk management frameworks for their suitability in being applied to IoT networks and introduced an IoT risk calculation model to suggest the significance of IoT requiring a unique approach to risk management.

The NIST Cybersecurity Framework is an approach to cybersecurity risk management that many organizations have adopted, both government and private sector, as it provides a broad and flexible approach (Gordon et al., 2020). The primary purpose of the NIST Cybersecurity Framework is to provide organizations with cybersecurity risk management using three main mechanisms: Core, Implementation Tiers, and Profiles, along with five basic tasks: Identify, Protect, Detect, Respond, and Recover (Gordon et al., 2020). Cybersecurity risk management notoriety comes in an abundance of data

breaches yearly; the NIST Cybersecurity Framework provides organizations with a common language and direction for mitigating risk in a digital world (Gordon et al., 2020). One of the biggest challenges in the private sector is adopting a cost-effective risk management plan. Gordon et al. (2020) suggested that utilizing the Gordon-Loeb Model for cost-benefit analysis, in combination with the NIST Cybersecurity Risk Management framework, can help organizations apply the more cost-benefit Implementation Tier. One increased measure used for risk analysis is quantification; Alodi and Massacci (2017) developed a model that quantifies the likelihood of an actual attack. Alodi and Massacci (2017) argued that widely used cybersecurity risk analysis standards stipulate biases and can lead to suboptimal resource distribution.

**Table 4**

*Summary of Cybersecurity Risk Management From Literature*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Alodi & Massacci, 2017	Developmental study	NA	Quantitative way to evaluate the likelihood of untargeted attacks	Developed a method that measures the exposure of a system to potential attacks
Eling et al., 2021	Literature review	7 panels	review research on individual steps of the cyber risk management process and on the overall process to highlight gaps	Cyber risk is hard to embed into overall enterprise risk management, and resilience is necessary

**Table 4**

*Summary of Cybersecurity Risk Management From Literature (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Gordon et al., 2020	Empirical study	NA	Integrating cost-benefit analysis into the NIST Cybersecurity Framework	The GL Model provides a logical approach to use when considering the cost-benefit aspects of cybersecurity investments
Kandasamy et al., 2020	Literature review	4 cybersecurity frameworks	Apply novel methods to IoT and IoMT (medical) devices to ascertain their risk level	A novel IoT risk computational model that computes risk impact and risk likelihood, leading to risk score
Lee, 2021	Literature review and developmental study	NA	Discussed cybersecurity trends coinciding with technological paradigm shifts	Developed a framework in which risk management activities are organized and evaluated in four-layer

### **Authentication**

Authentication is an access control method that provides a significant security measure that allows authorized users access to information systems while blocking unauthorized users from gaining access (Mujeye, 2021). Authentication into an organization's IS is an entry point into the systems. Traditional authentication mechanisms are starting to be seen as inconvenient with newer technology replacing how

we currently gain access to systems (Frank et al., 2012). The most used authentication mechanism is passwords, and although much research has gone into finding alternatives, their use is set to increase (Woods & Siponen, 2018). Protecting IS against misuse is vital, and authentication controls are a crucial part of the layered protection in preventing access and protecting an IS against misuse (D'Arcy et al., 2009). The three main protocols used for access are identification, authentication, and authorization; all three work together to provide layered security in authenticating to IS (Nandy et al., 2019).

#### *Overview of Authentication Methods*

The authentication process starts with the user providing identification to the IS; the system will then authenticate the user and authorize their access to the system (Ometov et al., 2018). Alphanumeric or text-based passwords, considered a traditional authentication method, continue to be the most popular and convenient way for users to authenticate (Gokhale & Waghmare, 2014). Due to passwords' vulnerability to online and offline attacks, they have frequently been researched to find an alternative method to authenticate users for system access (Jarecki et al., 2018). The three original factor groups of authentication type are 'something a person knows,' knowledge such as an alphanumeric password; 'something a person has,' possession such as a token or smart card; and 'something a person is,' biometrics such as a person's fingerprints, face or voice (Menkus, 1998; Ometov et al., 2018). Another authentication type is behavioral-based, 'something you do,' which utilizes behavioral attributes to authenticate (Mahfouz et al., 2017). The most used method is 'something you know, and although there are different techniques to implement it, such as question/answer, identifying images, or character-based, text-based passwords are the popular choice (Erlich & Zvira, 2009).

Originally, Single-Factor Authentication (SFA), in which only a one-factor group was used to authenticate, such as a PIN or password, was the standard for accessing IS but was suggested to be weak (Ometov et al., 2018). A more secure method of authenticating is a combination of two or more authentication factor groups known as Multi-Factor Authentication (MFA) (Mujeje, 2021). MFA is taking one method like a token (something a person has) and a pin (something a person knows) and requiring both for a user to authenticate successfully (Mujeje, 2021). Multi-modal authentication is a technique introduced to authenticate continuously by using post-login, nonobstructive verification of a user based on behavioral biometrics (Gasti et al., 2016).

Beyond MFA, all SFA authentication methods continue to be researched for a more advanced and secure method. For example, research has examined whether behavioral biometric features can be captured and utilized for authentication (Frank et al., 2012; Sae-Bae et al., 2014). Frank et al. (2012) developed a proof-of-concept framework containing 30 behavioral features based on the user interface of using a touch screen. Research shows that the number of accounts users have accumulated over time has increased the number of passwords a user has for authentication (Brumen, 2020; Theofanos et al., 2021). Passwords remain the superior choice for authentication, despite multiple alternatives that exist, and research suggests that they will be around for much of the future due to their simplicity and reliance (Dillon et al., 2020; Furnell, 2019; Pearman et al., 2019; Shay et al., 2010; Wang et al., 2017; Woods & Siponen, 2018). Much research continues to be dedicated to identifying a more secure way to authenticate and improve password methods or replace them altogether (Zheng & Jia, 2017).

## *Passwords*

The concept of passwords precedes modern-day technology, but even with the advancements that have been made, they continue to be the most used authentication method (Shay et al., 2010). One crucial factor in creating passwords is password entropy, and most organizations create their password policy to ensure users create a more secure password that is harder to crack (Shay et al., 2010). Shay et al. (2010) conducted a survey and they suggested that although most users find these more robust password policy requirements inconvenient, they feel more confident in the level of protection they are suggested to provide (Shay et al., 2010). IS research on password security predominantly observes and explores security behavior in two ways: policy compliance and user memory (Woods, 2019).

Zheng and Jia (2017) proposed a new password authentication method in which separators are inserted between the user's keystrokes, which were suggested to improve the resistance against usual password attacks. The method exhibited practicality, a low memory burden on users, and provided high password strength, but still had limitations. The system itself would still be vulnerable to SQL injections or cross-script attacks since this technique uses browser extensions or back-end JavaScript code (Zheng & Jia, 2017). A benchmarking tool was explored to improve password authentication by measuring the strength of the password attributes, which could improve system security (Mattord et al., 2013). NIST (Grassi et al., 2017) recently updated the guidelines for password policies to ease the memorability factor on users and try to make it easier to create more secure passwords; some of the guideline's recommendations are:

1. Be at least eight characters in length; space characters allowed;

2. A password strength meter should be used and compared to a list of compromised values;
3. Limit the number of failed attempts;
4. Securely transmit and store passwords;
5. Remove the requirement for composition rules;
6. Remove the requirement for periodic password changes;
7. Allow users to paste passwords;
8. Allow showing of password when entering; masking not required;
9. Allow password managers;

Users continue to be the weakest link in password security, and even after decades of research into passwords, not much has changed (Brumen, 2020). Brumen (2020) suggested that strict password management policies, such as using auto-generated passwords, were ineffective as they hindered the user's effectiveness in remembering them. Although these password policies are created to ensure the security of the user's account and organizational systems as the complexity increases, it was suggested that users get annoyed, and their actions possibly risk the integrity of security and the systems (Dillon et al., 2020). The most common password policy recommendations to help ease the stress for users and secure their accounts and systems are password managers and MFA (Dillon et al., 2020; Grimes, 2020). The benefits of a password manager are that they not only store and automatically fill in the passwords for users but also autogenerate random and robust passwords (Pearman et al., 2019). Despite the benefits, research suggested that many still do not use password managers due to concerns about security, convenience, and usability (Pearman et al., 2019). Password managers have introduced

an equalized way for users to use passwords securely, and most research has explored the technical aspects. However, more work needs to be done on human behavior (Alkaldi et al., 2019). Alkaldi et al. (2019) used the Self-Determination Theory (SDT) to empirically explore the contentment of users' SDT needs and observe the influence of adopting password managers, suggesting there was relevance in encouraging adoption.

Yildirim and Mackie (2019) suggested that providing users with a specific password guideline upon creating a password assisted users in creating stronger passwords and showed to be more beneficial than strict policy enforcement. Not only did the method help with creating a stronger password, but users were satisfied with the method, and it did help with remembering their passwords, but a small percentage did admit to still writing their passwords down (Yildirim & Mackie, 2019). Most children in school have had technology embedded in their lives from a young age and have never experienced a life without it (Theofanos et al., 2021). Since most systems require authentication, Theofanos et al. (2021) explored children's perceptions, habits, and understanding of passwords. They found that most of their knowledge of password hygiene came primarily from home and school compared to the influence of the Internet and friends (Theofanos et al., 2021). Children have a proper understanding of passwords but have still demonstrated bad password habits despite it. It was suggested that emphasizing positive perceptions of passwords with children early on could promote more vital cybersecurity in the future (Theofanos et al., 2021). Although passwords continue to be the chosen authentication method for their convenience and simplicity in implementation, they are still subject to conventional password attacks (Zheng & Jia, 2017).



**Table 5***Summary of Passwords From Literature*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Alkaldi et al., 2019	Factorial experimental	470 participants	Harnessed the tenets of self-determination theory to encourage the adoption of password managers	Satisfying the three needs, particularly autonomy and relatedness, did indeed encourage the adoption
Bruman, 2020	Experimental and observational study	40 users	Participants were assigned a random string, passphrase, and PsychoPass passwords and had to memorize them	System-assigned strong passwords are inappropriate and put an unacceptable memory burden on users
Dillon et al., 2020	Empirical survey	51 users	An online scenario-based survey asking users to create passwords while increasing restrictions examined using the Shapiro-Wilk test	The increased use of password restrictions increases the chances of workarounds and compromising password security
Mattord et al., 2013	Developmental research	NA	Explored password strength requirements, password usage methods, and password reset requirements	Develop a benchmarking tool to assess authentication methods for web-based systems

**Table 5***Summary of Passwords From Literature (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Pearman et al., 2019	Interview study	30 participants	Semi-structured interviews on user behaviors, beliefs, and understanding of password creation, account security and password management and storage	Users of built-in password managers are often driven by convenience, whereas users of separately installed password managers prioritize security
Shay et al., 2010	Empirical survey and synthesis	470 computer users	Collected data about behaviors and practices related to the use and creation of passwords and opinions on stronger requirements	Users find new requirements annoying and struggle to comply, more likely to share and reuse passwords than write them down, modify old passwords, use dictionary words and names
Theofanos et al., 2021	Empirical survey	1505 students	Self-report survey to understand what challenges US grade school children face regarding passwords	Children understand password security but do not comply
Woods, 2019	Literature review	NA	Literature review on password and intrinsic motivation	Finding how to motivate users to put more effort into the password process

**Table 5***Summary of Passwords From Literature (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Yildirim & Mackie, 2019	Experimental study	308 participants	User-friendly guideline approach to password creation persuasive messages that motivate and influence users	The password creation methods and persuasive message provided to users convinced them to create cryptographically strong and memorable passwords
Zheng & Jia, 2017	Experimental study and empirical analysis	NA	Add a middleware between user input and the website database to add separators in passwords	Introduced a method combined PWD that, through inserting separators, strengthens password security

*Common Password Attacks*

Passwords grant authorized access to systems, and the security of those systems ultimately relies on the protection and confidentiality of that individual passphrase; if an adversary were to obtain this passphrase, they could gain unauthorized access (Notoatmodjo & Thomborson, 2009). According to Notoatmodjo and Thomborson (2009), there are three category types of password attacks are:

1. System end attacks
2. Communication transit attacks
3. End-user attacks

The most common password attacks include brute-force attacks, dictionary attacks, rainbow-table attacks, credential stuffing, shoulder surfing, replay attacks, phishing attacks, and key loggers (Bhanushali et al., 2015; Pal et al., 2019; Raza et al., 2012, Tatli, 2015). A system-end attack is an attack on the system primarily because this is where the passwords are stored; examples of these types of attacks are brute-force attacks, dictionary attacks, rainbow-table attacks, and credential stuffing, where the adversary runs through trial-and-error of possible combinations (Notoatmodjo & Thomborson, 2007, Pal et al., 2019; Tatli, 2015). Communication attacks would be an attack on the communication traffic between an end system and end-user; examples of attacks that target the communication channel are a Man-In-The-Middle (MITM) attack, replay attack, or eavesdropping; the adversary sits in between a session and sniffs or manipulates the traffic (Hao et al., 2018; Notoatmodjo & Thomborson, 2009). One of the most common attacks on the end-user is a social engineering attack; some of the most common social engineering attacks include phishing, shoulder surfing, and keyloggers (Bhanushali et al., 2015; Pal et al., 2019; Raza et al., 2012).

A brute-force attack consists of an adversary trying as many combinations of passwords and passphrases to break into the system and gain access (Raza et al., 2012). The difference between a brute-force attack and a dictionary attack is that a dictionary attack uses common words usually found to be passwords and is not as time-consuming as brute-force attacks (Raza et al., 2012). A rainbow table attack is done by utilizing a unique table containing hashed output values; it is used to crack password hashes by comparing and ultimately divulging their plaintext values (Tatli, 2015). Users who reuse passwords are most vulnerable to a credential stuffing attack involving an adversary

utilizing a list of stolen credentials to try and access all different accounts (Nathan, 2020; Sahin & Li, 2021).

One approach suggested to improve password security against these attacks was the exploration of the Game Changer Password System (Brumen, 2019). As an enhancement of the password process, it presents a user with a game to choose from, such as a board game, and then the user needs to place four pieces or so in spots on the board that the user initially set up as an authentication measure (Brumen, 2019). Other common suggestions are security awareness for high entropy passwords and security policies enforcing these password complexity rules (Chanda, 2016; Shay et al., 2010; Tatli, 2015).

Attacks on the communication channel exist in different forms, such as eavesdropping, when an adversary sits between two parties and sees the traffic, which can be active or passive (Si et al., 2020). Eavesdropping attacks, such as MITM attacks or replay attacks, are done when the adversary can capture the traffic and manipulate the traffic (Alkeem et al., 2017). Si et al. (2020) proposed a secrecy transmission scheme to improve artificial noise by utilizing instantaneous channel state information. This was suggested to improve the secrecy performance for communication to confuse eavesdroppers (Si et al., 2020).

A phishing attack comes in many forms. A user is contacted via text, phone call, or email, masquerading as a legitimate person or business and tricking the user into divulging their passwords or credit card information (Lei et al., 2008). Another social engineering attack on the end-user is shoulder surfing, a method where an adversary stands behind the user as they input their information and captures passwords or more which can be done by recording the user with a camera (Lai & Arko, 2021; Lei et al.,

2008; Notoatmodjo & Thomborson, 2009). Lai and Arko (2021) explored a way to resist the effectiveness of shoulder surfing by introducing a scheme where the user is presented with a pattern on the screen that shows the user how to input their password. This method is suggested to prevent the adversary from accurately capturing the input password (Lai & Arko, 2021). Another social engineering attack is key loggers; this is software that can be installed on a local computer by tricking a user into unwittingly clicking on a link and working in the background; it records all keystrokes and creates a file log for the adversary to review (Raza et al., 2012). Although many different types of password attacks exist, there are many technological controls to try and defend against them. However, the more significant challenge is preventing PWWA as they void those protections and create vulnerabilities.

#### *Password Workarounds*

Passwords ensure security protection and privacy against unauthorized access to an organization's network or individual personal accounts. These passwords are meant to be protected for secrecy by the individuals. However, much research has suggested the opposite is happening, and users are utilizing many types of PWWA to cope with organizational password policies and memory challenges in trying to remember many passwords (Das et al., 2014; Bryant & Campbell, 2006; Güven et al., 2022; Kirlappos et al., 2015; Rajah et al., 2020; Silic & Back, 2014; Siponen et al., 2020; Stanton et al., 2005; Whitty et al., 2015; Woods, 2019; Woods & Siponen, 2018; Woods & Siponen, 2019). Different contributing factors to password behavior have been researched, such as classifying different security behaviors (Stanton et al., 2005) and exploring age and gender concerning insecure password practices (Bryant & Campbell, 2006). Adams and

Sasse (1999) posited that users' PWWA habits happen because of the lack of knowledge of real-world threats; when threats were evident to the users, they displayed exemplary password behaviors. On the contrary, the belief is that if the user is informed, then information leaks will happen, but abstaining from informing users of the reasoning behind secure passwords causes them to decrease users motivation, resulting in stricter security password policies (Adams & Sasses, 1999). A compiled list of PWWA found in literature is shown in Table 6.

According to Alter (2014), workarounds are when a user either facilitates or intentionally applies actions contradictory to organizational procedures or expectancies to overcome a technical restriction. The stricter password policies and the multiple accounts a user has eventually increased user fatigue, leading to PWWA, such as reusing passwords across multiple accounts, leading to a security vulnerability (Das et al., 2014). If an adversary were to compromise just one of those accounts, they would have access to multiple accounts (Das et al., 2014). Levy and Gafni (2021) outlined such a domino effect and provided multiple cases of its massive impact on a single company and a whole industry. Notoatmodjo and Thomborson (2009) suggested that users mentally classified their accounts based on perceived importance and were less likely to reuse passwords for more important accounts. Samadi et al. (2018) explored ways to prevent users from reusing passwords by introducing two mind-hash techniques, 3-word and random letter hash, which showed some success in the limited study. Wang and Reiter (2018) suggested that although decades of research have been conducted to stop password reuse, the progress has been slow. They introduced a technical framework that

would allow websites to coordinate, making it harder for users to reuse passwords while protecting security and privacy (Wang & Reiter, 2018).

Alomari and Thorpe (2020) explored users' behaviors when creating and recalling passwords. They suggested that users appeared willing to sacrifice security over memorability on occasionally used accounts, security over memorability and speed for email accounts, and more robust security over speed for financial accounts (Alomari & Thorpe, 2020). Hospitals utilize password-authenticated devices and systems, where time is of the essence, and life can be at risk; it was observed that passwords were written down everywhere and even on medical devices where a username and password were posted and shared (Koppel et al., 2015). Although the users are not malicious in their behavior, it does produce an inevitable conflict. When patient care is at risk, the system user becomes creative and motivated to bypass password policies (Koppel et al., 2015). Siponen et al. (2020) suggested users utilize neutralization techniques, or rationalizations, to cope with their actions of bypassing organizational password security policy, which is a crucial concerning habit. Education training was implemented to explore if it was effective against neutralization techniques and suggested it decreased the use, and users showed greater intent to create stronger passwords (Siponen et al., 2020). The increase of password entropy through policies increases the memory burden on users and leads to PWWA; even when users can use their own strategies to create passwords, they can memorize the passwords, but they are weaker (Guo et al., 2019). Guo et al. (2019) proposed a figure design on the keyboard to replace memorized textual passwords, and participants felt very strongly that this technique was much more secure than traditional methods.



Although there are options to assist users with the burdens of passwords, such as password managers, research suggested that users tend to have issues when interacting with them, which deters them from using password managers (Huaman et al., 2021). Rajah et al. (2020) explored personal data breaches in users who utilized PWWA and suggested that weak passwords entropy length, easy-to-guess passwords, and common passwords significantly impact personal data breaches. A significant factor in personal data breaches was the lack of MFA. It is suggested to utilize this for all accounts where the option is available, as it could mitigate personal data breaches (Rajah et al., 2020). Arduin and Vieru (2017) utilized Alter's (2014) theory of workarounds to find a link between workarounds and IS security policies. A conceptional model was developed containing four characteristics: intentional, self-benefiting, rule-breaking, and possible damage to generate knowledge on a new threat when a workaround is an input (Arduin & Vieru, 2017). Disregarding information security policies, especially password policies, is costly for the organization and the users because they can introduce several vulnerabilities, increasing the risk (Woods & Siponen, 2019).

**Table 6**

*Summary of PWWA From Literature*

<b>PWWA Number</b>	<b>PWWA</b>	<b>Literature Sources</b>	<b>Description</b>
1	Password recording	Alomari & Thorpe, 2019; Bryant & Campbell, 2006; Chanda, 2016; Chowdhury et al., 2020; Guo et al., 2019; Kaleta et al., 2019; Koppel et al., 2015; Notoatmodjo & Thomborson, 2009; Shay et al., 2010; Siponen et al., 2020; Stanton et al., 2005; Tankeski et al., 2019; Woods & Siponen, 2019; Woods, 2019	Write down/record on paper, mobile, computer, or other devices

**Table 6***Summary of PWWA From Literature (continued)*

<b>PWWA Number</b>	<b>PWWA</b>	<b>Literature Sources</b>	<b>Description</b>
2	Password reuse	Alomari & Thorpe, 2019; Arduin & Vieru, 2017; Bryant & Campbell, 2006; Chanda, 2016; Das et al., 2014; Golla et al., 2017; Guo et al., 2019; Güven et al., 2022; Huaman et al., 2021; Ives et al., (2004); Kaleta et al., 2019; Koppel et al., 2015; Nathan, 2020; Notoatmodjo & Thomborson, 2009; Rajah et al., 2020; Sahin & Li, 2021; Shay et al., 2010; Siponen et al., 2020; Sun et al., 2012; Tankeski et al., 2019; Trabelsi & Missaoui, 2018; Wang & Reiter, 2018; Whitty et al., 2015; Woods & Siponen, 2019; Woods, 2019	Reuse the same password for different accounts
3	Password sharing	Alomari & Thorpe, 2019; Chowdhury et al., 2020; Dang-Pham et al., 2017; Kirlappos et al., 2015; Koppel et al., 2015; Notoatmodjo & Thomborson, 2009; Shay et al., 2010; Siponen et al., 2020; Stanton et al., 2005; Tankeski et al., 2019; Wang & Reiter, 2018; Whitty et al., 2015; Woods & Siponen, 2019; Woods, 2019; Woods, 2019	Share work or personal passwords for any account
4	Weak password selection strategies	Alomari & Thorpe, 2019; Bryant & Campbell, 2006; Chanda, 2016; Guo et al., 2019; Güven et al., 2022; Huaman et al., 2021; Kaleta et al., 2019; Kirlappos et al., 2015; Notoatmodjo & Thomborson, 2009; Rajah et al., 2020; Shay et al., 2010; Siponen et al., 2020; Stanton et al., 2005; Tankeski et al., 2019; Whitty et al., 2015; Woods & Siponen, 2019; Woods, 2019	Use repeated patterns, names, meaningful numbers, or dates

**Table 6***Summary of PWWA From Literature (continued)*

<b>PWWA Number</b>	<b>PWWA</b>	<b>Literature Sources</b>	<b>Description</b>
5	Password change	Alomari & Thorpe, 2019; Chowdhury et al., 2020; Das et al., 2014; Shay et al., 2010; Tankeski et al., 2019; Woods & Siponen, 2019	Password change to a variation of an old password
6	Password change trigger	Alomari & Thorpe, 2019; Bryant & Campbell; Shay et al., 2010; Siponen et al., 2020; Stanton et al., 2005	Change password when informed it has been compromised or frequently
7	Storing passwords	Chanda, 2016; Woods, 2019	Physically or logically storing passwords

### **Summary of What is Known and Unknown**

A literature review of different aspects of data breach, cybersecurity risk, and authentication was conducted in the cybersecurity research field to provide a foundation for this research study. Through this literature review, assorted PWWA techniques were identified as they relate to the cybersecurity risk of data breaches. The PWWA techniques identified from literature had shown they were frequently used (Alomari & Thorpe, 2019) and a threat to an organization (Notoatmodjo & Thomborson, 2009) and can result in a domino effect impact on an organization (Levy & Gafni, 2021). It is known that textual passwords will continue to be the most common authentication method used for system and account access (Güven et al., 2022; Huaman et al., 2021). It is also known that the number of accounts users will require, for personal and professional accounts, will continue to increase, which in contrast would increase the number of passwords

required, creating a memory burden on users (Mujeje et al., 2016; Shay et al., 2010; Woods & Siponen, 2019).

In 2017, modifications to the NIST guidelines regarding passwords aimed to reduce the burden on users (Grassi et al., 2017). An influx of password breaches in large organizations has increased, exposing stolen credentials (Bhagavatula et al., 2020). Woods (2019) highlighted the need to motivate users to take password security more seriously, as security policies are insufficient. What is not known is whether users understand the impact of using PWWA techniques or their perception of the cybersecurity risk they pose to an organization is something that needs to be further researched. Thus, this research study expanded on the existing knowledge of PWWA and the perceived impact based on IS users' and SMEs' input. This study developed a taxonomy to align these PWWA techniques with their perceived threat level and frequency of reported engagement.

## Chapter 3

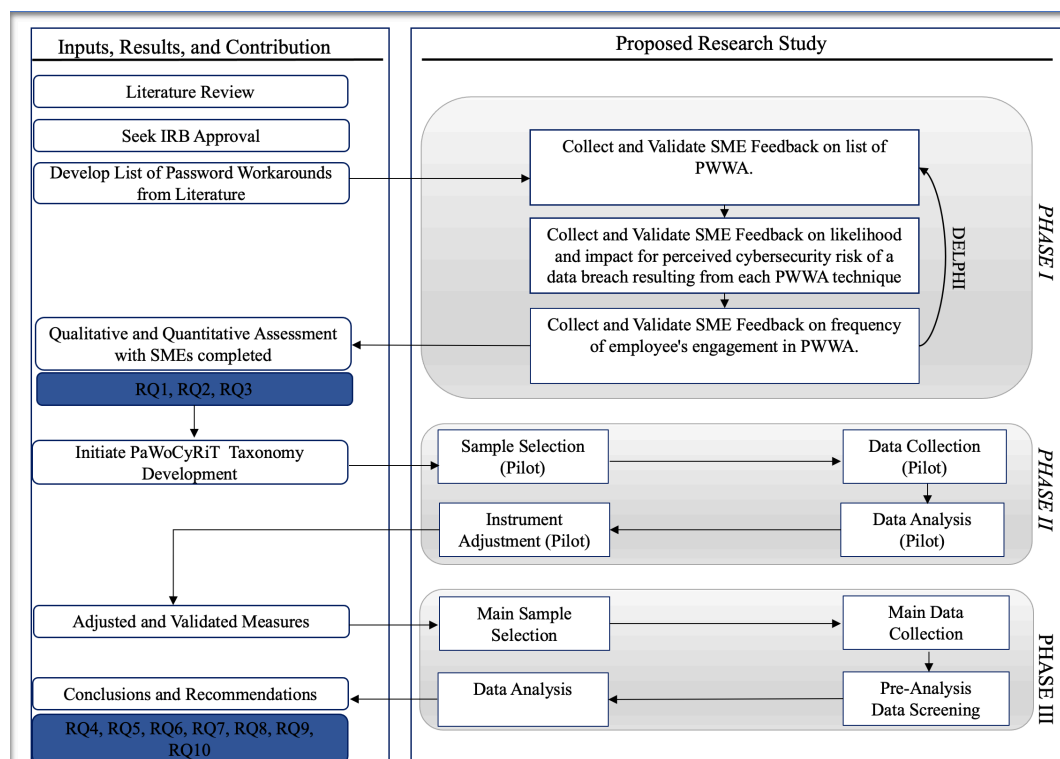
### Methodology

#### Overview of Research Design

This research study was a developmental design conducted in three phases utilizing qualitative and quantitative methods (Ellis & Levy, 2009). Collecting both data sets, qualitative and quantitative, is considered a sequential mixed-methods approach and is a suitable method for the developmental design, providing a viable empirical measurement (Creswell & Clark, 2017). Developmental research can be seen as bridging theory and practice, leading to new methods, models, and tools to solve organizational problems (Ellis & Levy, 2010). The research design is depicted in Figure 2, an overview of the research design process to develop and validate the PaWoCyRiT.

**Figure 2**

*An Overview of the Research Design Process to Develop and Validate the PaWoCyRiT*



## Phase One

In the first phase, a literature review was conducted to compile a list of PWWA provided to the SMEs for validation. In total, 10 major PWWA were identified to include the following:

**Table 7**

*PWWA From Literature*

<b>PWWA Number</b>	<b>PWWAs</b>
1	Record passwords (write down/record on paper, mobile, computer, or other devices)
2	Reuse passwords
3	Shared passwords
4	Created weak passwords (use repeated patterns, names, meaningful numbers, or dates, etc.)
5	Change passwords to previously used passwords
6	No Password Change Due to Trigger (not changing password periodically, when prompted or when compromised)
7	Storing passwords physically in the open
8	Storing passwords physically in a private area
9	Storing passwords digitally in a password vault app/tool/keychain
10	Storing passwords digitally in the browser

The IRB memorandum for using human subjects was approved (See Appendix A). Next, the first phase of this research utilized the Delphi method. The identified list of PWWA was used for the SMEs to validate and provide feedback on the likelihood and impact of perceived cybersecurity risk of data breaches for each technique. This research study comprised of SMEs with cybersecurity backgrounds and employees who frequently

use IS for work and personal use. Upon IRB approval, SMEs and IS users were solicited via e-mail recruitment letters (See Appendix B and Appendix C) via sources such as LinkedIn and Facebook and by users forwarding the recruitment letter with the survey link. Survey criteria for SMEs included cybersecurity experience, certification, or education, aiming to survey 25 candidates. The background of SMEs was validated through the survey demographic questions that are presented at the end of the survey. SMEs for this survey were inquired through LinkedIn based on a search that meets the SME criteria of experience, education, or certifications. The recruitment letter for SMEs (See Appendix B) was sent via a LinkedIn message asking for participation as a SME; the message included a consent note clarifying that clicking on the link that leads to the survey conveys consent.

The validation consisted of the SMEs verifying the list and expanding any PWWA techniques they have experienced. The SMEs were also asked to provide feedback on the frequency of their use of PWWA techniques, the frequency of their coworkers' engagement using each PWWA technique, and rank each PWWA technique based on their perceived severity, which identified the technique numerically for the PaWoCyRiT. IS users had fewer criteria than SMEs. A message was sent on LinkedIn and other social media platforms to the prospective IS user participants (See Appendix C), which included a consent note, link, and a request to forward the survey link to all who would participate. Randomly solicited SMEs from LinkedIn may minimize the lack of truthfulness when responding to questions about coworkers' behaviors.

This phase used a survey (See Appendix D and Appendix E) to record SME responses. The feedback provided by the SMEs is expected to answer RQ1, RQ2, and RQ3.

## **Phase Two**

Phase two consisted of a pilot selection, collection, adjustment, and analysis. The pilot was conducted to ensure reliability and validity and identify if any measurement issues would have hindered the results (Straub, 1989). Once the pre-analysis was completed, the main data analysis began. The completion of the first phase addressed RQ1, RQ2, and RQ3. In phase two, the IS user recruitment letter (See Appendix C) containing the link for the IS user survey with the validated PWWA techniques and scales was presented to a smaller sample for the pilot sample selection, collection, and analysis before adjusting for the main data collection in phase three.

## **Phase Three**

In phase three, the adjusted survey (See Appendix E) was presented to over 300 employee participants who are frequent IS users for their work and daily use. Once the responses were received, a data pre-analysis was done to validate the main data collection for accuracy and identify any missing data. The adjusted and validated measurements were then used in phase three for main data collection, surveying employees' perceptions on the likelihood and impact of cybersecurity risk of data breaches for each technique. The employees were then asked about their self-reported and coworker's frequency use of the validated PWWA, collecting demographic data simultaneously. Phase three results were used to develop and validate the PaWoCyRiT and answer RQ4, RQ5, RQ6, RQ7, RQ8, RQ9, and RQ10.

## **Sample**

According to Terrell (2016), "sample size should be large enough to allow for equal representation of the characteristics that you have identified as important" (p. 66). A panel of SMEs used in research studies does not have size limitations, but due to this



research study soliciting SMEs with expert credentials, the size can consist of 20 to 25 SMEs (Skinner et al., 2015). The survey size for the group of SMEs were required to have a background in cybersecurity based on the following criteria: a practical level of cybersecurity experience (at least five years), industry IT/Cybersecurity certification, and education relating to IS/cybersecurity; the aim was to have 25 SMEs survey while soliciting up to 50 SMEs. This research study aimed to survey a minimum of 300 employee participants; too small or large a sample size may cause inconclusive results. Research has suggested that the ideal sample size is between 30 and 550 (Sekaran & Bougie, 2016). The survey solicited 500 potential participants to achieve the target number of 300 participants and to alleviate any issues of not receiving enough participants for the 300-sample size.

### **Survey Tool**

Cicchetti et al. (1985) conducted computer-simulated research on the number of categories that should be used in empirical research and found that utilizing a 7-point scale measurement was more reliable than using anything less. Therefore, measurements for this research used a 7-point Likert scale for SMEs and employees reporting on the frequency of engagement of PWWA use by themselves and their coworkers. The perceived likelihood and impact of data breaches for each PWWA were measured using a 7-point Likert scale. A Likert scale is an accepted measurement tool in scholarly research; it can produce original data and be associated with numbers or assorted values (Ellis & Levy, 2012). For each validated PWWA, the SMEs and employees were asked to use the scales to identify the perceived level of risk of data breach(impact), reported coworker frequency engagement, and self-reported frequency engagement for each PWWA (See Appendix D and Appendix E).

Validity is a critical part of research and helps future researchers provide a reliable instrument that can produce similar research constructs, as a lack of validity and reliability will render the research untrusted (Straub, 1989). Preliminary qualitative exploratory research was used to establish instrument validation and reliability before using a quantitative empirical technique for data collection. External validity ensures the results are applicable across most environments and can be generalized for any setting (Ellis & Levy, 2009). Threats to external validity, which, according to Straub (1989), “deals with persons, settings, and times to which findings can be generalized” (p. 150), were addressed by ensuring a larger sample size and maintaining the same questions for all participants. Given the issues of truthfulness in the responses and attempts to measure more accurately, additional details on handling the measures were included in the methodology section of this research.

According to Levy (2006), “pre-analysis data preparation deals with the process of detecting irregularities or problems with the collected data” (p. 153). This research study utilized a web-based survey platform to collect data from SMEs and employees for the Delphi method, pilot data collection, and main data collection. The pre-analysis validated the data’s quality and tried to mitigate any discrepancies before the main data collection. The advantages of using a web-based survey platform are that the data can be collected from participants at their convenience, and the automatic collection of responses allows for a more efficient process for data analysis.

“The web-based quantitative data collection site will be designed to preclude data entry errors, thereby assuring the researcher of the validity of the data collected.

Because of that validity, quantitative data analysis will include the appropriate descriptive and inferential tools” (Terrell, 2016, p. 242).

The main data collection then went through the main data analysis to answer the remaining research questions and design and develop the PaWoCyRiT to compare the responses of the SMEs and the employees. The research questions RQ4, RQ5, RQ6, RQ7, RQ8, RQ9, and RQ10 were addressed after phase three was completed.

### **Resources**

IRB approval was obtained to work with human subjects through surveys (See Appendix A). The human subjects involved the Delphi method of surveying SMEs, and surveying IS users. An online survey tool was used, called Qualtrics, for convenient access for the SMEs and IS users and for better data collection for this research. No PII was collected, and the users were informed that all surveys and information were completely voluntary, and their anonymity were safeguarded. For the data collected, Statistical Package for the Social Sciences (SPSS) was used for quantitative data analysis.

### **Summary**

This chapter provides an overview of the methodology that was used for this research study. This research study utilized a sequential mixed-methods approach, both qualitative and quantitative, to collect the research data and develop, validate, and test the taxonomy. This research study contained three phases, with the first phase using the Delphi method and collecting data from SMEs to validate the list of PWWA established in the literature review and answered RQ1, RQ2, and RQ3. The second phase involved conducting the pilot to ensure the reliability and validity of the data. The third phase involved the main data collection and analysis that was used to answer the remaining research questions:

RQ4, RQ5, RQ6, RQ7, RQ8, RQ9, and RQ10, as well as led to the development and validation of the PaWoCyRiT.

## Chapter 4

### Results

#### **Overview**

This chapter covers the data collection results from all three phases of this developmental research design (See Figure 2) and the development of the PaWoCyRiT. The expert panel confirmation, validation, perception, and feedback are presented in Phase I. Phase I used the Delphi method to survey SMEs and included two rounds of data collection. Next, Phase II is presented in which a pilot was completed to validate all the input provided by the SMEs supplementarily. Following were the results of Phase III, in which the IS users were surveyed to include their perception of the PWWAs leading to data breaches, self-reported engagement of PWWAs, and reported co-workers' engagement of PWWAs. The chapter concludes with a summary and comparison of the perception of each PWWA that may lead to a data breach, the self-reported use and reported co-worker's use, and the ranking of the PWWAs and the developed PaWoCyRiT.

#### **Data Analysis**

##### *Results Phase I-Subject Matter Expert (SME) Panel Round 1*

Phase I of this research study included developing a thorough list of PWWAs from the literature. A review of the current literature on password security was used to develop the list of PWWAs used for the SMEs' Phase I survey. The first round of the Delphi method was utilized with a target number of 25 SMEs. 28 SMEs' responses were received after soliciting over 101 SMEs via email, LinkedIn messages, and sharing from other SMEs to those who worked in cybersecurity. In the first round, the 28 SMEs answered

demographic questions and provided their input and perceptions of each PWWA. A 7-point Likert scale was presented for the SMEs to respond to and used to validate the PWWAs by responding to the probability that each of the 10 identified PWWA, when used by co-workers, would lead to an organizational data breach. The next series of Likert scale questions had the SME self-report their frequency use of each PWWA, followed by the SME's report of co-workers' frequency use of each PWWA. After, the SMEs were asked to rank each of the 10 identified PWWAs. Lastly, the SMEs were asked to provide any additional PWWAs they could think of that were not listed in the above, and some SMEs made contact via this other section at the end of the survey to provide minor feedback and additional PWWAs, which were added to round 2.

Although a range of 51% to 100% is needed for validation during the Delphi rounds, 75% or greater consensus is standard as an acceptable level (Dupuis et al., 2016). For this study, an agreement level of 75% or more was used as a scale to validate each PWWA, and out of the 10 PWWAs presented in the first round, only four were found to have an agreement level above 75%; therefore, a second round of Delphi was required. Due to the lack of consensus on validating the original PWWA list in round one, it allowed for adjustments based on the feedback received from the first round for the second round. The second round of the Delphi survey was adjusted per the feedback, which included the following:

- Reworded the PWWA Likert scale questions to clarify better what was being asked for validation, risk, and frequency, adding bold and colored text for distinction.

- Reworded the PWWA’s responses to clarify better what each action entailed, adding bold characters for distinction.
- Moved demographic questions to the end of the survey.
- Added “Mixed Sectors” in the IT experience question.
- Changed “Do you hold a degree” to “What is the highest degree” to eliminate multiple responses.
- Removed the ranking of the PWWA since it was not necessary to answer any of the research questions.
- Additional question asking if the SME participated in round 1
- Added five additional PWWAs based on SME feedback that was deemed feasible (See Table 8).

**Table 8***Delphi Round 2 Adjusted PWWAs List*

<b>PWWA Number</b>	<b>PWWAs</b>
1	Documenting passwords (write down/record on paper, saved in mobile, computer, or other devices)
2	Reusing the same passwords for multiple accounts
3	Sharing passwords (amongst admins, co-workers, others)
4	Creating weak passwords (use repeated patterns such as keyboard patterns, number or letter patterns, names, meaningful numbers, or dates, etc.)
5	Using default passwords (not changing factory or admin set default passwords)
6	Changing passwords to previously used passwords (cycling among the same password list)

**Table 8***Delphi Round 2 Adjusted PWWAs List (continued)*

<b>PWWA Number</b>	<b>PWWAs</b>
7	No password change when triggered periodically (not changing passwords periodically or when prompted by notification of expiration)
8	No password change when triggered due to an incident (not changing your password after being notified your credentials have of been compromised)
9	No password change when triggered due to an incident (not changing your password after being notified your credentials may have possibly been compromised)
10	Storing passwords physically in the open (office, home, public areas, etc.)
11	Storing passwords physically in a private area (safe, locked office, locked drawer, etc.)
12	Storing passwords digitally in a password vault app/tool/keychain
13	Storing passwords digitally in the browser (clicking “Remember password” in browsers)
14	Storing passwords in draft emails or texts
15	Emailing or texting passwords

*Phase I-Subject Matter Expert (SME) Panel Round 2*

In the second round of the Delphi method, SMEs were solicited via recruitment emails on LinkedIn and forwarding. The goal was also set at 25-30 SMEs, the same as the first round, in which 27 SMEs responded. All 27 SMEs met the requirements to be considered SMEs through one or more: the level of cybersecurity experience, industry IT cybersecurity certifications, or education relating to cybersecurity, making all responses valid. Table 9 provides the descriptive statistics of the 27 participants’ SME criteria. Of the 11 SMEs who were intermediate/experienced level at their organization (40.74%),



eight had one or more advanced IT certifications, and the remaining three had master's degrees. Of the nine SMEs with no IT certifications (33.33%), all nine held a bachelor's degree or higher in IT/Cybersecurity. The two SMEs with no degree in IT/Cybersecurity hold an advanced IT/cybersecurity certification and a supervisor position or above. The SMEs also responded to which sector they had the most IT/cybersecurity experience in, with 18 (66.67%) being government (federal, state, local), two (7.41%) education, two (7.41%) private sector, three (11.11%) mixed sectors, and two (7.41%) other.

**Table 9**

*Descriptive SMEs Criteria (N=27)*

<b>Demographic Item</b>	<b>N</b>	<b>%</b>
<b>Level at Organization:</b>		
Entry Level	0	0
Intermediate/Experienced	11	40.74
Supervisor	6	22.22
Manager	5	18.52
Director/VP	2	7.41
Executive/C-Suite	3	11.11
<b>IT/Cybersecurity Certification:</b>		
Yes	18	66.67
No	9	33.33
<b>Highest degree in IT/Cybersecurity:</b>		
Doctorate	5	18.52
Masters	17	62.96
Bachelors	3	11.11
Associates	0	0
None	2	7.41

*SMEs Results from Delphi*

There were three research questions answered in phase one of this research study. First, SMEs needed to validate the list of PWWA, which were identified in literature. The results on the validation improved drastically from the first round due to the better clarification, reaching consensus on the validation of 12 out of the 15 PWWAs as validated insecure PWWAs that would lead to a data breach (See table 10), thus answering RQ1. The following three PWWAs were not validated with a 75% or greater consensus and removed for the IS User survey and were removed for the main data collection:

1. No password change when triggered periodically (not changing passwords periodically or when prompted by notification of expiration)
2. Storing passwords physically in a private area (safe, locked office, locked drawer, etc.)
3. Storing passwords digitally in a password vault app/tool/keychain

The lack of validation for the three PWWAs suggests that these practices are not widely recognized as deviations from secure password management. PWWA7, no password change when triggered periodically (not changing passwords periodically or when prompted by notification of expiration), might be considered inconvenient, given emerging views that frequent password changes can lead to weaker security and no reason other than policy to change it. PWWA11, storing passwords physically in a private area (safe, locked office, locked drawer, etc.), could be perceived as adequately safe, provided the physical security sufficiently offers a layer of defense. PWWA12, storing passwords digitally in a password vault app/tool/keychain, is often regarded as a

secure practice due to its encryption and security features. Therefore, these practices may likely align with current secure password management standards rather than being regarded as insecure or PWWAs.

**Table 10**

*PWWAs Validation Percentage of Agreement (N=27)*

<b>PWWA Number</b>	<b>PWAAs</b>	<b>% of Agreement</b>
1	Documenting passwords (write down/record on paper, saved in mobile, computer, or other devices)	92.6
2	Reusing the same passwords for multiple accounts	92.6
3	Sharing passwords (amongst admins, co-workers, others)	85.2
4	Creating weak passwords (use repeated patterns such as keyboard patterns, number or letter patterns, names, meaningful numbers, or dates, etc.)	81.5
5	Using default passwords (not changing factory or admin set default passwords)	77.8
6	Changing passwords to previously used passwords (cycling among the same password list)	81.5
7	No password change when triggered periodically (not changing passwords periodically or when prompted by notification of expiration)	55.5

**Table 10***PWWAs Validation Percentage of Agreement (N=27) (continued)*

<b>PWWA Number</b>	<b>PWAAs</b>	<b>% of Agreement</b>
8	No password change when triggered due to an incident (not changing your password after being notified your credentials have of been compromised)	85.2
9	No password change when triggered due to an incident (not changing your password after being notified your credentials may have possibly been compromised)	85.2
10	Storing passwords physically in the open (office, home, public areas, etc.)	77.8
11	Storing passwords physically in a private area (safe, locked office, locked drawer, etc.)	51.9
12	Storing passwords digitally in a password vault app/tool/keychain	37
13	Storing passwords digitally in the browser (clicking “Remember password” in browsers)	81.5
14	Storing passwords in draft emails or texts	81.5
15	Emailing or texting passwords	81.5

Second, to identify the SMEs’ measures for perceived cybersecurity risk of data breach resulting from the validated list of PWWA techniques, the SMEs were asked to identify, on a 7-point Likert scale, their perceived level of risk on how likely each of the validated PWWA would lead to a data breach. A level of agreement of 75% or more was reached on 10 of the remaining 12 PWWA, finalizing the list to 10 total PWWA and

answering RQ2 (See Table 12). The following two were removed based on SMEs' non-consensus as a risk of data breach:

1. Storing passwords digitally in the browser (clicking "Remember password" in browsers)
2. Storing passwords in draft emails or texts

SME's lack of validation on the risks of data breaches associated with these two specific PWWAs from the original list, PWWA13 and PWWA14, could be due to varying perceptions of their security. PWWA13, storing passwords digitally in the browser (clicking "Remember password" in browsers), though convenient, can be considered secure if the browser and device have strong security measures such as encryption. The risk of a breach might be considered low but still significant. PWWA14, the practice of storing passwords in draft emails or texts, might be seen as risky due to possible email account vulnerabilities. However, some might consider it a lower-risk method than more exposed alternatives, leading to mixed opinions among SMEs.

**Table 11**

*SMEs Identified Measure of Perceived Risk of Data Breach on Validated PWWAs (N=27)*

<b>PWWA Number</b>	<b>PWWA</b>	<b>% of Agreement</b>
1	Documenting passwords (write down/record on paper, saved in mobile, computer, or other devices)	77.8
2	Reusing the same passwords for multiple accounts	92.6
3	Sharing passwords (amongst admins, co-workers, others)	88.9

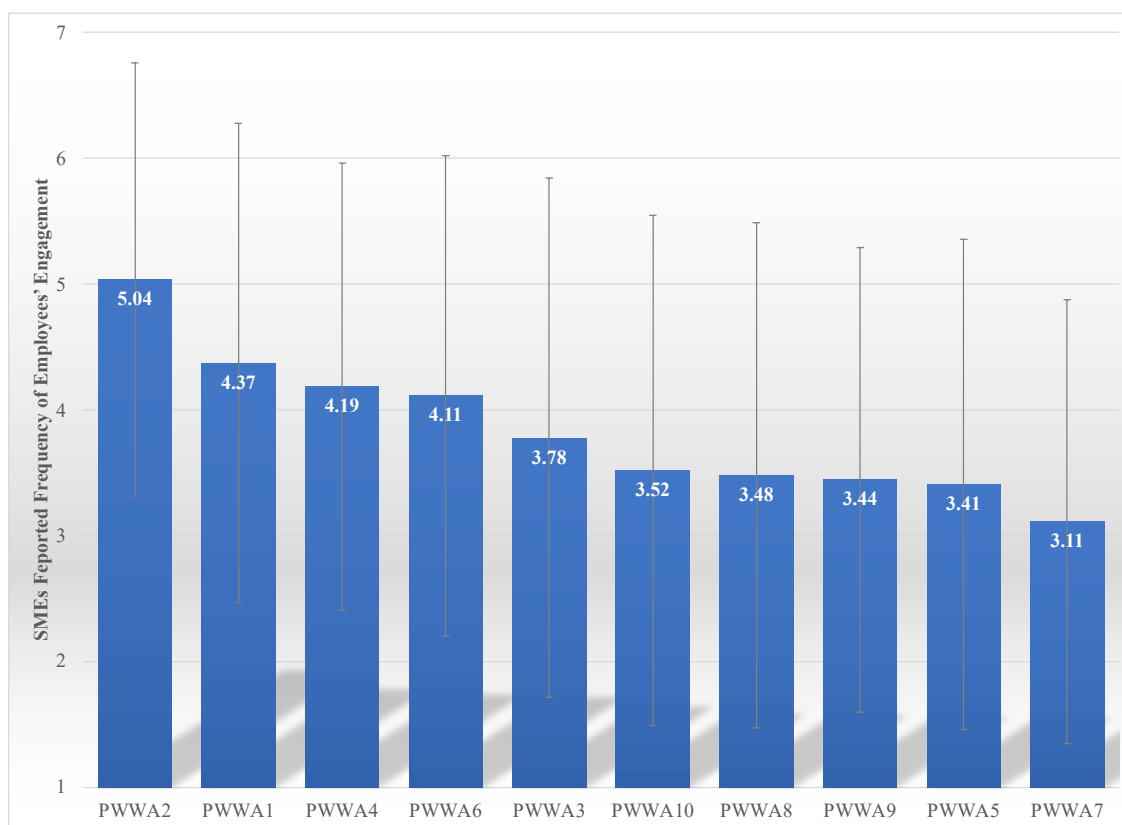
**Table 11***SMEs Identified Measure of Perceived Risk of Data Breach on Validated PWWA (N=27)**(continued)*

<b>PWWA Number</b>	<b>PWWA</b>	<b>% of Agreement</b>
4	Creating weak passwords (use repeated patterns such as keyboard patterns, number or letter patterns, names, meaningful numbers, or dates, etc.)	88.9
5	Using default passwords (not changing factory or admin set default passwords)	96.3
6	Changing passwords to previously used passwords (cycling among the same password list)	77.8
7	No password change when triggered due to an incident (not changing password after being notified of being compromised)	92.6
8	No password change when triggered due to an incident (not changing password after being notified of possible compromise)	85.2
9	Storing passwords physically in the open (office, home, public areas, etc.)	92.6
10	Storing passwords digitally in the browser (clicking “Remember password” in browsers)	51.9
11	Storing passwords in draft emails or texts	63
12	Emailing or texting passwords	77.8

Third, the SMEs (N=27) were asked about the frequency they have observed or are aware of done by co-workers to engage in the use of PWWAs. The study methodology involved analyzing average (AVGSCORE) and standard deviation (STDSCORE) scores. The scores reflected the frequency of reported usage for each technique, with higher scores indicating more frequent usage. For SMEs (N=27), the final validated PWWA techniques (See Table 12), ranked as follows based on their mean scores reported co-workers' engagement in PWWAs usage: the top technique was PWWA 2 (M= 5.04; SD = 1.72). This was followed by PWWA 4 (M= 4.19; SD = 1.78), PWWA 6 (M= 4.11; SD = 1.91), PWWA 1 (M= 4.37; SD = 1.90), PWWA 3 (M= 3.78; SD = 2.06), PWWA 10 (M= 3.52; SD = 2.03), PWWA 8 (M= 3.48; SD = 2.01), PWWA 9 (M= 3.44; SD = 1.85), PWWA 5 (M= 3.41; SD = 1.95), and concluding with PWWA 7 (M= 3.11; SD = 1.76) results can be seen in Figure 3.

**Figure 3**

*SMEs Reported Frequency of Co-worker's Engagement in PWWAs Ranking (N=27)*



The SMEs provided positive feedback on the adjusted questions and survey without further revisions. With the removal of the three PWWAs, which were not successfully validated by SMEs, the IS user survey was ready for the pilot.

### **Phase 2 – Pilot Test**

An additional Round 2 was conducted during the Delphi process due to necessary adjustments based on initial feedback from Round 1 by SMEs. After the completion of Round 2, positive feedback was received from the SMEs, confirming that all adjustments made from Round 1 feedback were sufficient. The IS user survey was then ready to be piloted. Pilot test participants, with the sole requirement of being daily IS users, were randomly solicited via social media and LinkedIn. There were eight participants in this



pilot round, and positive feedback was received, with participants affirming that all questions and responses were clear and understandable. This indicated that no adjustments were required before the main data collection. The IS user survey mirrored the SME survey, except for the following adjustments:

- Removed PWWA validation- this was only for SMEs to validate the PWWA list.
- Removed “What sector do you have/had the most IT/cybersecurity-related experience in?”
- Removed “What is the highest degree in any field related to computing (e.g., information systems, computer science, information technology, computer engineering, cybersecurity) do you hold?”
- Removed “Do you hold a current and active advanced or specialized industry IT/Cybersecurity certification?”
- Three PWWA total were removed from the original list for the IS user survey:
  1. No password change when triggered periodically (not changing passwords periodically or when prompted by notification of expiration)
  2. Storing passwords physically in a private area (safe, locked office, locked drawer, etc.)
  3. Storing passwords digitally in a password vault app/tool/keychain

During the main data analysis, two additional PWWAs were excluded because SMEs did not validate them as practices leading to data breaches, as explored in RQ2:

1. Storing passwords digitally in the browser (clicking “Remember password” in browsers)

## 2. Storing passwords in draft emails or texts

After removing five PWWAs from the original 15, the finalized list of SME-validated PWWAs had been established for the main data analysis after collection. This finalized list is shown in Table 12. Due to the successful consensus achieved in the Delphi round 2 and positive pilot feedback, the survey was ready for main data collection.

**Table 12**

*Finalized SME Validated Adjusted PWWA List*

<b>PWWA Number</b>	<b>PWWA</b>
1	Documenting passwords (write down/record on paper, saved in mobile, computer, or other devices)
2	Reusing the same passwords for multiple accounts
3	Sharing passwords (amongst admins, co-workers, others)
4	Creating weak passwords (use repeated patterns such as keyboard patterns, number or letter patterns, names, meaningful numbers, or dates, etc.)
5	Using default passwords (not changing factory or admin set default passwords)
6	Changing passwords to previously used passwords (cycling among the same password list)
7	No password change when triggered due to an incident (not changing password after being notified of being compromised)
8	No password change when triggered due to an incident (not changing password after being notified of possible compromise)
9	Storing passwords physically in the open (office, home, public areas, etc.)
10	Emailing or texting passwords

### **Phase 3 – Main Data Collection**

In this phase, the primary focus was on sample selection and main data collection, followed by pre-analysis data screening, leading to the main data analysis process and culminating in the development of the PaWoCyRiT. In phase three, the emphasis shifted to recruiting daily IS users for sample selection and completing the primary data collection. This process involved sending an IS user recruitment letter (See Appendix C) and the survey link through well-known social media platforms like LinkedIn and Facebook. Participants were also actively encouraged to share the survey, further facilitating data collection. Utilizing the PWWAs from Table 11, the survey repeatedly employed a 7-point Likert scale to inquire about participants' perceptions of the impact of a data breach associated with each PWWA. The questions also surveyed participants' self-reported engagement frequency and the reported frequency of their co-workers of each PWWA. Demographic information was collected, including age, gender, years of experience in the IS field, cybersecurity awareness training/experience, organizational level, and the number of managed password accounts. The main data collection phase concluded with 307 IS user participant responses, surpassing the initial target of 300 responses. Upon completing the sample selection and primary data collection, a pre-analysis data screening was conducted to ensure the data's reliability and to detect multivariate outliers (Levy, 2008). This pre-analysis utilized the Mahalanobis Distance to analyze for perfect response patterns. Based on this preliminary analysis, four data sets were excluded from the study. Among these, three were removed due to being perfect responses (data points 26, 27, and 74), and one outlier (data point 142) was identified using the Mahalanobis Distance method. The data set was then partitioned into group one IS Users and group two SMEs, with three distinct measure types considered. Measure

type one encompassed the reported perceived level of risk associated with data breaches for each PWWA technique. Measure type two addressed the reported engagement of co-workers, whether through observation or awareness of the technique being implemented. Finally, measure type three captured the self-reported frequency of use for each PWWA technique. Now that the pre-analysis phase has concluded, the main data analysis can proceed, addressing the remaining research questions: RQ4, RQ5, RQ6, RQ7, RQ8, RQ9, and RQ10.

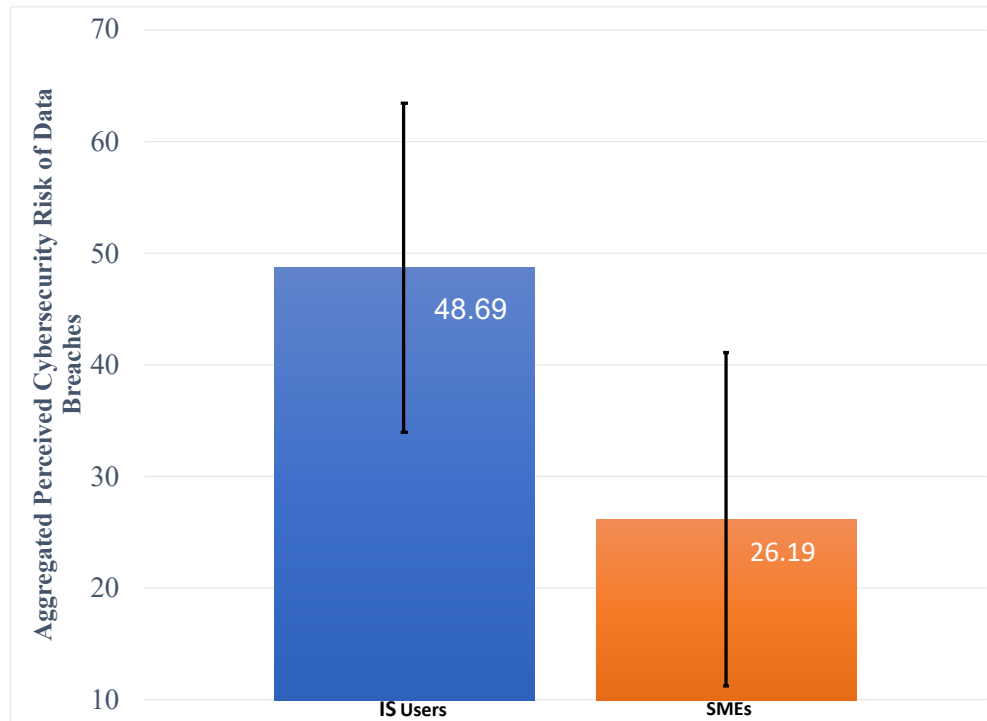
#### *Main Data Collection- Research Questions*

For RQ4, the analysis of IS users (group one) data using the perceived level of data breach (measure type one) involved obtaining the aggregated score for each IS user response across all 10 validated PWWAs, followed by calculating the average of the aggregated score and the standard deviation of all 303 IS Users responses. This process created a bar chart (refer to Figure 4) visually representing employees' aggregated perceived cybersecurity risk of data breaches associated with the PWWA techniques. The chart also displays SMEs (group two) aggregated scores for a visual. Later in the research, the aggregated data of the perceived level of data breach (measure type one) for both IS users (group one) and SMEs (group two) was compared using an Analysis of Variance (ANOVA) in SPSS 29.

**Figure 4**

*IS Users and SMEs Aggregated Perceptions of PWWAs Will Lead to Data Breach*

(N=330)



RQ5 focused on analyzing the SMEs (group two) data, employing the same methodology to obtain the aggregated scores from the IS users' data across all 10 PWWAs. Average and standard deviation scores were calculated for all SMEs (N=27) aggregated scores. Then, SPSS was used to compare these findings with those from RQ4. This research question aimed to find if there were any statistically significant mean differences in employees' aggregated perceived level of risk resulting from each validated PWWA technique, as compared to the perceived risk levels indicated by the SMEs. Using ANOVA, a p-value less than 0.05 is typically considered evidence of a significant difference between groups. Several key observations emerge in examining the differences in perceived cybersecurity risks between IS Users and SMEs across the 10

PWWA techniques. There is no statistically significant difference in perception between the two groups for PWWA1 with a p-value of 0.137 and PWWA2 with a p-value of 0.590. This suggests that IS users and SMEs share similar viewpoints regarding potential cybersecurity risks for these techniques. However, the data indicates evident differences in perceptions of other techniques. PWWA3 stands out with a p-value of 0.001, signaling a robust statistically significant difference between the groups. This disparity suggests that IS users and SMEs have notably different perceptions concerning the cybersecurity risks associated with PWWA3. Similar patterns of significant differences in perception are also evident for PWWA4 ( $p = 0.014$ ), PWWA5 ( $p < 0.001$ ), PWWA7 ( $p = 0.008$ ), PWWA8 ( $p = 0.012$ ), PWWA9 ( $p < 0.001$ ), and PWWA10 ( $p = 0.022$ ). Each of these PWWAs exhibits a p-value less than 0.05, traditionally considered the threshold for statistical significance.

However, not all techniques show this divergence. For instance, PWWA6, with a p-value of 0.179, indicates no significant difference in perceptions between the groups, aligning more with the patterns seen in PWWA1 and PWWA2.

**Table 13**

*ANOVA Differences in Perceived Cybersecurity Risk of Data Breaches (N=330)*

<b>PWWA Techniques</b>	<b>Sum of Squares (Between Groups)</b>	<b>df (Between Groups)</b>	<b>Mean Square (Between Groups)</b>	<b>F-value</b>	<b>Sig. (p-value)</b>
PWWA1	6.913	1	6.913	2.227	0.137
PWWA2	0.657	1	0.657	0.291	0.590
PWWA3	56.313	1	56.313	10.429	<b>0.001**</b>
PWWA4	21.187	1	21.187	6.065	<b>0.014*</b>
PWWA5	95.775	1	95.775	21.036	<b>&lt;0.001***</b>
PWWA6	5.385	1	5.385	1.813	0.179
PWWA7	32.161	1	32.161	7.140	<b>0.008**</b>

\* -  $p < .05$ , \*\* -  $p < .01$ , \*\*\* -  $p < .001$

**Table 13**

*ANOVA Differences in Perceived Cybersecurity Risk of Data Breaches (N=330)*

*(continued)*

<b>PWWA Techniques</b>	<b>Sum of Squares (Between Groups)</b>	<b>df (Between Groups)</b>	<b>Mean Square (Between Groups)</b>	<b>F-value</b>	<b>Sig. (p-value)</b>
PWWA8	25.764	1	25.764	6.309	<b>0.012*</b>
PWWA9	75.596	1	75.596	15.510	<b>&lt;0.001***</b>
PWWA10	24.609	1	24.609	5.316	<b>0.022*</b>

\* -  $p < .05$ , \*\* -  $p < .01$ , \*\*\* -  $p < .001$

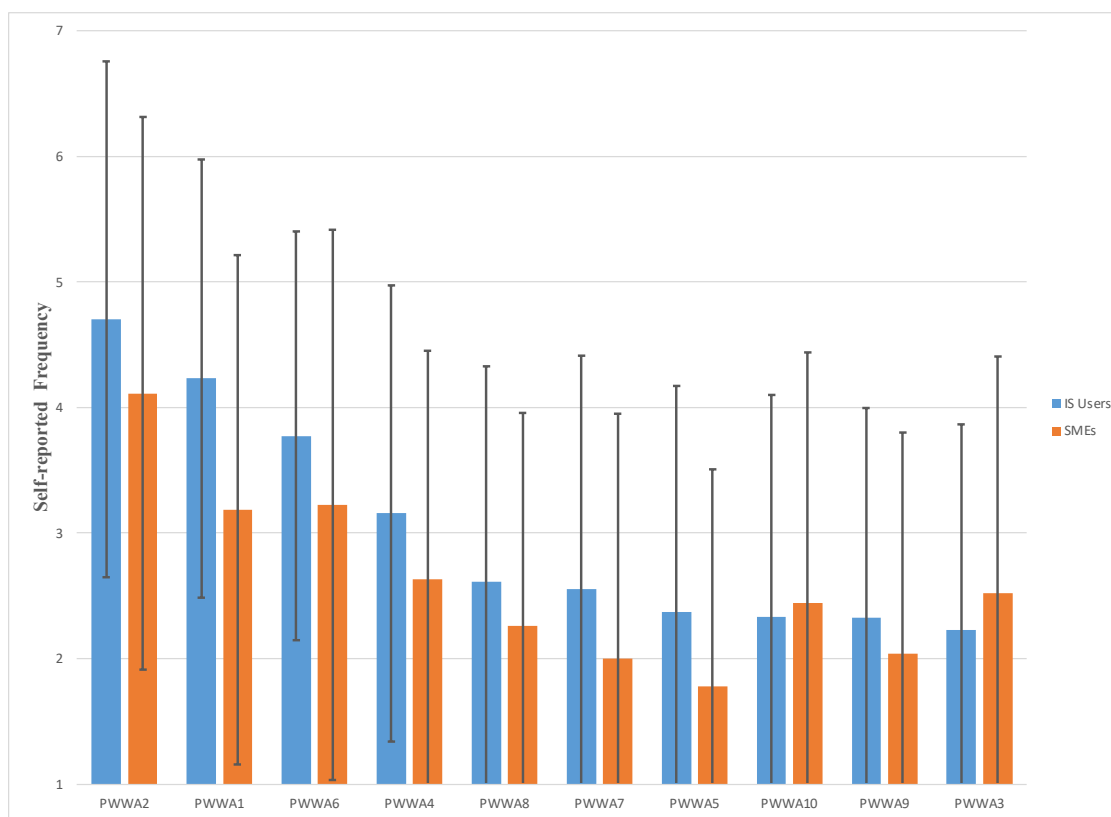
RQ6 was focused on analyzing the PWWA techniques reported by IS users (group one) and SMEs (group two), specifically based on their self-reported engagement (measure type three). The main components of the analysis included calculating the mean and standard deviation of the self-reported frequencies of each PWWA technique. For IS Users, the results highlighted the prominence of PWWA 2 (M= 4.70; SD = 1.74) as the predominant technique utilized. This was closely shadowed by PWWA 1 (M= 4.23; SD = 2.06) and then PWWA 6 (M= 3.77; SD = 1.86). The remaining techniques, PWWA 3 (M= 2.23; SD = 1.63), PWWA 4 (M= 3.16; SD = 1.82), PWWA 5 (M= 2.37; SD = 1.72), PWWA 7 (M= 2.55; SD = 1.80), PWWA 8 (M= 2.61; SD = 1.77), PWWA 9 (M= 2.32; SD = 1.67), and PWWA 10 (M= 2.33; SD = 1.63) revealed average scores ranging from 2.23 to 3.16 with associated standard deviations reflecting diverse consistency levels within the IS users' data.

PWWA 2 (M= 4.11; SD = 2.03) emerged as SMEs' most frequently reported used technique. PWWA 1 (M= 3.19; SD = 2.20) and PWWA 6 (M= 3.22; SD = 1.95) were observed next in line regarding frequency. The subsequent techniques, PWWA 3 (M= 2.52; SD = 2.19), PWWA 4 (M= 2.63; SD = 1.82), PWWA 5 (M= 1.78; SD = 1.69),

PWWA 7 (M= 2.00; SD = 1.73), PWWA 8 (M= 2.26; SD = 1.99), PWWA 9 (M= 2.04; SD = 1.76), and PWWA 10 (M= 2.44; SD = 1.89), showed average scores between 1.78 and 2.63 with their corresponding standard deviations, again signifying a range of engagement levels in the SMEs. A graph (See Figure 5) was generated to aid in visualizing the data. Additionally, the PWWA techniques were ranked in descending order of frequency of engagement by IS users.

### Figure 5

*SMEs and IS Users Self-reported Frequency Use of PWWAs (N=330)*



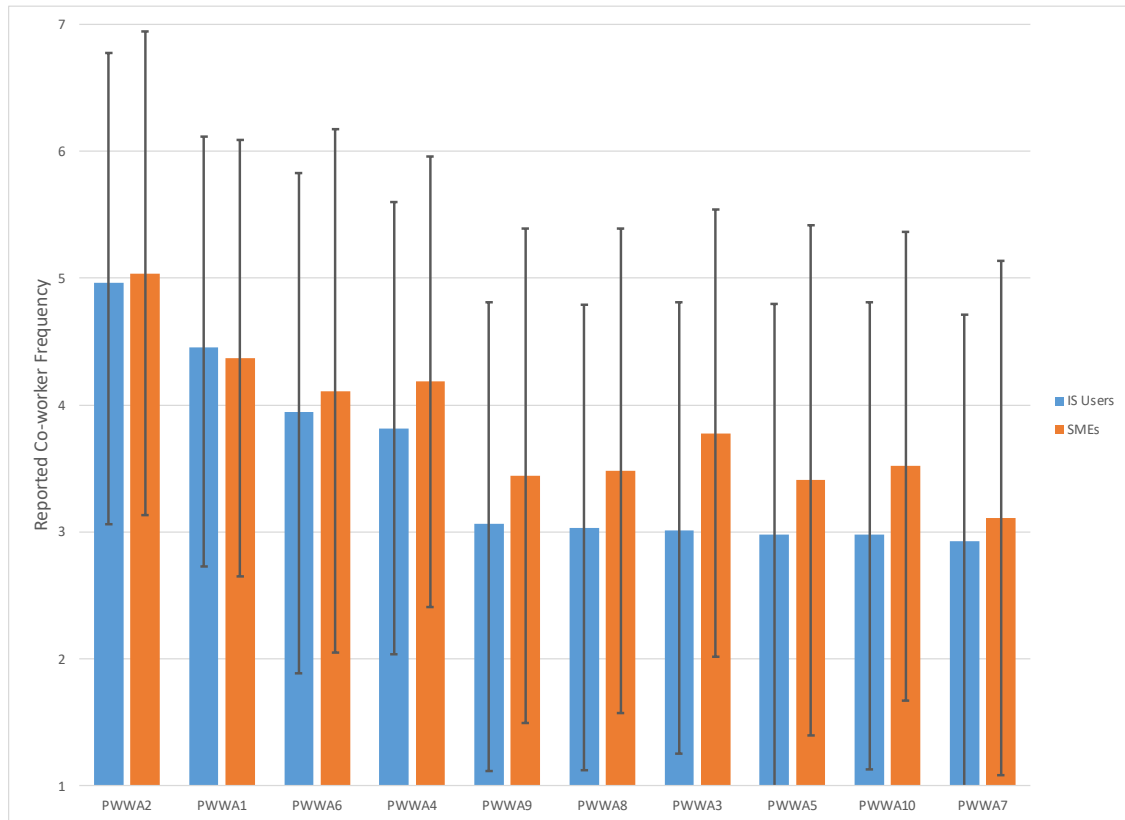
RQ7 utilized a similar technique as RQ6 but with a distinction in the data source. Instead of self-reported data (measure type three), it relied on the reported frequency of PWWA techniques as indicated by IS users (group one), specifically regarding the frequency of their co-workers' engagement (measure type two) in these techniques. The



key components of the analysis encompassed calculating the mean and standard deviation of the reported frequencies for each PWWA technique based on SMEs and IS users' observations of their co-workers. The IS user data showed the following trend: PWWA 2 was identified as the top technique reported (M= 4.97; SD = 1.66), followed by PWWA 1 (M= 4.45; SD = 1.81), PWWA 6 (M= 3.95; SD = 1.76), PWWA 4 (M= 3.82; SD = 1.78), PWWA 3 (M= 3.01; SD = 1.88), PWWA 8 (M= 3.03; SD = 1.82), PWWA 9 (M= 3.06; SD = 1.83), with PWWA 5 and PWWA 10 both having similar scores (M= 2.98; SD = 1.75 for PWWA 5 and SD = 1.79 for PWWA 10) and PWWA 7 (M= 2.93; SD = 1.80). Furthermore, the findings were structured by ranking the PWWA techniques based on the frequency reported by IS users regarding their co-workers' use. These rankings were then compared with the SMEs' data from RQ3 (See Figure 3) and presented in Figure 6.

**Figure 6**

*SMEs and IS Users Reported Frequency of Co-worker Engagement in PWWAs (N=330)*



RQ8 aimed to identify statistically significant differences between SMEs (group two) and employees' (group one) self-reported frequency engagement (measure type three) and reported frequency of co-workers' engagement (measure type two) in PWWA techniques. For the first part of this study, a One-Way ANOVA, executed in SPSS, was used to compare IS users (group one) and SMEs (group two) self-reported engagement (measure type three) in PWWAs; the data revealed a statistically significant difference only for PWWA1 ( $p = 0.012$ ). For all other PWWAs (PWWA2 to PWWA10), there were no significant differences between the two groups, with p-values all exceeding the 0.05 threshold.

**Table 14**

*ANOVA Analysis of SMEs and IS Users Self-reported PWWA Usage Frequency*

*Differences (N=330)*

<b>PWWA</b>	<b>Sum of Squares</b>	<b>df</b>	<b>Mean Square</b>	<b>F-value</b>	<b>Significance</b>
PWWA1	27,116	1	27,116	6,344	<b>0.012*</b>
PWWA2	8,684	1	8,684	2,776	0.097
PWWA3	2,049	1	2,049	0,727	0.395
PWWA4	6,932	1	6,932	2,100	0.148
PWWA5	8,781	1	8,781	2,983	0.085
PWWA6	7,501	1	7,501	2,162	0.142
PWWA7	7,621	1	7,621	2,370	0.125
PWWA8	3,060	1	3,060	0,955	0.329
PWWA9	2,033	1	2,033	0,721	0.396
PWWA10	0,325	1	0,325	0,119	0.731

\* -  $p < .05$ , \*\* -  $p < .01$ , \*\*\* -  $p < .001$

For the second part of RQ8, the significant differences in the reported co-worker frequency (measure type two) of PWWAs between IS users (group one) and SMEs (group two), ANOVA was run on the validated 10 PWWAs. The majority of these, specifically PWWA1, PWWA2, PWWA4, PWWA5, PWWA6, PWWA7, PWWA8, PWWA9, and PWWA10, did not exhibit statistically significant differences between the groups, indicating a broad similarity in the reported frequencies between IS users and SMEs for these PWWAs (p-values ranging from 0.136 to 0.835). However, a notable exception was observed in the case of PWWA3, where a significant difference was identified with a p-value of 0.045, which falls below the conventional threshold of 0.05 for statistical significance. The results suggest that, for PWWA3, there exists a meaningful discrepancy in the reported frequencies between the two groups, necessitating further exploration to understand the underlying causes of this variance.

**Table 15***ANOVA Analysis of Co-worker PWWA Usage Reported Frequency Differences (N=330)*

<b>PWWA</b>	<b>Sum of Squares</b>	<b>df</b>	<b>Mean Square</b>	<b>F-value</b>	<b>Significance</b>
PWWA1	0.166	1	0.166	0.050	0.823
PWWA2	0.122	1	0.122	0.044	0.835
PWWA3	14.492	1	14.492	4.040	<b>0.045*</b>
PWWA4	3.394	1	3.394	1.067	0.302
PWWA5	4.525	1	4.525	1.457	0.228
PWWA6	0.666	1	0.666	0.212	0.646
PWWA7	0.837	1	0.837	0.260	0.610
PWWA8	5.060	1	5.060	1.507	0.221
PWWA9	3.613	1	3.613	1.073	0.301
PWWA10	7.272	1	7.272	2.230	0.136

\* - p&lt;.05, \*\* - p&lt;.01, \*\*\* - p&lt;.001

RQ9 involved conducting an Analysis of Covariance (ANCOVA) using SPSS to investigate whether there are statistically significant differences in the perceived level of cybersecurity risk related to data breaches resulting from each validated PWWA technique based on several demographic factors. The analysis considered the following demographic factors: (a) age, (b) gender, (c) years of computer experience, (d) years of cyber awareness training, and (e) job level for SMEs (N=27) and IS users (N=303).

**Table 16***Descriptive Statistics of the IS Users (N=303)*

<b>Demographic Item</b>	<b>N</b>	<b>Percentage (%)</b>
<b>Gender</b>		
Male	74	24.4%
Female	228	75.2%
Non-binary /Third gender	1	0.3%

**Table 16***Descriptive Statistics of the IS Users (N=303) (continued)*

<b>Demographic Item</b>	<b>N</b>	<b>Percentage (%)</b>
<b>Age</b>		
18-30	215	71%
31-40	50	16.5%
41-50	28	9.2%
51-60	6	2.0%
61 or older	4	1.3%
<b>Number of Years of IS Experience</b>		
Less than 1	5	1.7%
1 to 4	21	6.9%
5 to 10	74	24.4%
11 to 15	86	28.4%
16 to 20	64	21.1%
21 to 25	35	11.6%
26 to 30	8	2.6%
More than 30	10	3.3%
<b>Number of Years of Cybersecurity Awareness Training</b>		
Less than 1	127	41.9%
1 to 4	88	29%
5 to 10	51	16.8%
11 to 15	19	6.3%
16 to 20	11	3.6%
21 to 25	5	1.7%
26 to 30	2	0.7%
More than 30	0	0%
<b>Level at Organization</b>		
Entry Level	152	50.2%
Intermediate/Experienced	96	31.7%
Supervisor	18	5.9%
Manager	25	8.3%
Director/VP	9	3%
Executive/C-Suite	3	1%

**Table 17***Descriptive Statistics of the SMEs (N=27)*

<b>Demographic Item</b>	<b>N</b>	<b>Percentage (%)</b>
<b>Gender</b>		
Male	20	74.1%
Female	6	22.2%
Non-binary /Third gender	1	3.7%
<b>Age</b>		
18-30	1	3.7%
31-40	5	18.5%
41-50	11	40.7%
51-60	10	37%
61 or older	0	0%
<b>Number of Years of IS Experience</b>		
Less than 1	0	0%
1 to 4	0	0%
5 to 10	0	0%
11 to 15	1	3.7%
16 to 20	3	11.1%
21 to 25	4	14.8%
26 to 30	2	7.4%
More than 30	17	63%
<b>Number of Years of Cybersecurity Awareness Training</b>		
Less than 1	1	3.7%
1 to 4	3	11.1%
5 to 10	3	11.1%
11 to 15	2	7.4%
16 to 20	7	25.9%
21 to 25	6	22.2%
26 to 30	3	11.1%
More than 30	2	7.4%

**Table 17***Descriptive Statistics of the SMEs (N=27) (continued)*

<b>Demographic Item</b>	<b>N</b>	<b>Percentage (%)</b>
<b>Level at Organization</b>		
Entry Level	0	0%
Intermediate/Experienced	11	40.7%
Supervisor	6	22.2%
Manager	5	18.5%
Director/VP	2	7.4%
Executive/C-Suite	3	11.1%

For this data analysis, the perceived level of cybersecurity risk of data breaches

(measure type one) as reported by IS users (group one) and SMEs (group two) for each validated PWWA technique was utilized. For SMEs, analysis indicates that only years of IS experience significantly affect the perceived level of cybersecurity risk associated with each PWWA technique ( $p = 0.002$ ). Age ( $p = 0.374$ ), gender ( $p = 0.100$ ), years of cyber awareness training ( $p = 0.145$ ), and job level ( $p = 0.402$ ) did not present statistically significant differences in perception.

**Table 18***ANCOVA Results for SMEs Perceived Cybersecurity Risk Based on Demographics**(N=27)*

<b>Demographic Variables</b>	<b>Type III Sum of Squares</b>	<b>df</b>	<b>Mean Square</b>	<b>F-value</b>	<b>Significance (p-value)</b>
AGE	0.091	1	0.091	0.822	0.374
GENDER	0.326	1	0.326	2.944	0.100
IS_EXP	1.302	1	1.302	11.759	<b>0.002**</b>
CYSECEXP	0.253	1	0.253	2.287	0.145
JOBLEVL	0.081	1	0.081	0.729	0.402

\* -  $p < .05$ , \*\* -  $p < .01$ , \*\*\* -  $p < .001$

For IS Users, there are distinct differences based on gender ( $p < 0.001$ ), years of computer experience ( $p < 0.001$ ), and job level ( $p < 0.001$ ). All these demographics show

statistically significant variations in the perceived level of cybersecurity risk linked to the PWWA techniques. Age, with a p-value of 0.083, is on the border of significance, whereas years of cyber awareness training ( $p = 0.468$ ) did not show any significant effect.

**Table 19**

*ANCOVA Results for IS Users Perceived Cybersecurity Risk Based on Demographics*

( $N=303$ )

Demographic Variables	Type III Sum of Squares	df	Mean Square	F-value	Significance (p-value)
AGE	0.105	1	0.105	3.021	0.083
GENDER	17.558	1	17.558	504.434	<0.001**
IS_EXP	2.020	1	2.020	58.037	<0.001**
CYSECEXP	0.018	1	0.018	0.528	0.468
JOBLEVL	1.203	1	1.203	34.558	<0.001**

\* -  $p < .05$ , \*\* -  $p < .01$ , \*\*\* -  $p < .001$

RQ10 aimed to utilize all the data (measure type one, two, and three) from IS users (group one) and SMEs (group two) to calculate the aggregated score of perceived cybersecurity risk of data breaches resulting from the PWWA techniques. This involved utilizing all the datasets to capture the reported perception of the risk associated with data breaches for each PWWA technique and the reported frequency of PWWA techniques' usage as self-reported (measure type three) and observed co-worker engagement (measure type three). By developing a PaWoCyRiT, each PWWA technique was positioned based on its level of perceived cybersecurity risk and reported frequency of usage, leading to the development of the PaWoCyRiT framework. This research study culminated in developing five distinct PaWoCyRiTs, methodically designed to display the particulars of PWWA techniques based on perceived cybersecurity risk and reported frequency. These PaWoCyRiTs drew insights from IS Users and SMEs. The analytical



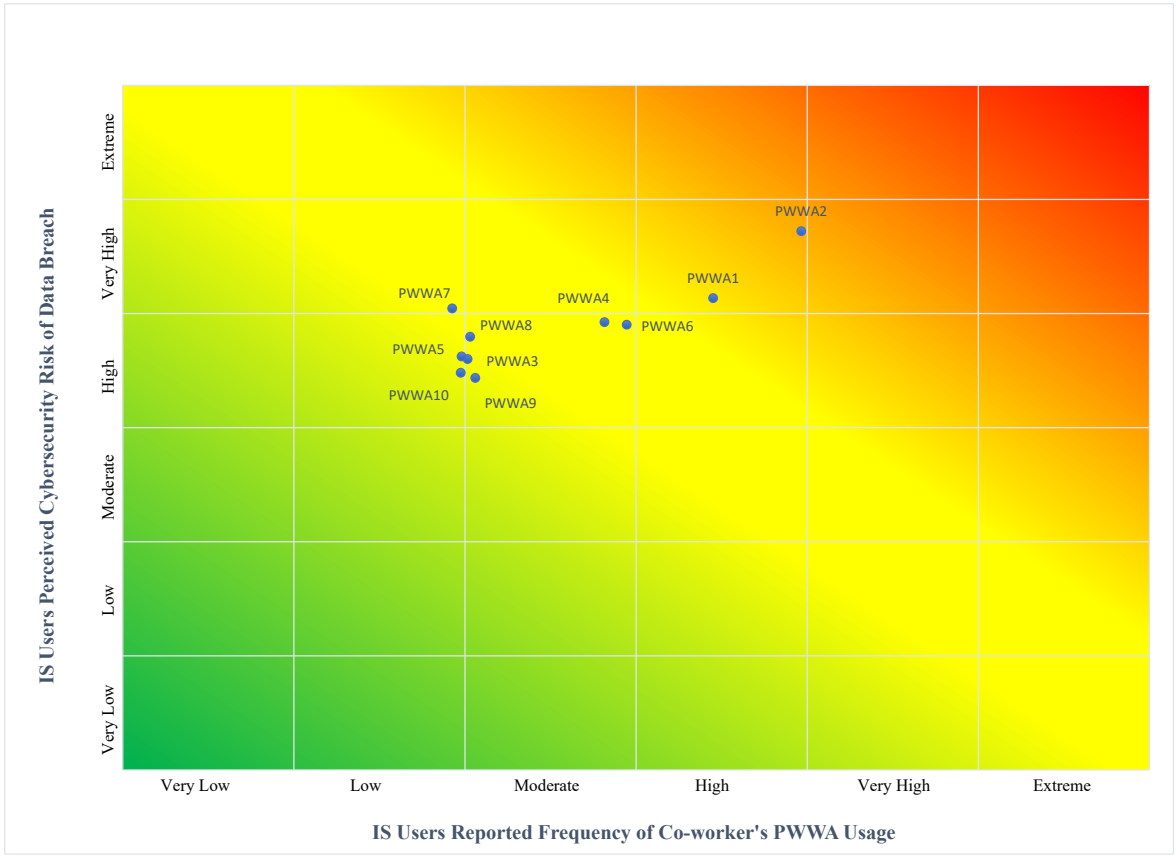
lens was a risk scale spanning from 1-7, with classifications encapsulated and placed on an X and Y axis of the PaWoCyRiT as Very Low (1-2), Low (2-3), Moderate (3-4), High (4-5), Very High (5-6), and Extreme (6-7).

The first PaWoCyRiT (See Figure 7) centered on IS users' responses based on their reported frequency of co-workers' use of each PWWA (measure type two) and the perceived level of cybersecurity risk of data breach that each PWWA poses (measure type one). Regarding perceived risks, PWWA techniques such as PWWA1, PWWA2, and PWWA7 emerged as Very High. Meanwhile, other techniques were predominantly placed within the High-risk category. The placement shifted slightly when data from the reported frequency of co-worker usage was observed, which presented a spectrum ranging from Low to High.

**Figure 7**

*PaWoCyRiT IS Users' Perceived Cybersecurity Risk and Reported Co-workers' Frequency*

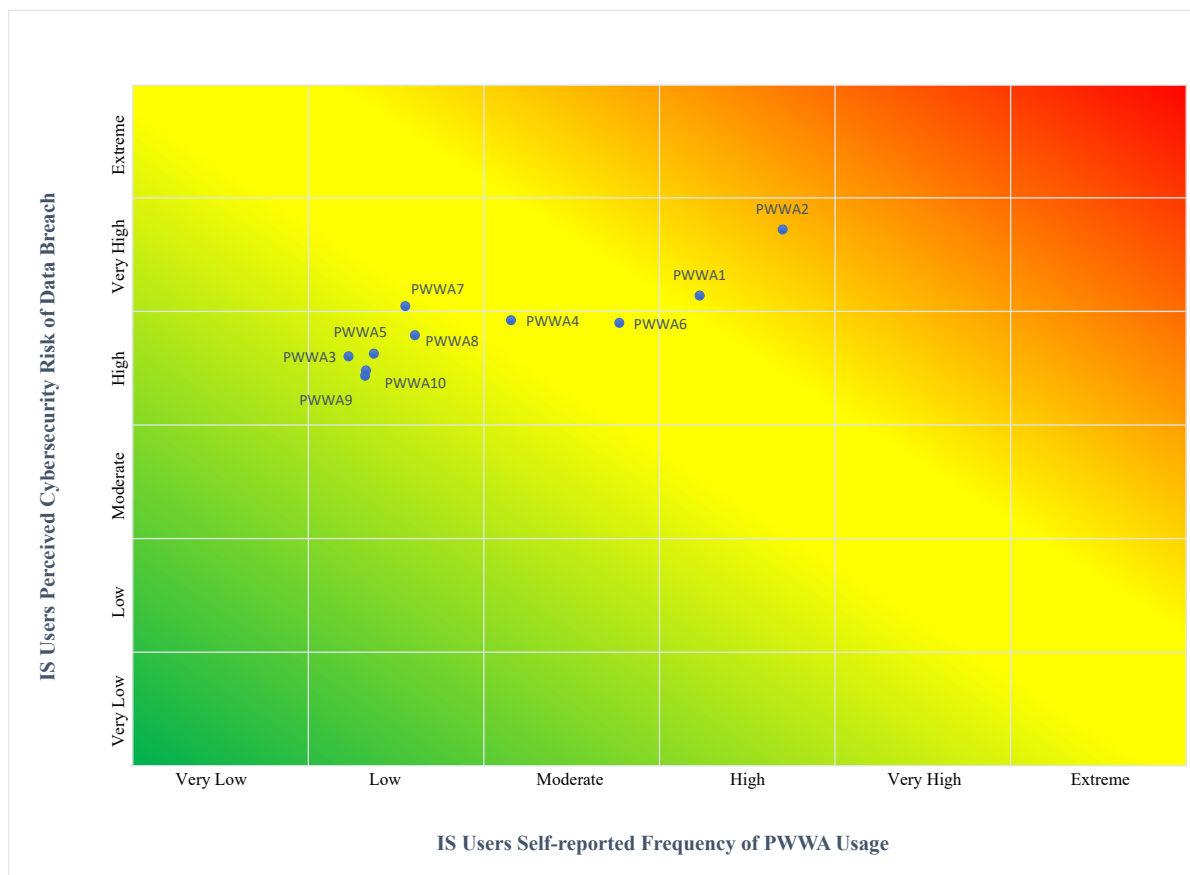
*Frequency*



The second PaWoCyRiT (See Figure 8) still revolved around IS users but compared their perceived level of cybersecurity risk of a data breach for each PWWA against self-reported frequency of engagement. Four techniques (PWWA1, PWWA2, PWWA4, and PWWA6) displayed Moderate to High self-engagement tendencies while perceived as having a High or Very High cybersecurity risk of data breach.

**Figure 8**

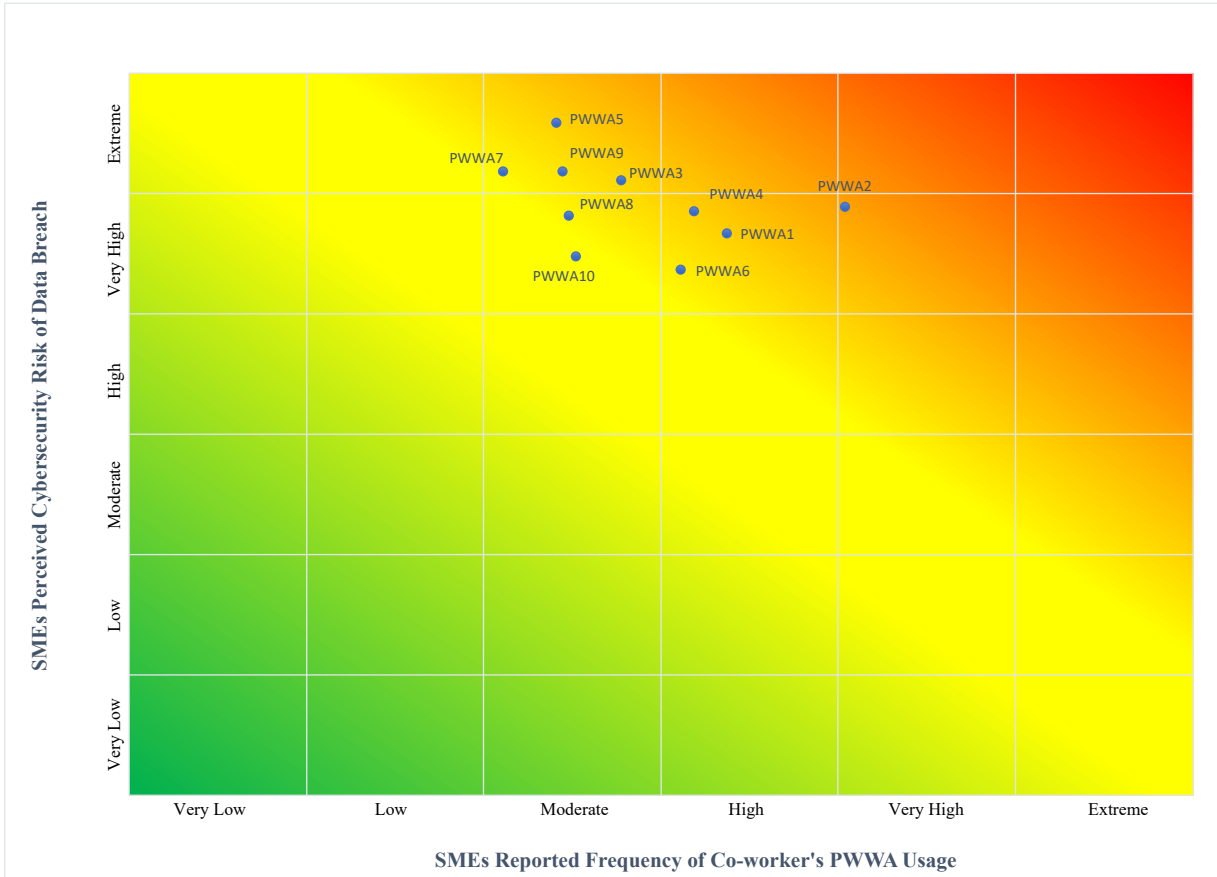
*PaWoCyRiT IS Users Perceived Cybersecurity Risk and Self-reported Frequency*



The comprehension accumulated as the focus was shifted to the third PaWoCyRiT (See Figure 9), focusing on SMEs. The SME's perceptions predominantly tilted towards the Very High to Extreme risk categories. Techniques like PWWA3, PWWA5, PWWA7, and PWWA9 perception of cybersecurity risk of data breach were categorized as Extreme. When analyzing the SMEs' reported frequency of co-worker usage, patterns largely indicated Very High frequent engagement for PWWA2, High usage for some techniques like PWWA1, PWWA4, and PWWA6, and Moderate usage for the rest.

**Figure 9**

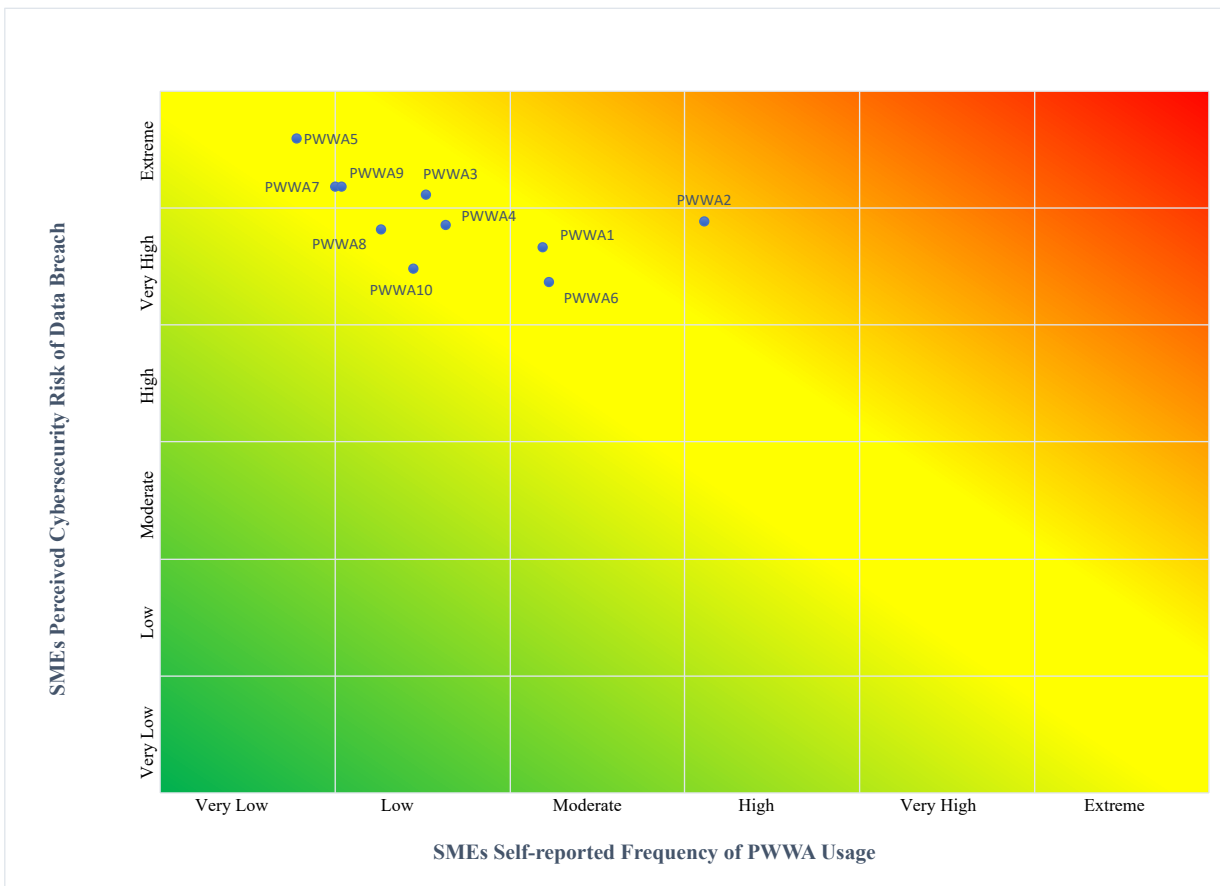
*PaWoCyRiT SMEs Perceived Cybersecurity Risk and Reported Co-workers Frequency*



The fourth PaWoCyRiT (See Figure 10) also utilized the SME group but contrasted with each PWWA technique’s self-reported engagement frequency. Techniques labeled as Very High or Extreme risks, including PWWA1, PWWA2, and PWWA6, often paralleled with Moderate to High self-usage frequencies while the rest were in the very low to low frequency.

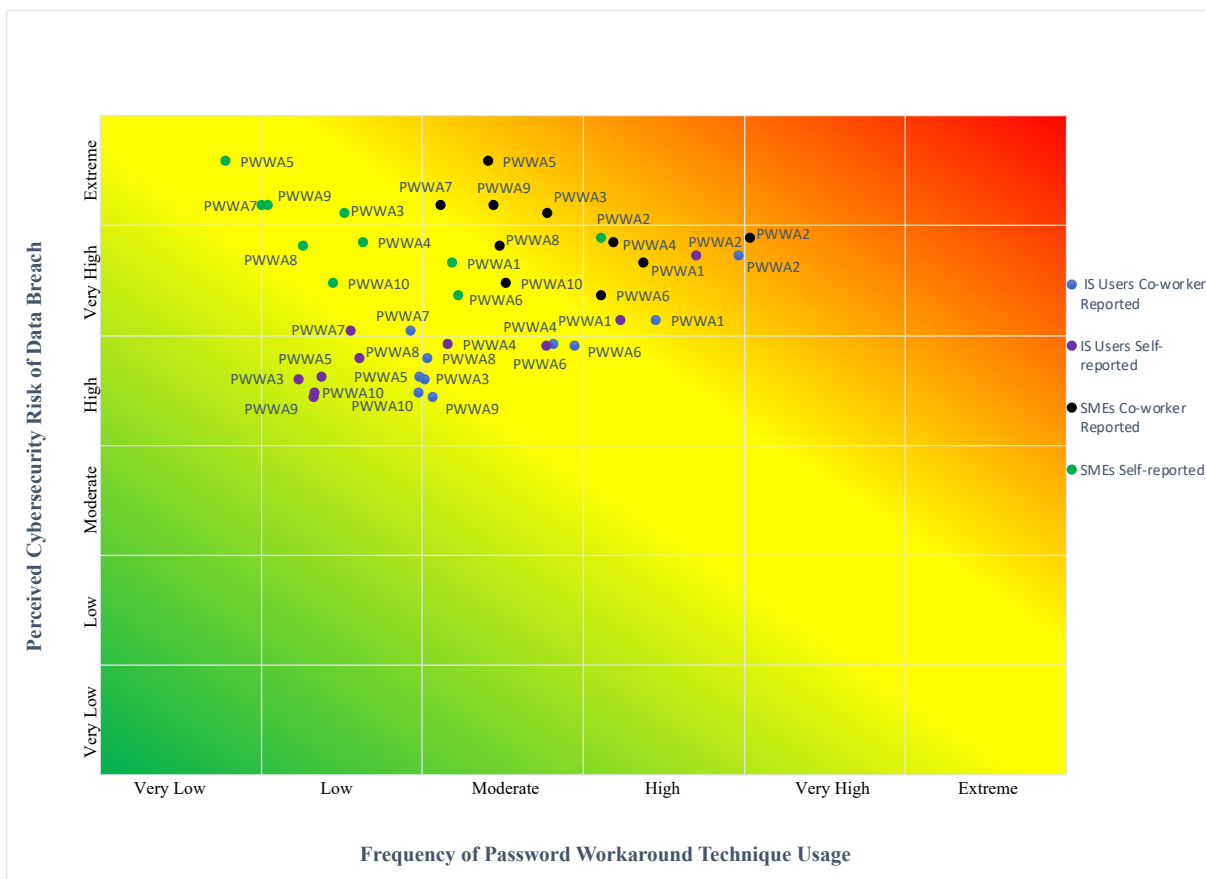
**Figure 10**

*PaWoCyRiT SMEs Perceived Cybersecurity Risk and Self-reported Frequency*



The fifth and final PaWoCyRiT (See Figure 11) combined all the previous four data points. Merging data from all previous PaWoCyRiTs, this synthesis underscored several relevant observations. Bridging these PaWoCyRiTs highlighted the ongoing strain between knowledge of potential cybersecurity risks associated with PWWAs and their actual frequency of use. This contrast compels a reassessment of current cybersecurity education paradigms and probes deeper into the human dimensions that mold cybersecurity behaviors, whether among novices or experts.

Figure 11

*PaWoCyRiT*

### Summary

The Delphi method effectively developed a validated list of 10 PWWAs. An analysis between SMEs and IS users revealed a significant difference in the perceived level of cybersecurity risk for seven PWWAs. Particularly, when aggregated, the IS users generally perceived a higher cybersecurity risk of the PWWAs than the SMEs. Rankings for both groups highlighted a distinct inclination for PWWA2, though differences in scores for other PWWAs like PWWA1 and PWWA6 suggested subtle measures of engagement among participants. A deviation in reported co-worker PWWA engagement was observed between SMEs and IS users. Statistically significant differences in self-

reported engagement occurred for PWWA1 and reported co-worker engagement for PWWA3. Demographic analysis indicated that only years of IS experience affected perceived risk among SMEs, while gender, years of IS experience, and job level influenced IS users' perceptions. Following, the development of the PaWoCyRiT model resulted in five variants, providing detailed perceived cybersecurity risk and self-reported and reported co-worker frequency assessments for both SMEs and IS user groups. SMEs perceived a heightened risk level, categorizing PWWA3, PWWA5, PWWA7, and PWWA9 as Extreme risk. Comparatively, IS users identified PWWA1 and PWWA2 under Very High risk and frequency. An overarching PaWoCyRiT incorporated all findings for an integrated comparison.

## Chapter 5

### Conclusions, Discussions, Implications, Recommendations, and Summary

#### **Conclusions**

Authentication is crucial for data privacy and security. However, various methods exist, from biometrics to token devices offering different levels of security; text-based passwords remain prevalent due to their user-friendly attributes (Güven et al., 2022). In recent years, the risk of data breaches has escalated, affecting businesses severely; such breaches, more severe than mere system intrusions, threaten data integrity, confidentiality, and availability (Du et al., 2022). Despite understanding password policies, individuals often favor bypassing organizational policies (Siponen et al., 2020). A significant portion of breaches were due to hacking, and a majority of these hacking breaches involved misplaced/stolen or brute-forced credentials (Verizon, 2020). Thus, the main goal of this research study aimed to design, develop, and empirically validate the PaWoCyRiT using the constructs of users' perceived cybersecurity risk of data breaches resulting from PWWA techniques and frequency of PWWA techniques usage. 10 specific goals were established, and a three-phase research methodology was utilized to achieve this main goal. First, using the Delphi method, an expert panel of SMEs was used to validate the original list of PWWAs found in literature to develop a reliable and valid list. Through the Delphi method, the SMEs also established identified measures, or their perceived level of cybersecurity risk each technique posed, to further validate the list of PWWA. The last part of the Delphi method involved the SMEs reporting their self-engagement and co-workers' engagement in each PWWA technique, completing phase one. In phase two, a brief pilot was undertaken to validate the survey instruments;



however, the pilot was utilized more as a preliminary test than a comprehensive evaluation due to the initiation of a second round of the Delphi method. Phase three involved the main data collection and analysis and concluded with the development of the PaWoCyRiT.

## **Discussions**

First, this study successfully identified a comprehensive list of validated PWWAs through the Delphi method. In the initial Delphi round, feedback from SMEs expanded the preliminary list of PWWAs found in the literature. During the second round, the SMEs further refined this list by validating the combined list from literature and feedback from the first Delphi round and assessing the perceived risk of each PWWA, eventually narrowing it down to 10 final PWWAs. Then, for comparison, their reported frequency of co-worker use and self-reported use of each PWWA. IS users then identified their perceived level of cybersecurity risk of a data breach for each validated PWWA and their reported frequency of co-worker use and self-use of each PWWA.

Both data sets, SMEs and IS users, were compared to see if there were differences between their aggregated perceived level of cybersecurity risk of a data breach for each PWWA. Individually, for the perceived level of cybersecurity risk of data breach for each PWWA, there were significant differences found for PWWA3, PWWA4, PWWA5, PWWA7, PWWA8, PWWA9, PWWA10. In an overall comparison, the IS users had a higher aggregated perceived level of cybersecurity risk of data breach when compared to the SMEs. Next, SMEs and IS users' most frequently self-reported engagement in PWWA techniques were compared. A significant takeaway from the ranking analysis is the consistent inclination towards PWWA2 across SMEs and IS users, suggesting a potential collective appeal or efficacy inherent to this technique. However, it is essential

to emphasize that while PWWA1 and PWWA6 emerged prominently within both groups after PWWA2, the variability in their scores—especially visible among SMEs—suggests obscure subtleties and measurements of engagement, demanding further research to interpret the underlying determinants.

When comparing IS users' reported co-worker frequency of engagement of PWWAs with the ranking of the SMEs' reported co-worker frequency engagement of PWWAs techniques from RQ3, it is noteworthy that both groups also gravitated towards PWWA2. Though, the other reported PWWA techniques usage varies between SMEs and IS users. Next, SMEs and IS users self-reported and reported co-worker engagement were compared for significant statistical differences. For self-reported engagement, only PWWA1 showed a significant difference, while for co-workers who reported frequency engagement, PWWA3 showed a statistical difference. After, another statistical analysis was done on the demographics of both groups to identify if any significant differences based on demographics and their perceived level of cybersecurity risk of data breach exists. For SMEs, only years of IS experience significantly influenced the perceived level of cybersecurity risk associated with different PWWA techniques ( $p = 0.002$ ). Among IS users, gender ( $p < 0.001$ ), years of IS experience ( $p < 0.001$ ), and job level ( $p < 0.001$ ) all showed significant variations in the perceived risk linked to PWWA techniques. Finally, the development of the PaWoCyRiT was established, creating five different PaWoCyRiT variations. The first two were based on the IS users' perceived cybersecurity risk of data breach and their reported frequency of co-workers' engagement, with the next PaWoCyRiT being their self-reported frequency engagement. Falling into the Very High risk and frequency in the High and Very High were PWWA1 and PWWA2, with

PWWA4 and PWWA6 next in High risk and Moderate frequency. For the next two PaWoCyRiTs, the SMEs perceived the cybersecurity risk of data breach and their reported frequency of co-workers' engagement, followed by the PaWoCyRiT of their self-reported frequency of engagement in PWWA usage. The SMEs' perceived level of risk for each PWWA was ranked much higher for PWWA3, PWWA5, PWWA7, and PWWA9 in the Extreme risk and the rest in Very High risk. For reported co-workers' engagement, SMEs reported PWWA2 being the highest frequency in Very High, PWWA1, PWWA4, and PWWA6 in High, with the rest in Moderate frequency. For SMEs' self-reported frequency, PWWA2 was put in the High while the rest were ranked between Very Low and Moderate. The fifth and final PaWoCyRiT was developed, combining all the four previous PaWoCyRiTs for an overall comparison.

### **Implications**

According to the results, certain PWWAs are frequently used despite the recognized high risk of data breach. This is suggestive of an intricate balance between perceived convenience and cybersecurity. PWWA1 (documenting passwords) and PWWA10 (emailing or texting passwords) may be chosen for convenience, disregarding the cybersecurity risks. Furthermore, PWWA2 (reusing the same passwords for multiple accounts), PWWA4 (creating weak passwords), and PWWA6 (changing passwords to previously used passwords) demonstrate the inclination of simplicity of recall over cybersecurity. In addition, PWWA3 (sharing passwords) and PWWA9 (storing passwords physically in the open) point to insufficient awareness of secure password management, which could suggest a psychological element where ease of use can minimize cybersecurity risk awareness.

Organizational culture and policies may be one significant influence on user adoption of PWWAs. Understanding the dynamics and using it to develop strategies to balance cybersecurity with user behavior to warrant more applicable cybersecurity practices, such as addressing the complacency seen in PWWA5 (using default passwords), PWWA7 (no password change when triggered due to an incident-compromise) and PWWA8 (no password change when triggered due to an incident-possible compromise), we can enhance organizational cybersecurity posture. This research study also highlights the necessity of syncing organizational communication and cybersecurity awareness training to promote the combination of bringing together awareness and action in cybersecurity. Gaining more insight into why users desire to participate in PWWA usage can identify the root causes, enabling organizations to address the behavior better and improve organizational cybersecurity management.

This research study contributes to the cybersecurity body of knowledge, providing several implications for researchers and additional insights into password behaviors and developed a taxonomy for measuring password behavior risk. SMEs and IS users recognize the inherent cybersecurity risk of PWWAs; however, there is an evident inconsistency between cybersecurity risk perception and reported engagement. With their cybersecurity expertise, SMEs identified certain PWWA techniques as riskier than IS users, highlighting the importance of cybersecurity training and knowledge. Some techniques, particularly PWWA1, PWWA2, PWWA4, and PWWA6, were frequently used despite being seen as high risk, indicating areas organizations should address. Observations of co-workers' usage patterns appear as valuable data points, highlighting the importance of cybersecurity awareness and practices. The findings stress the need for

comprehensive interventions with a blend of education and practical tools to address the root causes driving risky behavior.

### **Recommendations**

The research study involving IS users (N=303) and SMEs (N=27) offers valuable insights into the perceived cybersecurity risk and engagement of PWWAs. Although the research goals were met, it would be beneficial to diversify participants' samples across different industries, job roles, and regions to further the findings in future research. An increase in SME participation could support expert insight depth. Adopting a longitudinal study approach could improve how people perceive cybersecurity risks and handle passwords. Additionally, conducting qualitative analyses could help uncover the root causes behind these behaviors. Assessing the real-world impact of cybersecurity awareness sessions and modern technological solutions could clarify their efficacy. Exploring the psychological foundations of PWWA adoption, understanding broader user behaviors, and evaluating the economic aspects of PWWA practices are similarly essential. These opportunities could collectively improve knowledge and identify more actionable assessments of PWWA techniques in cybersecurity.

### **Summary**

This research study has addressed the research problem of the use of PWWA techniques by employees in organizations that may pose significant cybersecurity risks of data breaches and financial damages. In phase I, a list of PWWA was developed from literature, and then this phase used the two rounds of the Delphi method employing cybersecurity SMEs to review and validate the list. This phase was used to answer the first three research questions:

RQ1. What are the SMEs' validated PWWA techniques that were identified in literature?

RQ2. What are the SMEs' identified measures for perceived cybersecurity risk of data breaches resulting from each validated PWWA technique?

RQ3. What are the SMEs' reported most frequently observed PWWA techniques co-workers use?

Phase II of this research was a pilot to provide a thorough review to confirm the study's reliability and validity and to address any measurement concerns before initiating the primary data analysis (Straub, 1989). Due to conducting two rounds of the Delphi method, the pilot study benefitted from refined expert consensus, ensuring greater accuracy and clarity in the finalized research instruments.

Phase III encompassed the primary data collection and analysis, leveraging a larger sample size to ensure broader representation and enhance the robustness of the findings. RQ3, RQ4, RQ6, RQ7, and RQ10 were analyzed using Microsoft Excel. In contrast, RQ5 and RQ8 employed ANOVA for their data assessment. RQ9 was analyzed using ANCOVA. The main research data was used to answer the remaining RQs:

RQ4. What are the employees' aggregated perceived cybersecurity risks of data breaches as a result of each validated PWWA technique?

RQ5. Are there any statistically significant mean differences in employees' aggregated perceived level of cybersecurity risk of data breaches as a result of each validated PWWA technique compared to those indicated by SMEs?

RQ6. What are the most frequently self-reported used PWWA techniques indicated by SMEs and employees' engagement in PWWA techniques?

RQ7. What are the most frequently reported PWWA techniques indicated by employees' reported frequency of co-workers' engagement in PWWA techniques?

RQ8. Are there any statistically significant mean differences between SMEs' and employees' self-reported and reported frequency of co-workers' engagement in PWWA?

RQ9. Do statistically significant differences exist in the perceived level of cybersecurity risk of data breaches as a result of each of the validated PWWA techniques based on (a) age, (b) gender, (c) years of computer experience, (d) years of cyber awareness training, and (e) job level?

RQ10. How are the PWWA techniques positioned on the proposed Password Workaround Cybersecurity Risk Taxonomy (PaWoCyRiT) using the aggregated score of perceived cybersecurity risk of data breaches resulting from the PWWA techniques VS. frequency of PWWA techniques usage?

This research highlights the level of perceived cybersecurity risks and user engagement in PWWAs usage, contributing significantly to the broader cybersecurity field and correlating the understanding gap between SMEs and IS users. A developed and validated list of PWWAs, derived through the Delphi method, serves as a foundational resource for future studies. Comparing the perceptions of SMEs and IS users revealed discrepancies between experts and users and highlighted the importance and requirement for cybersecurity awareness training strategies and organizational communication to improve effective cybersecurity practices within an organization. The analysis of the demographics underlines the central role of individual characteristics in shaping cybersecurity perceptions, which has been overlooked in prior research. Most notably, the introduction of the PaWoCyRiT model stands as a significant leap, offering organizations a structured and comprehensive tool to assess and navigate the complex domain of

PWWA-related risks and behaviors. In summary, this research enhances the granularity of our understanding of password cybersecurity risk perceptions. It provides a tool and insights for practitioners to strengthen cybersecurity measures in a more user-centric manner.



## Appendix A

### Institutional Review Board Approval Letter



#### MEMORANDUM

**To:** Michael Rooney  
College of Engineering and Computing

**From:** Ling Wang, Ph.D.  
College Representative, College of Engineering and Computing

**Date:** October 25, 2022

**Subject:** IRB Exempt Initial Approval Memo

**TITLE:** An Empirical Assessment of the Use of Password Workarounds and the Cybersecurity Risk of Data Breaches– NSU IRB Protocol Number 2022-482

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **October 25, 2022**. You may proceed with your study.

*Please Note: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.*

**Level of Review:** Exempt

**Type of Approval:** Initial Approval

**Exempt Review Category:** Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

**Post-Approval Monitoring:** The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

**Annual Status of Research Update:** You are required to notify the IRB Office annually if your

Page 1 of 2

research study is still ongoing via the *Exempt Research Status Update xForm*.

**Final Report:** You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the *Exempt Research Status Update xForm*.

**Translated Documents:** No

*Please retain this document in your IRB correspondence file.*

CC: Ling Wang, Ph.D.

Yair Levy, Ph.D.

## Appendix B

### Subject Matter Expert Recruitment Letter

Dear Information Systems Security **Subject Matter Expert (SMEs)**,

I am a Ph.D. Candidate in Cybersecurity Management at the College of Computing and Engineering at Nova Southeastern University (NSU). My dissertation is chaired by Dr. Yair Levy, and this work is part of the Levy CyLab Projects (<http://CyLab.nova.edu/>).

My research study seeks to validate the types of insecure password or password workarounds behaviors observed in literature and your experience. The survey I am seeking assistance with aims to develop a taxonomy of password workarounds and place them on a matrix based on perceived risk called the Password Workaround Cybersecurity Risk Taxonomy (PaWoCyRiT). The study will be an online survey that participants can access from any device with Internet access. The survey will consist of preliminary demographic questions, all non-PII, and questions based on your expertise and experience. I am requesting your help in a few areas in the development of the user survey and development of the PaWoCyrRit:

1. Your validation of a list of password workarounds that have been identified in a literature review
2. Your ranking of the perceived severity of the risk of causing a data breach
3. Your experience of witnessing or knowing that users/coworkers have utilized each of the password workaround techniques

If you choose to participate in this research study, you understand and agree that your participation and responses are entirely voluntary. All your responses will be completely anonymous, and no personally identifiable information will be collected or traced to the originator. You also understand that you may choose to stop your participation in this research at any time. The survey should take 15-25 minutes and is formatted to be completed on a mobile device or computer. To consent to participate in this survey, please click the link below:

[https://asu.co1.qualtrics.com/jfe/form/SV\\_8rcc3ROUXYVHApw](https://asu.co1.qualtrics.com/jfe/form/SV_8rcc3ROUXYVHApw)

The survey should take 15-20 minutes and can be completed on mobile devices. I appreciate the support and assistance in contributing to this research study. If you wish to receive the study's findings, please contact me via email, and I will provide a copy of the academic research publication resulting from this study.

Very respectfully,  
Michael J. Rooney  
Ph.D. Student in Cybersecurity Management  
Nova Southeastern University  
Email: [mr2640@mynsu.nova.edu](mailto:mr2640@mynsu.nova.edu)

## Appendix C

### Information Users Recruitment Letter

Dear Information Systems User Participant,

I am a Ph.D. Candidate in Cybersecurity Management at the College of Computing and Engineering at Nova Southeastern University (NSU). My dissertation is chaired by Dr. Yair Levy, and this work is part of the Levy CyLab Projects (<http://CyLab.nova.edu/>). I am seeking participants for my dissertation study. My research study seeks to validate the types of insecure password or password workarounds behaviors observed in literature and your experience.

If you choose to participate in this research study, you understand and agree that your participation and responses are entirely voluntary. All your responses will be completely anonymous, and no personally identifiable information will be collected or traced to the originator. You also understand that you may choose to stop your participation in this research at any time.

If you would like to participate, please go to:

[https://asu.co1.qualtrics.com/jfe/form/SV\\_8DnHYRQhztMdQCa](https://asu.co1.qualtrics.com/jfe/form/SV_8DnHYRQhztMdQCa)

The survey should take 15-20 minutes and can be completed on mobile devices.

Thank you very much for your time.

Very respectfully,  
Michael J. Rooney  
Ph.D. Candidate in Cybersecurity Management  
Nova Southeastern University  
Email: [mr2640@mynsu.nova.edu](mailto:mr2640@mynsu.nova.edu)

## Appendix D

### Subject Matter Expert Survey- Round 1



#### Subject Matter Expert Survey

##### SME PWWA Survey

Dear Cybersecurity SMEs,

This survey should take between 15-20 minutes and can be completed on mobile devices. I appreciate the support and assistance in contributing to this research study. If you wish to receive the study's findings, please contact me via email, and I will provide a copy of the academic research publication resulting from this study.

Very respectfully,  
Michael J. Rooney  
Ph.D. Candidate in Cybersecurity Management  
College of Computing and Engineering  
Nova Southeastern University



What age category includes your age?

- 18-30
- 31-40
- 41-50
- 51-60
- 61 or older

What is your gender?

- Male
- Female
- Non-binary / third gender
- Prefer not to say

What sector is the one you have/had the most IT/cybersecurity related experience in?

Government (Federal, State, Local)

Education

Private Sector

Other (specify)

What is your level at the organization you are in now?

Entry Level

Intermediate/Experienced

Supervisor

Manager

Director/VP

Executive/C-Suite

How many years have you utilized computers/information systems?

Less than 1

1-4

5-10

11-15

16-20

21-25

26-30

More than 30

How many accounts, personal and work, do you have that require password for authentication (require a password to login)?

Less than 10

11-20

21-30

31-40

Over 40

How many years of cybersecurity experience do you have?

Less than 1

1-4

5-10  
11-15  
16-20  
21-25  
26-30  
More than 30

Do you hold a current and active advanced or specialized industry IT/Cybersecurity certification? (i.e. CISM, CISSP, CISA, CASP+, GSE, CEH, Google, AWS, Microsoft, etc.)

Yes (specify)

No

Do you hold a degree in any field related to computing (e.g. information systems, computer science, information technology, computer engineering, cybersecurity)?

Doctorate

Masters

Bachelors

Associate

None

Field of study

How likely do you think that employees engaged in each of the following Password Workarounds will lead to an organizational data breach?

- 1 - Extremely unlikely, 0%
- 2 - Moderately Unlikely, 1-10%
- 3 - Slightly Unlikely, 10-30%
- 4 - Possibly Likely, 30-50%
- 5 - Slightly Likely, 50-70%
- 6 - Moderately Likely, 70-90 %
- 7 - Extremely Likely, 90-100 %







	Never (0%)	Rarely (1- 10%)	Occasionally (10-30%)	Sometimes (30-50%)	Frequently (50-70%)	Usually (70-90%)	Always (90- 100%)
PW4. Created weak passwords (use repeated patterns, names, meaningful numbers, or dates, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW5. Change passwords to previously used passwords	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW6. No Password Change Due to Trigger (not changing password periodically, when prompted or when compromised)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW7. Storing passwords physically in the open	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW8. Storing passwords physically in a private area	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW9. Storing passwords digitally in a password vault app/tool/keychain	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW10. Storing passwords digitally in the browser	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please drag and drop in order, your perception of the severity of each Password Workarounds risk of a data breach (1 most severe, 10 least severe)

Record passwords (write down/record on paper, mobile, computer, or other devices)

Reuse passwords

Shared passwords

Created weak passwords (use repeated patterns, names, meaningful numbers, or dates, etc.)

Change passwords to previously used passwords

No Password Change Due to Trigger (not changing password periodically, when prompted or when compromised)

Storing passwords physically in the open

Storing passwords physically in a private area

Storing passwords digitally in a password vault app/tool/keychain

Storing passwords digitally in the browser

Can you think of any other Password Workarounds that should be added to this list? (Please add as many as you can suggest in each box)

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

Other Password Workaround

This is the end of the survey. Please click "End Survey" to record your response.

### Subject Matter Expert Survey



Powered by Qualtrics

## Appendix E

### Subject Matter Expert Survey- Round 2



#### Subject Matter Expert Survey

##### SME PWWA Survey

Dear Cybersecurity SMEs,

This **anonymous** survey should take 15-20 minutes and can be completed on mobile devices. I appreciate the support and assistance in contributing to this research study. If you wish to receive the study's findings, please contact me via email, and I will provide a copy of the academic research publication resulting from this study.

Very respectfully,  
Michael J. Rooney  
Ph.D. Candidate in Cybersecurity Management  
College of Computing and Engineering  
Nova Southeastern University



#### Password Workarounds Validation

For the following 15 Password Workarounds, we ask that you would please **\*validate\*** each that was identified in literature and by experts in round 1, using your expert opinion about the level of agreement, from 1=Strongly Disagree to 7=Strongly Agree, that each one is a valid password workaround that may lead to a data breach.

- 1 - Strongly Disagree
- 2 - Disagree
- 3 - Somewhat Disagree
- 4 - Neither Agree or Disagree





	1- Extremely Unlikely	2- Moderately Unlikely	3- Slightly Unlikely	4- Possibly Likely	5- Slightly Likely	6- Moderately Likely	7- Extremely Likely
PW6. Changing passwords to previously used passwords (cycling among the same password list)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW7. No password change when triggered periodically (not changing passwords periodically or when prompted by notification of expiration)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW8. No password change when triggered due to an incident (not changing password after being notified of being compromised)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW9. No password change when triggered due to an incident (not changing password after being notified of possible compromise)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW10. Storing passwords physically in the open (office, home, public areas, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW11. Storing passwords physically in a private area (safe, locked office, locked draw, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW12. Storing passwords digitally in a password vault app/tool/keychain	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW13. Storing passwords digitally in the browser (clicking "Remember password" in browsers)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW14. Storing passwords in draft emails or texts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW15. Emailing or texting passwords	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

### Password Workarounds Co-worker's Engagement (That you have observed or aware of done)

Please find below the same set of 15 Password Workarounds and indicate on each one the **\*frequency\***, from 1=Never to 7=Always, that you have **observed or are aware of done** by **co-workers** to engage in each of the following Password Workarounds?

- 1 - Never
- 2 - Rarely
- 3 - Occasionally
- 4 - Sometimes







	1-Never	2-Rarely	3-Occasionally	4-Sometimes	5-Frequently	6-Usually	7-Always
PW8. No password change when triggered due to an incident ( <b>not changing password after being notified of being compromised</b> )	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW9. No password change when triggered due to an incident ( <b>not changing password after being notified of possible compromise</b> )	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW10. Storing passwords <b>physically in the open</b> (office, home, public areas, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW11. Storing passwords <b>physically in a private area</b> (safe, locked office, locked draw, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW12. Storing passwords <b>digitally in a password vault app/tool/keychain</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW13. Storing passwords <b>digitally in the browser</b> (clicking "Remember password" in browsers)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW14. Storing passwords <b>in draft emails or texts</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW15. Emailing or texting passwords	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Did you participate in round 1 of this SME Survey for Password Workarounds?

- Yes
- No

What age category includes your age?

- 18-30
- 31-40
- 41-50
- 51-60
- 61 or older

What is your gender?

- Male
- Female
- Non-binary / third gender

Prefer not to say

How many years have you utilized computers/information systems (essential use, work, school, etc.)?

Less than 1  
1-4  
5-10  
11-15  
16-20  
21-25  
26-30  
More than 30

How many years of cybersecurity security awareness training/experience do you have?

Less than 1  
1-4  
5-10  
11-15  
16-20  
21-25  
26-30  
More than 30

What is your level at the organization you are in now?

Entry Level  
Intermediate/Experienced  
Supervisor  
Manager  
Director/VP  
Executive/C-Suite

What sector do you have/had the most IT/cybersecurity-related experience in?

Government (Federal, State, Local)  
Education  
Private Sector  
Mixed Sectors  
Other (Please specify below)

What is the highest degree in any field related to computing (e.g. information systems, computer science, information technology, computer engineering, cybersecurity) do you hold?

Doctorate  
Masters  
Bachelors  
Associate  
None

How many personal and work accounts do you have that require a password for authentication (require a password to log in)?

Less than 10  
11-20  
21-30  
31-40  
Over 40

Do you hold a current and active advanced or specialized industry IT/Cybersecurity certification? (i.e. CISM, CISSP, CISA, CASP+, GSE, CEH, Google, AWS, Microsoft, etc.)

Yes (Please specify highest certificate below)

No

This is the end of the survey. Please click "Next" to end survey and record your response.

### Subject Matter Expert Survey



Powered by Qualtrics

# Appendix F

## Information Systems Users Survey



### Information Systems User Survey

#### IS Users PWWA Survey

Dear Information Systems User,

This **anonymous** survey should take between 10-15 minutes and can be completed on mobile devices. I appreciate the support and assistance in contributing to this research study. If you wish to receive the study's findings, please contact me via email, and I will provide a copy of the academic research publication resulting from this study.

Very respectfully,  
 Michael J. Rooney  
 Ph.D. Candidate in Cybersecurity Management  
 College of Computing and Engineering  
 Nova Southeastern University



### Password Workarounds Risk to Data Breach

Please find below a set of 12 Password Workarounds. Please indicate based on your perceived level of \*risk\*, from 1=Extremely Unlikely to 7=Extremely Likely, that each one of the following Password Workarounds may lead to an organizational data breach?

- 1 - Extremely Unlikely
- 2 - Moderately Unlikely
- 3 - Slightly Unlikely
- 4 - Possibly Likely
- 5 - Slightly Likely

6 – Moderately Likely

7 – Extremely Likely

	1- Extremely Unlikely	2- Moderately Unlikely	3- Slightly Unlikely	4- Possibly Likely	5- Slightly Likely	6- Moderately Likely	7- Extremely Likely
PW1. Documenting passwords (write down/record on paper, saved in mobile, computer, or other devices)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW2. Reusing the same passwords for multiple accounts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW3. Sharing passwords (amongst admins, coworkers, others)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW4. Creating weak passwords (use repeated patterns such as keyboard, number or letter patterns, names, meaningful numbers, or dates, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW5. Using default passwords (not changing factory or admin set default passwords)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW6. Changing passwords to previously used passwords (cycling among the same password list)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW7. No password change when triggered due to an incident ( <b>not changing password after being notified of being compromised</b> )	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW8. No password change when triggered due to an incident ( <b>not changing password after being notified of possible compromise</b> )	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW9. Storing passwords <b>physically in the open</b> (office, home, public areas, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW10. Storing passwords <b>digitally in the browser</b> (clicking "Remember password" in browsers)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW11. Storing passwords <b>in draft emails or texts</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW12. Emailing or texting passwords	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Password Workarounds Co-worker's  
Engagement (That you have observed or  
aware of done)**







	1-Never	2-Rarely	3-Occasionally	4-Sometimes	5-Frequently	6-Usually	7-Always
PW8. No password change when triggered due to an incident ( <b>not changing password after being notified of possible compromise</b> )	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW9. Storing passwords <b>physically in the open</b> (office, home, public areas, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW10. Storing passwords <b>digitally in the browser</b> (clicking "Remember password" in browsers)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW11. Storing passwords <b>in draft emails or texts</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PW12. Emailing or texting passwords	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

What age category includes your age?

- 18-30
- 31-40
- 41-50
- 51-60
- 61 or older

What is your gender?

- Male
- Female
- Non-binary / third gender
- Prefer not to say

How many years have you utilized computers/information systems (essential use, work, school, etc.)?

- Less than 1
- 1-4
- 5-10
- 11-15
- 16-20
- 21-25
- 26-30
- More than 30

How many years of cybersecurity security awareness training/experience do you have?

- Less than 1
- 1-4
- 5-10
- 11-15
- 16-20
- 21-25
- 26-30
- More than 30

What is your level at the organization you are in now?

- Entry Level
- Intermediate/Experienced
- Supervisor
- Manager
- Director/VP
- Executive/C-Suite

How many personal and work accounts do you have that require a password for authentication (require a password to log in)?

- Less than 10
- 11-20
- 21-30
- 31-40
- Over 40

This is the end of the survey. Please click "Next" to end survey and record your response.

### Information Systems User Survey



Powered by Qualtrics

## References

- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40–46.
- Africk, E., & Levy, Y. (2021). An examination of historic data breach incidents: What cybersecurity big data visualization and analytics can tell us? *The Online Journal of Applied Knowledge Management*, 9(1), 31–45.
- Alali, M., Almogren, A., Hassan, M. M., Rasan, I. A. L., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*, 74, 323–339.
- AlFayyadh, B., Thorsheim, P., Jøsang, A., & Klevjer, H. (2012). Improving usability of password management with standardized password policies. *Proceedings of the 7th Conference on Network and Information Systems Security (SAR-SSI)* (pp. 38–45).
- Alkaldi, N., Renaud, K., & Mackenzie, L. (2019). Encouraging password manager adoption by meeting adopter self-determination needs. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 6, (pp. 4824–4833).
- Alkeem, E. A., Shehada, D., Yeun, C. Y., Zemerly, M. J., & Hu, J. (2017). New secure healthcare system using cloud of things. *Cluster Computing*, 20(3), 2211–2229.
- Allodi, L., & Massacci, F. (2017). Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 37(8), 1606–1627.
- Alter, S. (2014). Theory of workarounds. *Communications of the Association for Information Systems*, 34, 1041–1066.
- 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.
- Arduin, P. E., & Vieru, D. (2017). Workarounds as means to identify insider threats to information systems security. *23rd Americas Conference on Information Systems*, (pp. 1-5).
- Bhagavatula, S., Bauer, L., & Kapadia, A. (2020). (How) Do people change their passwords after a breach? *arXiv*, 1-8.
- Bhanushali, A., Mange, B., Vyas, H., Bhanushali, H., & Bhogle, P. (2015). Comparison of graphical password authentication techniques. *International Journal of Computer Applications*, 116(1), 11-14.

- Blackwood-Brown, C., Levy, Y., D'Arcy, J. (2019). Cybersecurity awareness and skills of senior citizens: A motivation perspective. *Journal of Computer Information Systems*, 61, 195-206.
- Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, 51(4), 64–68.
- Boell, S. K., & Cecez-Kecmanovic, D. (2015). What is an information system? *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 4959–4968).
- Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2013). Supply chain risk management practices for federal information systems and organizations. *NIST Special Publication 800-161*, 1–282.  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf>
- Brason, S. (2020). Contextual awareness: Advancing identity and access management to the next level of security awareness. *Enterprise Management Associates Summary Research Report*, 1-21.
- Brumen, B. (2019). Security analysis of game changer password system. *International Journal of Human-Computer Studies*, 126, 44–52.
- Brumen, B. (2020). System-assigned passwords: The disadvantages of the strict password management policies. *Informatica*, 31(3), 459–479.
- Bryant, K., & Campbell, J. (2006). User Behaviours associated with password security and management. *Australian Journal of Information Systems*, 14(1), 88-100.
- Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *International Journal of Information and Computer Security*, 11, 431–448.
- Chanda, K. (2016). Password security: An analysis of password strengths and vulnerabilities. *Computer Network and Information Security*, 7, 23–30.
- Chen, H. S., & Jai, T.M. (2021). Trust fall: data breach perceptions from loyalty and non-loyalty customers. *The Service Industries Journal*, 41(13-14), 947–963.
- Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, 97, 1-13.

- Chua, H. N., Teh, J. S., & Herbland, A. (2021). Identifying the effect of data breach publicity on information security awareness using hierarchical regression. *IEEE Access*, *9*, 121759–121770.
- Cialdini, R. B., & Trost, M. R. (1998). Social influence: Social norms, conformity and compliance. In D. T. Gilbert, S. T. Fiske, & G. Lindzey (Eds.), *The handbook of social psychology* (p. 151–192). McGraw-Hill.
- Cicchetti, D. V., Showalter, D., Tyrer, P. J. (1985). The effect of number of rating scale categories on levels of interrater reliability: A Monte Carlo investigation. *Applied Psychological Measurement*, *9*(1), 31-36.
- Covello, V. T., & Mumpower, J. (1985). Risk analysis and risk management: An historical perspective. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, *5*(2), 103–120.
- Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.
- Dalkey, N., & Helmer, O. (1963). An experimental application of the delphi method to the use of experts. *Management Science*, *9*(3), 458–467.
- Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Applications of social network analysis in behavioural information security research: Concepts and empirical analysis. *Computers and Security*, *68*, 1–15.
- Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. *Proceedings Network and Distributed System Security Symposium*, (pp. 1-15).
- Davis, K., Levy, Y., & Delak, B. (2018). Towards a development of cybersecurity risk-responsibility taxonomy of small enterprises for data breach mitigation. *Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018*, (pp. 1-6).
- D’Arcy, J., Adjerid, I., Angst, C. M., & Glavas, A. (2020). Too good to be true: Firm social performance and the risk of data breach. *Information Systems Research*, *31*(4), 1200–1223.
- 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.
- Dillon, R., Chawla, S., Hristova, D., Göbl, B., & Jovicic, S. (2020). Password policies vs. usability: When do users go “bananas”? *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications*, (pp. 148–153).

- Du, H., Lehmann, C. M., & Willson, V. L. (2022). Would you give me your password? *Journal of Information Systems*, 36(2), 17–52.
- Dupuis, M. J., Crossler, R. E., & Endicott-Popovsky, B. (2016). Measuring the human factor in information security and privacy. *IEEE Hawaii International Conference on System Sciences*, (pp. 3676-3685).
- Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, 24(1), 93–125.
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, 6, 323-337.
- Ellis, T. J., & Levy, Y. (2010). A guide for novice researchers: Design and development research methods. *Proceedings of the 2010 InSITE Conference*, 10, (pp. 107–118).
- Ellis, T. J., & Levy, Y. (2012). Data sources for scholarly research: Towards a guide for novice researchers. *Proceedings of the 2012 InSITE Conference* (pp. 405–416).
- Elmrabit, N., Yang, S., Yang, L., Zhou, H. (2020). Insider threat risk predication based on Bayesian network. *Computers & Security*, 96, 1-19.
- ENISA. (2020). Threat landscape 2020 data breach.  
<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach>
- Erlich, Z., & Zviran, M. (2009). Authentication methods for computer systems security. In Khosrow-Pour M. *Encyclopedia of information science and technology*. (Vol. 1, 119 pp. 288- 293). Hershey, PA: Information Science Reference.
- Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, 80, 74–89.
- Farik, M., & Ali, A. S. (2015). Analysis of default passwords in routers against brute-force attack. *International Journal of Scientific & Technology Research*, 4(9), 341-345.
- Federal Bureau of Investigation (FBI) (2020). Internet crime report 2020. *Internet Crime Complaint Center (IC3)*.
- Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, 22(5), 410–430.

- Fielding, J. (2020). The people problem: how cyber security's weakest link can become a formidable asset. *Computer Fraud & Security*, 2020(1), 6–9.
- Ford, A., Al-Nemrat, A., Ghorashi, S. A., & Davidson, J. (2021). The impact of data breach announcements on company value in European markets. *WEIS 2021: The 20th Annual Workshop on the Economics of Information Security*, (pp.1-8).
- Frank, M., Biedert, R., Ma, E., Martinovic, I., & Song, D. (2012). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Transactions on Information Forensics and Security*, 8(1), 136–148.
- Fritz, J., & Kaefer, F. (2017). The rise of the mega breach and what can be done about it. *Journal of Applied Security Research*, 12(3), 392–406.
- Furnell, S. (2019). Password meters: inaccurate advice offered inconsistently? *Computer Fraud & Security*, 2019(11), 6–14.
- Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, 2020(12), 6–12.
- Garfinkel, S. L. (2012). Inside risks the cybersecurity risk. *Communications of the ACM* 55(6), 29–32.
- Gasti, P., Šeděnka, J., Yang, Q., Zhou, G., & Balagani, K. S. (2016). Secure, fast, and energy-efficient outsourced authentication for smartphones. *IEEE Transactions on Information Forensics and Security*, 11(11), 2556–2571.
- Ghafir, I., Prenosil, V., Alhejailan, A., & Hammoudeh, M. (2016). Social engineering attack strategies and defence approaches. *Proceedings of IEEE 4th International Conference on Future Internet of Things and Cloud* (pp. 145–149).
- Gilbert, F. (1992). Breach of system security and theft of data: Legal aspects and preventive measures. (2014). *Computers & Security*, 11(6), 508-517.
- Giwah, A. D. (2018). User information security behavior towards data breach in Bring Your Own Device (BYOD) enabled organizations - Leveraging protection motivation theory. *SoutheastCon 2018*, 1-5.
- Gokhale, A. S., & Waghmare, V. S. (2016). The shoulder surfing resistant graphical password authentication technique. *Procedia Computer Science*, 79, 490-498.
- Golla, M., Filipe, L., Wei, M., Dürmuth, M., Ur, B., Hainline, J., & Redmiles, E. (2018). What was that site doing with my Facebook password? Designing password-reuse notifications. *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 1549–1566).



- Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly*, 41(3), 703-727.
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, 6(1).
- Grimes, R. A. (2020). Creating a solid password policy. *Computer Fraud & Security*, 2020(7), 20.
- Grassi, P. A., Garcia, M. E., Fenton, J. L. (2017). Digital identity guidelines. National Institute of Standards and Technology, Gaithersburg, MD, Special Publication Series (800), NIST SP 800-63-3, Updated 03-02-2020.
- Guo, Y., Zhang, Z., & Guo, Y. (2019). Optiwords: A new password policy for creating memorable and strong passwords. *Computers & Security*, 85, 423–435.
- Guo, Y. Y., Zhang, Z., Guo, Y. Y., & Guo, X. (2020). Nudging personalized password policies by understanding users' personality. *Computers and Security*, 94.
- Güven, E. Y., Boyaci, A., & Aydin, M. A. (2022). A novel password policy focusing on altering user password selection habits: A statistical analysis on breached data. *Computers & Security*, 113, 1-13.
- Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, 35(2), 683–714.
- Han, W., Xu, M., Zhang, J., Wang, C., Zhang, K., & Sean Wang, X. (2021). TransPCFG: Transferring the grammars from short passwords to guess long passwords effectively. *IEEE Transactions on Information Forensics and Security*, 16, 451–465.
- Hao, F., Metere, R., Shahandashti, S. F., & Dong, C. (2018). Analyzing and patching SPEKE in ISO/IEC. *IEEE Transactions on Information Forensics and Security*, 13(11), 2844–2855.
- Hibbeln, M., Jenkins, J. L., Schneider, C., Valacich, J. S., & Weinmann, M. (2017). How is your user feeling? Inferring emotion through human-computer interaction devices. *MIS Quarterly*, 41(1), 1–21.
- Hohmann, E., Brand, J. C., Rossi, M. J., & Lubowitz, J. H. (2017). Expert opinion is necessary: Delphi panel methodology facilitates a scientific approach to consensus. *Arthroscopy: The Journal of Arthroscopic & Related Surgery*, 34(2), 349–351.

- Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime, 22*(2), 242–260.
- Houshmand, S., Aggarwal, S., & Flood, R. (2015). Next gen PCFG password cracking. *IEEE Transactions on Information Forensics and Security, 10*(8), 1776–1791.
- Huaman, N., Amft, S., Oltrogge, M., Acar, Y., & Fahl, S. (2021). They would do better if they worked together: The case of interaction problems between password managers and websites. *IEEE Symposium on Security and Privacy*, (pp. 1-15).
- Irfan, K., Anas, A., Malik, S., & Amir, S. (2018). Text based graphical password system to obscure shoulder surfing. *Proceedings of 2018 15th International Bhurban Conference on Applied Sciences and Technology* (pp. 422–426).
- Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.
- Jarecki, S., Krawczyk, H., Shirvanian, M., & Saxena, N. (2018). Two-factor authentication with end-to-end password security. *Public-Key Cryptography – PKC 2018, 10770*, 431–461.
- Joint Task Force on Cybersecurity Education (2017). *Curricula guidelines for post-secondary degree in cybersecurity*. [https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017\\_web.pdf](https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf)
- Joint Task Force Transformation Initiative. (2013). *Security and privacy controls for federal information systems and organizations (NIST Special Publication 800-53 Rev. 4)*. National Institute of Standards and Technology. (Updated January 22, 2015).
- Joseph, R. C. (2018). Data breaches: Public sector perspectives. *IT Professional, 20*(4), 57–64.
- Kaleta, J. P., Lee, J. S., & Yoo, S. (2019). Nudging with construal level theory to improve online password use and intended password choice: A security-usability tradeoff perspective. *Information Technology and People, 32*(4), 993–1020.
- Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security, 1–18*.
- Katsumata, P., Hemenway, J., & Gavins, W. (2010). Cybersecurity risk management. *The 2010 Military Communications Conference*, (pp. 890–895).
- Khan, F., Kim, J.H., Mathiassen, L., Moore, R. (2021). Data breach management: An integrated risk model. *Information & Management, 58*, 1-12.

- Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). Shadow security as a tool for the learning organization. *ACM SIGCAS Computers and Society*, 45(1), 29-37.
- Kissel, R. (2013). Glossary of key information security terms (NIST IR 7298r2). <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>
- Koppel, R., Smith, S., Blythe, J., & Kothari, V. (2015). Workarounds to computer access in healthcare organizations: You want my password or a dead patient? *Studies in Health Technology and Informatics*, 208, 215–220.
- Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research*, 135, 559–571.
- Landeta, J. (2006). Current validity of the Delphi method in social sciences. *Technological Forecasting and Social Change*, 73(5), 467–482.
- Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659–671.
- Levy, Y. (2006). Assessing the value of e-learning systems. Hershey, PA: Information Science Publishing.
- Levy, Y. (2008). An empirical development of critical value factors (CVF) of online learning activities: An application of activity theory and cognitive value theory. *Computers & Education*, 51(4), 1664-1675
- Lai, J., & Arko, E. (2021). A shoulder-surfing resistant scheme embedded in traditional passwords. *Proceedings of the 54th Hawaii International Conference on System Sciences* (pp. 7144-7152).
- Lei, M., Xiao, Y., Vrbsky, S. V., Li, C.-C., & Liu, L. (2008). A virtual password scheme to protect passwords. *IEEE International Conference on Communications*, (pp. 1-6).
- Levy, Y., & Gafni, R. (2021). Introducing the concept of cybersecurity footprint. *Information and Computer Security*, 1-13.
- 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.
- Lin, S. C., Yen, D. C., Chen, P. S., & Lin, W. K. (2013). Coding behavior of authentication code on the internet. *Computers in Human Behavior*, 29(5), 2090-2099.

- Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care: Official Journal of the European Society for Engineering and Medicine*, 24(1), 1–9.
- Lund, B. D. (2020). Review of the Delphi method in library and information science research. *Journal of Documentation*, 39, 88.
- Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. *Information Resources Management Journal*, 24(3), 1–8.
- Mahfouz, A., Mahmoud, T. M., & Eldin, A. S. (2017). A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications*, 37, 28–37.
- Mattord, H., Levy, Y., & Furnell, S. (2013). Factors of password-based authentication. *Proceedings of the Nineteenth Americas Conference on Information Systems*, 3, (pp. 1685–1693).
- Masuch, K., Greve, M., Trang, S., & Kolbe, L. M. (2022). Apologize or justify? Examining the impact of data breach response actions on stock value of affected companies? *Computers & Security*, 112, 1-13.
- Matulevicius, R., Mayer, N., & Heymans, P. (2008). Alignment of misuse cases with security risk management. *The Third International Conference on Availability, Reliability and Security*, (pp. 1397–1404).
- Mayer, P., Zou, Y., Schaub, F., & Aviv, A. J. (2021). “Now I’m a bit angry:” Individuals’ awareness, perception, and responses to data breaches that affected them. *Proceedings of the 30th USENIX Security Symposium* (pp. 393-410).
- Me, G., & Pesticcio, L. (2018). Tor black markets: Economics, characterization and investigation technique. In H. Jahankhani (Ed.), *Cyber Criminology* (pp. 119–140). Springer International Publishing.
- Menkus, B. (1998). Understanding the use of passwords. *Computers & Security*, 7(2), 132-136
- Mertler, C. A., & Reinhart, R. V. (2016). *Advanced and multivariate statistical methods (6th ed.): Practical application and interpretation*. New York, NY: Routledge
- Mujeye, S. (2021). A survey on multi-factor authentication methods for mobile devices. *The 4th International Conference on Software Engineering and Information Management*, (pp. 199–205).

- Mujeye, S., Levy, Y., Mattord, H., & Li, W. (2016). Empirical results of an experimental study on the role of password strength and cognitive load on employee productivity. *Online Journal of Applied Knowledge Management*, 4(1), 99–116.
- Nandy, T., Idris, M. Y. I. B., Md Noor, R., Mat Kiah, L., Lun, L. S., Annuar Juma'at, N. B., Ahmedy, I., Abdul Ghani, N., & Bhattacharyya, S. (2019). Review on security of Internet of Things authentication mechanism. *IEEE Access*, 7, 151054–151089.
- Nathan, M. (2020). Credential stuffing: new tools and stolen data drive continued attacks. *Computer Fraud & Security*, 2020(12), 18–19.
- National Initiative for Cybersecurity Careers and Study Cybersecurity glossary. (2021, March 04). <https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#D>
- National Institute of Standards and Technology (NIST). (2017, June). Digital identity guidelines authentication and lifecycle management. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>
- National Institute of Standards and Technology (NIST). (2012, September). Guide for conducting risk assessments. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- National Institute of Standards and Technology (NIST). (2006, March). Minimum security requirements for federal information and information Systems (FIPS PUB 200). <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>
- Neigel, A. R., Claypoole, V. L., Waldfole, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, 92, 101731.
- Notoatmodjo, G., & Thomborson, C. (2009). Passwords and perceptions. *Proceedings of the Seventh Australasian Conference on Information Security*, 98, (pp. 71–78).
- Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography and Communications*, 2(1), 1.
- Pace, D. K., & Sheehan, J. (2002). Subject matter expert (SME)/ Peer use in M & S V & V. *Proc. Workshop on Foundations for Modeling and Simulation (M&S) Verification and Validation (V&V) in the 21st Century*, 1–34.
- Pal, B., Daniel, T., Chatterjee, R., & Ristenpart, T. (2019). Beyond credential stuffing: Password similarity models using neural networks. *2019 IEEE Symposium on Security and Privacy*, (pp. 1-18).

- Patterson, E. S. (2018). Workarounds to intended use of health information technology: A narrative review of the human factors engineering literature. *Human Factors*, 60(3), 281–292.
- Pearman, S., Zhang, S. A., Bauer, L., Christin, N., & Cranor, L. F. (2019). Why people (don't) use password managers effectively. *Fifteenth Symposium On Usable Privacy and Security*, (pp. 319–338).
- Perakslis, E. D., & Stanley, M. (2016). A cybersecurity primer for translational research. *Science Translational Medicine*, 8(322), 1–4.
- Ponemon Institute (2020). Cost of a data breach report.  
<https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf=>
- Poyraz, O. I., Canan, M., McShane, M., Pinto, C. A., & Cotter, T. S. (2020). Cyber assets at risk: monetary impact of U.S. personally identifiable information mega data breaches. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 45(4), 616–638.
- Rajah, P. R. S., Dastane, O., Bakon, K. A., & Johari, Z. (2020). The effect of bad password habits on personal data breach. *International Journal of Emerging Trends in Engineering Research*, 8(10), 6950–6960.
- Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*, 27(2-3), 183–213.
- Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal*, 19(4), 439–444.
- Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for cybersecurity risk planning. *Decision Support Systems*, 51(3), 493–505.
- Reeves, A., Calic, D., & Delfabbro, P. (2021). “Get a red-hot poker and open up my eyes, it’s so boring”: Employee perceptions of cybersecurity training. *Computers & Security*, 106, 1–13.
- Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, 11(1), 74–104.
- Rosati, P., Deeney, P., Cummins, M., Werff, L. V. D., & Lynn, T. (2018). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance*, 47, 458–469.

- Sae-Bae, N., Memon, N., Isbister, K., & Ahmed, K. (2014). Multitouch gesture-based authentication. *IEEE Transactions on Information Forensics and Security*, 9(4), 568–582.
- Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, 53, 65-78.
- Samadi, S., Vempala, S., & Kalai, A. T. (2018). Usability of humanly computable passwords. *Sixth AAI Conference on Human Computation and Crowdsourcing*, (pp. 174-183).
- Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare (Basel)*, 8(2), 1-18.
- Sahin, S., & Li, F. (2021). Don't forget the stuffing! Revisiting the security impact of typo-tolerant password authentication. *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (pp. 252–270).
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th Ed.). West Sussex, United Kingdom: John Wiley & Sons Ltd.
- Shay, R., Cranor, L. F., Komanduri, S., Durity, A. L., Huh, P. (Seyoung), Mazurek, M. L., & Christin, N. (2014). Can long passwords be secure and usable? *Proceedings of the 32nd annual ACM conference on human factors in computing systems* (pp. 2927–2936).
- Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., & Cranor, L. F. (2010). Encountering stronger password requirements: User attitudes and behaviors. *ACM International Conference Proceedings of the 6th Symposium on Usable Privacy and Security* (pp. 1-20).
- Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers and Security*, 61, 130–141.
- Shinde, N., & Kulkarni, P. (2021). Cyber incident response and planning: a flexible approach. *Computer Fraud & Security*, 2021(1), 14–19.
- Si, J., Cheng, Z., Li, Z., Cheng, J., Wang, H.-M., & Al-Dhahir, N. (2020). Cooperative jamming for secure transmission with both active and passive eavesdroppers. *IEEE Transactions on Communications*, 68(9), 5764–5777.
- Silic, M., & Back, A. (2014). Shadow IT – A view from behind the curtain. *Computers & Security*, 45, 274–283.

- Sillic, M. (2019). Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the shadow IT context. *Computers and Security, 80*, 108–119.
- Siponen, M., Puhakainen, P., & Vance, A. (2020). Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Computers and Security, 88*, 1-12.
- Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems, 37*(1), 31–63.
- Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security, 15*(4), 708-722.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.
- Sun, H. M., Chen, Y. H., & Lin, Y. H. (2012). oPass: A user authentication protocol resistant to password stealing and password reuse attacks. *IEEE Transactions on Information Forensics and Security, 7*(2), 651–663.
- Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency planning guide for federal information systems (NIST SP 800-34r1). <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>
- Taneski, V., Heričko, M., & Brumen, B. (2019). Systematic overview of password security problems. *Acta Polytechnica Hungarica, 16*(3), 143–165.
- Tatli, E. I. (2015). Cracking more password hashes with patterns. *IEEE Transactions on Information Forensics and Security, 10*(8), 1656–1665.
- Terrell, S. R. (2016). Writing a proposal for your dissertation. Guilford.
- Theoharidou, M., Papanikolaou, N., Pearson, S., & Gritzalis, D. (2013). Privacy risk, security, accountability in the cloud. *IEEE 5th International Conference on Cloud Computing Technology and Science*, (pp. 177–184).
- Theofanos, M., Choong, Y.-Y., & Murphy, O. (2021). ‘Passwords keep me safe’ – Understanding what children think about passwords. *Proceedings of the 30th USENIX Security Symposium* (pp. 19–35).
- Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., Margolis, D., Paxson, V., & Bursztein, E. (2017). Data breaches, phishing, or malware? Understanding the risks of stolen



- credentials. *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 1421–1434).
- Topper, J. (2018). Compliance is not security. *Computer Fraud and Security*, 2018(3), 5–7.
- Trabelsi, S., & Missaoui, C. (2018). Dissuading stolen password reuse. *Emerging Technologies for Authorization and Authentication*, 11263, 116–128.
- Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). Do users' perceptions of password security match reality? *Conference on Human Factors in Computing Systems Proceedings* (pp. 3748–3760).
- Verizon. (2020). 2020 data breach investigations report. <https://enterprise.verizon.com/resources/reports/dbir/>
- Wang, D., & Wang, P. (2018). Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE Transactions on Dependable and Secure Computing*, 15(4), 708–722.
- Wang, D., Cheng, H., Wang, P., Huang, X., & Jian, G. (2017). Zipf's law in passwords. *IEEE Transactions on Information Forensics and Security*, 12(11), 2776–2791.
- Wang, K. C., & Reiter, M. K. (2018). How to end password reuse on the web. *Network and Distributed System Security Symposium*, (pp. 1–16).
- Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, 44, 1–15.
- Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, 18(1), 3–7.
- Wibisono, A., Sammon, D., & Heavin, C. (2020). Modelling data activities in workarounds: a narrative network approach. *Journal of Decision Systems*, 1–12.
- Woods, N. (2019). The light side of passwords: Turning motivation from the extrinsic to the intrinsic research in progress. *Proceedings Workshop on Information Security and Privacy* (pp. 1–11).
- Woods, N., & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human Computer Studies*, 111, 36–48.

- Woods, N., & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human Computer Studies*, 128, 61–71.
- Xu, M., Schweitzer, K. M., Bateman, R. M., & Xu, S. (2018). Modeling and predicting cyber hacking breaches. *IEEE Transactions on Information Forensics and Security*, 13(11), 2856–2871.
- Yildirim, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, 18(6), 741–759.
- Zheng, W., & Jia, C. (2017). CombinedPWD: A new password authentication mechanism using separators between keystrokes. *13th International Conference on Computational Intelligence and Security*, (pp. 557–560).
- Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. *International Journal of Human Computer Studies*, 133, 26–44.