


November 2020

Digital Identity: A Human-Centered Risk Awareness Study

Toufic N. Chebib
University of South Florida

Follow this and additional works at: <https://scholarcommons.usf.edu/etd>

 Part of the [Business Administration, Management, and Operations Commons](#), [Databases and Information Systems Commons](#), and the [Library and Information Science Commons](#)

Scholar Commons Citation

Chebib, Toufic N., "Digital Identity: A Human-Centered Risk Awareness Study" (2020). *Graduate Theses and Dissertations*.
<https://scholarcommons.usf.edu/etd/8523>

This Dissertation is brought to you for free and open access by the Graduate School at Scholar Commons. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Scholar Commons. For more information, please contact scholarcommons@usf.edu.

Digital Identity: A Human-Centered Risk Awareness Study

by

Toufic N. Chebib

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Business Administration
Muma College of Business
University of South Florida

Co-Major Professor: Jung Chul Park, Ph.D.
Co-Major Professor: Loran Jarrett, D.B.A.
Joann Quinn, Ph.D.
Paul Solomon, Ph.D.

Date of Approval:
October 23, 2020

Keywords: Cybersecurity, Privacy, Information Security Management, Online Interactions,
Online Threats, Adapted Thematic Analysis

Copyright © 2020, Toufic N. Chebib

ACKNOWLEDGMENTS

I would like to thank my family for always being there for me. I especially thank my parents for raising their two boys on great values of maintaining integrity in our relationships and work, self-respect, and respect for others, as well as instilling into us a sense of servant leadership. My father, Nicolas, and my mother, Margaret, have always been and still are an exemplary couple in teaching us family values and finding joy in helping others around us. My parents have always taught us not to be afraid to aim for the stars, work hard, and be humble. A big thank you to my brother Ziad for always being a rock I can lean on during tough times.

The journey to get this far through my studies has not been easy. When I first moved to the United States in December 2000, I had a couple of hundred dollars that my father managed to put aside for me; times were tough. He always taught me to be the best I can be in everything I do. My goal was to seek knowledge and get a terminal degree. Here I am, 20 years later, making my dream come true. I always dreamt of being an astronaut; little did I know that being an astronaut was all about breaking barriers and reaching new heights in life.

I want to also thank my DBA cohort members for being a great support channel throughout this program. Thank you to my dissertation chairs and committee: Dr. Jung Chul Park, Dr. Loran Jarrett, Dr. Joann Quinn, and Dr. Paul Solomon. I also thank my dissertation team and cohort members, Mark Mattia, Michael Summers, and Brad Puckey, for listening to my progress updates for almost a year. A special thank you to Dr. Vernetta Williams for being a fantastic dissertation process guide and writing coach, particularly for keeping me motivated and

focused. Congratulations to the Doctor of Business Administration class of 2020; this year has not been easy, but we made it through. Best of luck in all your future endeavors.

TABLE OF CONTENTS

List of Tables	v
List of Figures	vi
Abstract	vii
Chapter One: Introduction	1
Background	1
Example of an Identity Theft Victim	2
Statement of Purpose	4
Purpose	4
Relevance	4
The Motivation for the Study	5
Researcher Bias and Assumptions	5
Research Question	6
Chapter Two: About Identity	8
Identity	8
Privacy	9
Data Privacy Risks	10
Privacy Laws, Regulations, and Frameworks	11
Digital Identity Management	12
Chapter Three: Literature Review	13
Overview	13
Themes from the Literature	14
Theme 1: Increased Use of the Internet	15
Theme 2: Definition of Digital Identity	16
Theme 3: Perspectives on Digital Identity and Privacy	18
Theme 4: Privacy Risks	21
Theme 5: Laws and Regulations Relating to Privacy and Digital Identity	24
Theme 6: Individuals Behavior and Habits	27
Theme 7: Tools and Training Enabling Digital Identity Management	28
Summary of Findings	31
Chapter Four: Methodology	34
Overview	34
Research Design	34
Interview Until Data Novelty Saturation	34

Process Followed	35
Thematic Analysis	35
Why the ATA for this Study.....	37
Data Collection.....	37
Participant Selection.....	38
Interview Participants Characteristics.....	39
Study Invitation.....	39
IRB Approval.....	39
Data Analysis	39
Coding Method	39
Top-down open coding	39
Bottom-up axial coding	40
Illustrate findings by themes or key concepts	41
Coding Results.....	41
Open coding	41
Chapter Five: Findings	47
Overview.....	47
Findings from the Interviews	47
Qualifier to the Study: High Internet Adoption and Use of Digital Identity	47
Most people 55 to 75 are active online.....	48
Online Accounts	49
Most of the people didn't remember all the online accounts they used in the last 5 to 10 years	49
Social media.....	50
Online banking	50
Online purchases	51
Digital identity includes online personal data as well as online interactions	51
Theme 1: People Accept the Risk When It Affects Their Convenience	52
Accept the risk as it is part of life right now, especially when the convenience outweighs the risks	52
Most study participants have been or know someone who has been affected by an online data breach	52
Study participants' online behavior was not affected by experiencing or knowing about cybersecurity breaches	53
Study participants' concern about their online reputation	53
People seem to trust their financial institutions to protect them and their money	54
Cybersecurity risks are not a deterrence	55
Theme 2: People Are Concerned That Companies Are Not Being Transparent with Regards to Being Good Custodians of Their Digital Identity.....	56
Companies are not providing details about data breaches	56
There is a high level of familiarity with the existence of online privacy rules, laws, and regulations.....	57

Companies are not transparent with people's personal data withheld or shared online.....	58
People want companies to be more transparent	58
Theme 3: People Are Aware of the Availability of Tools and Trainings to Help Manage the Risks.....	59
Awareness to keep digital identity secure.....	59
People's awareness of tools and training.....	60
People's exposure to cybersecurity training	61
Cybersecurity training is helpful	61
Low adoption of password management tools.....	62
Theme 4: People Want More Transparency and Control Over Their Digital Identity to Help Them Ease Their Concerns of the Risks	62
People want more transparency and control over their online digital data.....	62
Solutions desired geared towards transparency and more control	63
Chapter Six: Discussion	65
Overview.....	65
Analysis	65
Qualifier to the Study: Increased Level of Internet Adoption Among People Caused the Wide Use of Digital Identity	65
Interpretation.....	66
Qualifier to the Study: People Are Aware of the Composition of Their Digital Identity	66
Interpretation.....	66
Theme 1: Relationship Between Digital Identity Risks and People's Online Behavior.....	67
Interpretation.....	68
Theme 2: Online Platforms Are a Risk to People's Digital Identity	70
Interpretation.....	72
Theme 3: Tools to Manage Digital Identity Risks.....	72
Interpretation.....	74
Theme 4: People Want More Transparency and Awareness to Keep Their Digital Identity Secure.....	75
Interpretation.....	76
Conclusions	77
Contribution to Academics and Practitioners	80
Limitations and Future Research.....	81
References	84
Appendix A: Interview Solicitation Flyer	92
Appendix B: IRB Verbal Consent Form	93
Appendix C: Interview Questionnaire.....	95

Appendix D: IRB Approval Exempt Form.....	97
Appendix E: ITRC 2019 Data Breach Report Statistics	98

LIST OF TABLES

Table 1:	Literature Review Summary of Findings.....	32
Table 2:	Open Coding and Groupings.....	41
Table 3:	Open Coding to Axial Coding.....	43
Table 4:	Axial Coding to Themes	45
Table 5:	Internet Adoption Comparison.....	67
Table 6:	Digital Identity Composition Awareness Comparison	67
Table 7:	Relationship Between Digital Identity Risks and People’s Online Behavior Comparison	70
Table 8:	Online Platforms are a Risk to People’s Digital Identity Comparison	72
Table 9:	Tools to Manage People’s Digital Identity Comparison.....	75
Table 10:	People Want More Transparency and Awareness to Keep Their Digital Identity Secure Comparison	77
Table 1A:	Breaches and Records Exposed (In Millions) by Year (2010 to 2019)	98

LIST OF FIGURES

Figure 1: The Two Major Categories of Identity	8
Figure 2: Digital Identity Composition.....	9
Figure 3: Literature Review Process.....	14
Figure 4: The Seven Themes from the Literature Review	15
Figure 5: The End-to-End Trust Model in the Interactions Between the Digital and Physical Worlds.....	28
Figure 6: Methodology Process Followed Thematic Analysis	35
Figure 7: Adapted Thematic Analysis Framework.....	37
Figure 8: Transcripts to Open Coding Relationship	40
Figure 9: Open Coding to Axial Coding Relationship	40
Figure 10: Axial Coding to Themes	41
Figure 11: The Four Major Themes from the Interviews	47

ABSTRACT

Cybersecurity threats and compromises have been at the epicenter of media attention; their risk and effect on people's digital identity is something not to be taken lightly. Though cyber threats have affected a great number of people in all age groups, this study focuses on 55 to 75-year-olds, as this age group is close to retirement or already retired. Therefore, a notable compromise impacting their digital identity can have a major impact on their life.

To help guide this study, the following research question was formulated, "What are the risk perceptions of individuals, between the ages of 55 and 75 with no IT background, pertaining to their digital identity?" The literature review helped identify seven themes that served as a base to generate a series of qualitative interview questions. Twenty interviews were conducted, transcribed, and coded following the Adapted Thematic Analysis framework, which resulted in four themes that answered the research question.

The themes relevant to the research question were: People accept the risk when it affects their convenience, people are concerned that companies are not being transparent with regards to being good custodians of their digital identity, people are aware of the availability of tools and training to help manage the risks, people want more transparency and control over their digital identity to help ease their concerns of the risks.

The findings from the literature review and the interviews led to a series of interpretations that validated the gaps found in the literature review. Notably, the quarantine caused by the unexpected event (i.e.: COVID-19 pandemic) forced people to an all-time high adoption of the

internet. People were aware of the risks pertaining to their digital identity, but their level of awareness varied. This gap developed the need for a personal risk assessment framework and the need for a benchmark of user-friendly best practices to help mitigate the risks. The increased adoption of new technologies similar to machine learning, artificial intelligence, and distributed ledger technologies like blockchain will help in creating more of a transparent ecosystem to interact online as well as reduce human intervention in reacting to and mitigating cybersecurity risks affecting digital identity.

CHAPTER ONE:

INTRODUCTION

Background

Cybersecurity breaches have been on the forefront of multiple newspapers, magazines, and other news outlets (Hodge, 2019). According to the Identity Theft Resource Center's (ITRC) 2019 Data breach report, between 2010 and 2019, the number of cybersecurity breaches, as well as the number of personal records exposed, more than doubled. In 2018, the ITRC reported that approximately 500 million records globally were exposed to bad actors (Identity Theft Resource Center, 2020) (See Appendix A for the statistics graph).

Cnet magazine, a prominent, technology-focused news outlet for information technology professionals, stated in one of its late 2019 articles that security breaches in companies like Amazon were caused by negligence. Additionally, these breaches left millions of users' data compromised to be bought and sold by the highest bidder of bad actors online, whom their purpose for acquiring this type of information, may lead to very undesired consequences for their victims.

The words "unsecured database" seemed to run on repeat through security journalism in 2019. Every month, another company was asking its customers to change their passwords and report any damage. Cloud-based storage companies like Amazon Web Services and ElasticSearch repeatedly saw their names surface in stories of negligent companies -- in the fields of health care, hospitality, government and elsewhere -- which left sensitive customer data unprotected in the open wilds of the internet, to be bought and sold by hackers who barely had to lift a finger to find it. - Cnet Magazine (Hodge, 2019)

Digital identity became the center of all the data breaches, as personal information was placed into the hands of unwanted parties and bad actors. People do not realize the severity and the effect of these data breaches, especially the post mortem of an identity theft event, until they hear it from someone first hand. Below is an article excerpt from an interview with an identity theft victim and the pains she experienced because her identity got compromised.

Example of an Identity Theft Victim

The article excerpt below is an extract from Forbes's website titled 'Someone Had Taken Over My Life': An Identity Theft Victim's Story. It illustrates the pains and suffering identity theft victims go through from the moment their identity gets compromised to the tedious cleanup process post-incident.

'Someone Had Taken Over My Life': An Identity Theft Victim's Story How did you first realize you were a victim of identity theft?

In February 2013, I came home after work on a Friday and received a phone call. I had gotten a

call the day before as well from a major credit card company asking me to call them, and I initially thought that that was fraudulent. I thought, 'Oh sure, I'm going to call this credit card company and talk to them about my account.'

[Sarcastically] I thought it didn't seem legit.

They said, 'We flagged this. We'll deactivate the card.' Even though there were all these flags, they still sent the credit card out to this address that was not mine. I hung up, and I thought, some lunatic has all my info. Do I call the police? Do I check my credit report? I decided, I'll check all three of my credit reports and see what the damage is, and then I'll follow up with the police.

There was no relaxing from that point on. It's been almost two years, and it's still like it just happened.

I went to Equifax, Experian and Transunion, and you're supposed to answer four security questions, which should be easy if it's you: Which of these four addresses have you lived at? Which of these employers have you worked for?

I couldn't get to two of my reports because she had infiltrated my credit history to the point that her information overrode mine.

So then what did you do?

That weekend, I placed a fraud alert on my credit reports, and I eventually froze them. With an alert, you get calls, and the next day I got multiple calls. I would get a call from Discover: Someone just called, it sounds fraudulent, you have a flag, did you just call? No.

Like, five months ago, I ordered my credit reports, and lo and behold, there's a medical collection agency. That one scares me more than any of them — to think she utilized my Social Security number to get medical attention. That's a whole other realm. It's a different animal.

How was the thief caught?

She was not a Mensa card-carrying person. She was very easy to track down. She had cable turned on at her apartment. Goods and services were mailed to her address. And when she signed up for a utility or phone, she used her name. Since it was linked to my Social Security Number, it updated it with fraudulent information. That's why I couldn't access my credit reports initially.

They had all of her information. It even had a past employer where I never worked.

The police department built a case against her, a warrant went out for her arrest, and a neighboring community arrested her.

She initially did not plead guilty. So, we had to go through the municipal court, grand jury, and the grand jury indicted her, and then pretrial and trial. She eventually did plead guilty, but since it's a non-violent felony, she did not serve jail time. She did community service, which is all the more infuriating, because identity theft is a revenue stream for criminals, and this outcome means it's much easier to be a criminal of identity theft than a criminal manufacturing drugs.

How have you been cleaning this up?

All companies have different ways in which they have you prove that you are who you say you are. When you are a victim of identity theft, you are put in the position of having to prove who you are to a greater extent than the criminal had to get goods and services. You're treated like you're trying to get out of paying for something.

One company wanted me to release the company and its affiliates, representatives' agents and employees to contact and obtain information from all references — personal, professional, employers, public agencies, licensing authorities and educational institutions, and it goes on. Here I am, a victim of identity theft, and I have to contact my employer and where I went to school? I hold the companies just as responsible as the criminal. I think there's a lot more due diligence they can extend at the onset. A number of companies were able to flag and say, this is identity theft, but a number of companies allowed it to happen. We hear about a hacking here a hacking there and are becoming accustomed to them. These companies can't just throw out the latest and greatest technology and say, this is going to make things easier for you. How might this affect us negatively? Who can get access to this? The companies make transactions easier for themselves, yet I and millions of others are stuck cleaning up this mess.

The government isn't much help either. You're bounced around from agency to agency: If you're an identity theft victim, here are the 400 steps you have to do.

How did this experience make you feel?

It's the most time-consuming, upsetting, emotional event you have to go through. Somebody went in and so easily removed my information and had their information override mine on this all important, encompassing document — my

credit report. You're told from a young age to establish credit responsibility so down the road, you can make a big purchase like a vehicle or home. Meanwhile, some lunatic has barely any information about me and gets access to all these goods and services — yet I have to go fill out all these affidavits and turn in my utility bills and all my personal data to remove this fraudulent charge. The companies didn't ask anywhere near that when they extended the credit. But now that it affects their bottom line, they turn around and make me do all this.

What advice would you have for others to prevent identity theft?

Be cautious with your information going forward. I always have been cautious, so I can't do anything differently. Even if you do all the right things and shred things, and ask all the right questions, that won't prevent you from being a victim. Wherever your information is held — where you file taxes, where you buy a car, go to school, get a job — they have your Social Security number. (Shin, 2014)

This article clearly highlights the severity of identity theft and the potential damage the cybersecurity breaches of personal data can cause. Thus, the motivation and purpose of this study are to listen to the voice of the people and gauge their awareness with regards to threats pertaining to their digital identity.

Statement of Purpose

Purpose

The purpose of this study was to explore people's awareness of the risks associated with their digital identity, including their online personal data and online interaction. The goal was to develop a baseline of themes pertaining to participants' knowledge of the risks associated with their digital identity as well as the means to help support the management of digital identity, online personal data, and online interactions.

Relevance

For this research to be relevant and interesting for people to read, there was an equal focus on practitioner and industry literature as on academic research. In his book *Qualitative Research in Business Management* (2013), Michael Myers highlighted the comparison between rigor and relevancy. The author stated that academic research tends to be rigorous; the more

rigorous it becomes, the less relevant it is to practitioners. In this dissertation, the focus was on bridging rigor and relevance while keeping the content relevant to the reader and the current business environment (Myers, 2013).

The Motivation for the Study

The motivation for this research study was instigated by the principal investigator's years of professional experience. The principal investigator spent more than ten years interacting with people and clients as an information technology-focused management consultant. The principal investigator recognized people's concern of not knowing enough about their digital identity and the impacts of its risks; this concern and risk sparked the interest to conduct this study. The principal investigator found a gap in the academic literature in regards to the voice of the people. As a result of this gap, the principal investigator decided to conduct this exploratory study to investigate what people know, with the hope of understanding why they know what they know and the gaps that need to be filled, to further enhance the awareness and management practices of digital identity risks and its attributed characteristics. While conducting this study, many biases and assumptions were made that affected the process and its outcome.

Researcher Bias and Assumptions

A bias to be considered in this research study is the principal investigator's work in the information technology industry. As a practitioner, the researcher consults with the management and C-suite executives managing the information technology (IT) and cybersecurity departments of small to large scale organizations, with more than a trillion dollars in their annual budget.

The author's background and experience as well as the researchers' knowledge of industry best practices and government-issued guidelines, laws, and regulations, influenced the insights that drove this study. The principal investigator leveraged publicly available information

as well as the University of South Florida's library access to resources when searching for literature about this study.

With regards to interview participants, the principal investigator relied on personal connections when he identified participants for this study, due to the quarantine imposed by the government caused by the unpredicted global COVID-19 pandemic. This quarantine caused the limitation of interviewing people via Zoom, which presumed that people had a computer and basic computer literacy to participate in this study. The unpredicted event variable and the solicitation of participants via online channels affected the outcome of this study, as research participants were comfortable with spending time online, possibly more than an average person in their age category.

Research Question

To help guide this study, the principal investigator used the following research question as a driver to keep the study focused: "What are the risk perceptions of individuals, 55 to 75-year-old with no IT background, pertaining to their digital identity?". This study sought to explore the risks people are aware of pertaining to their digital identity, specifically, people between the age of 55 to 75, as they are close to or already retired. Therefore, any major event in their life relating to the loss of assets would be hard to recover from in a short period of time.

This research question was answered by conducting a literature review to determine what literature was published by academics and practitioners in this area. The participant interviews were used as a validating mechanism to the findings in the literature by summarizing the findings into themes that would help answer and support the proposed research question. To help establish the stage and provide a background of some topics discussed in this study, chapter two

is used as a high-level guideline that helps define and contextualize some of the terminology to understand the topics discussed in this study.

CHAPTER TWO: ABOUT IDENTITY

Identity

Defining identity is somewhat of a controversial topic. Different dictionaries give identity distinct definitions (Cambridge English Dictionary, 2020; Merriam-Webster, 2020b). The commonalities lie in associating human behavior to personas or personalities that are uniquely associated with individuals. Associating behaviors, actions, and interactions attributed to what can be associated with an individual uniquely identifies a person and is part of his or her identity.

Identity can be divided into two categories: physical and digital identities, as illustrated in the diagram below. They are the two essential identity aspects identified in the literature (Alashoor, Baskerville, & Zhu, 2016). Associating the physical with the digital is very important to increase the trust and authenticity of digital interactions (Camp, 2004).

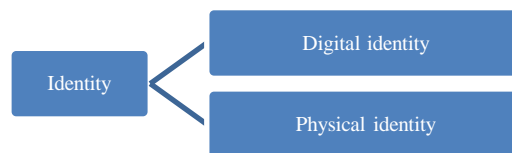


Figure 1. The Two Major Categories of Identity.

Digital identity encompasses online personal data and digital interactions described in the diagram below. Digital identity contains personal identifiers, attributes, and digital relationships and interactions (Alashoor et al., 2016).

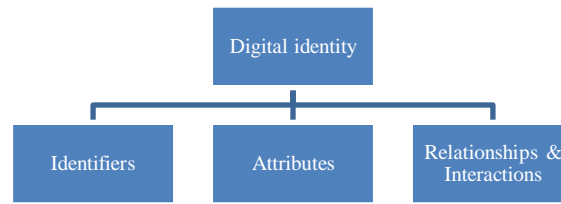


Figure 2. Digital Identity Composition.

Due to the continuous improvements and discoveries as part of the evolution of technologies, the definition of digital identity is continuously changing with technology enhancements. What is valid currently might not be valid in the near future; it may likely evolve or morph into a different definition. Likewise, the description of digital identity will probably change with time (Sullivan, 2018).

From an academic perspective, researchers have tried different approaches to identify the online attributes of digital identity and their economic impacts (Mueller, Park, Lee, & Kim, 2006).

Sullivan, a renowned researcher in the digital identity space, explored digital identity from a legal perspective and highlighted the necessity of the right to have a digital identity for everyone from an international perspective (2018).

Trust is very important in online interactions. Establishing trust is critical when bridging the gap that associates digital and physical identity together. Researchers have tried to define digital identity, its problems, and the issue of trusting it in cyberspace while considering the different aspects of digital identity when authenticating the digital with the physical (Katzan, 2011).

Privacy

Privacy is defined by the Merriam Webster English dictionary as the “freedom from unauthorized intrusion” (Merriam-Webster, 2020a). It is the right of a person to be let alone if

the individual requests it. To understand how privacy relates to the individual, understanding personal data privacy is essential.

Personal data privacy is construed to be the freedom of personal data from unauthorized intrusion (International Association of Privacy Professionals, 2020). When personal data privacy gets mentioned in social circles, most people refer to the massive data breaches that affect large organizations. The intrusion of wearable technologies, including Apple's Siri and Amazon's Alexa, as well as the intrusion to privacy that online social networks cause amplify the effect of data privacy intrusion (Srivastava & Geethakumari, 2013). Thus, it is important to understand data privacy risks.

Data Privacy Risks

Facebook, Target, Experian, Marriott, Amazon, and many other Fortune 100 organizations were victims of cyber-attacks or were involved in leaking personal data unintentionally or intentionally to third-party organizations. These fortune 100 breaches are among the cases of personal data compromises that have led to personal identifiable information (PII) being exposed to unwanted parties. One of the most recent breaches that exposed millions of records is the Marriott breach from 2018 (Perlroth, Satariano, & Tsang, 2018). The New York Times featured this breach on its front page on December, 2018, because of its severity and implications to millions of people globally where Marriott had a presence. The abstract of the front page article is below:

The hotel chain asked guests checking in for a treasure trove of personal information: credit cards, addresses and sometimes passport numbers. On Friday, consumers learned the risk. Marriott International revealed that hackers had breached its Starwood reservation system and had stolen the personal data of up to 500 million guests. (Perlroth et al., 2018)

Internet users run into the problem of having control and losing track of their personal data used and disclosed online. Losing control of online data creates a high risk and increases the probability of data being found in the hands of unwanted parties. There is also an emerging risk attributed to a multitude of websites, applications, and software requiring login credentials and personal information that cause users to lose track of what data they stored on what platform (Florencio & Herley, 2007).

Professionals are busy and have a short memory span; they cannot remember what information they stored on what website (Florencio & Herley, 2007). The necessity to stay on top of the information provided to different web applications becomes essential with every new application used to maintain visibility over digital personal data and reduce risks as recommended by the National Institute of Science and Technology's Cybersecurity Framework (National Institute of Standards and Technology [NIST], 2018a). Similar to NIST, governments around the world started to take action to pass privacy-related laws and regulations.

Privacy Laws, Regulations, and Frameworks

Different countries, like the United States and the European Union, passed laws to address the gap in regulations. They have all been segregated initiatives to try to protect digital information and identities. With the emergence of these rules and regulations, people lack the awareness of what these rules do and what kind of risks they help protect them against (Sullivan, 2018). One recently published law that had a significant impact internationally on digital personal information is the enforcement of the General Data Protection Regulation in the European Union (European Union, 2016).

The National Institute of Standards and Technology (NIST) put together a framework, NIST 800-63-3, explaining digital identity and its attributes. In essence, the framework was

geared towards enterprises and United States government agencies, to be used as a guideline to manage digital identity and authentication mechanisms. This framework defines digital identity as well as its attributes and minimum technological use standards (NIST, 2017).

The NIST cybersecurity framework (NIST CSF) defines and serves as an overarching model for the cybersecurity readiness of an enterprise. It includes modules that assess the cybersecurity readiness of an organization but can also be applied to individuals, specifically the awareness and training modules, which applies to individuals being aware of risks and being trained to identify cyber risks (NIST, 2018a).

Digital Identity Management

Digital identity management includes the use of cybersecurity tools, as well as training and awareness, in order to help with managing cyber risks.

Cybersecurity training, available on the market, attempts to establish a baseline of awareness among its recipients. Phishing training and awareness were created as a way to make people more aware of known hackers techniques that are utilized to steal people's information and compromise their personal data (Higashino, Kawato, Ohmori, & Kawamura, 2019).

Several tools and solutions to manage aspects of digital identity, similar to LifeLock and LastPass, emerged in the last ten years. The tools on the market that help in managing digital identity and enhance people's awareness and visibility over their digital identity are lacking; they need to be more user friendly in order to increase their adoption (Choi, Wang, & Lowry, 2020).

Several aspects covered in this chapter leave a lot of intriguing ideas to be further explored in detail from the lens of academics and practitioners in the literature review chapter that follows.

CHAPTER THREE:

LITERATURE REVIEW

Overview

The literature review process started with a search around digital identity and the risks pertaining to online interactions. The search resulted in more than 300 articles; some were relevant to the topic, and some were not. After careful consideration of the articles from the search, a handful was selected as the base to build the foundation of the literature review by looking at the relevant articles describing digital identity and its risks.

The process of the search started with using different keywords in the Proquest ABI/INFORM Global search platform; the keywords and keyword combinations are: "digital identity," "digital identity AND risks," "online personal data," "online personal data AND risks." The preliminary search was conducted through ABI/INFORM using the stated keywords, performing an abstract, peer-reviewed, full-text search. Then, articles were sorted through and filtered appropriately. The rest of the literature sources came from second-hand references within the first set of articles found in the search as well as cybersecurity industry known sources and articles found in different academic and practitioner conferences attended.

After selecting the appropriate academic articles as well as finding sources commonly used by practitioners in the cybersecurity industry, the next step was to perform an analysis of the themes of the articles found in the literature search to find overarching, common themes to categorize and illustrate in my literature review.

The analysis of the themes found helped synthesize the findings that constitute this literature review. The goal of synthesizing findings was to prioritize and filter through the appropriate themes and topics that appeared in the literature as relevant to this research. To conclude, gaps pertinent to the findings in the literature were highlighted to justify the reason for conducting this study and its important contribution to academia and practice.

The figure below depicts the process followed for the literature review.



Figure 3. Literature Review Process.

Themes from the Literature

Seven themes, illustrated in figure 4, were discovered during the literature review process that tell a very intriguing story. The story debuts with how the wide use of the internet caused an increase in the use of digital identity, which led to the creation of different ways to mitigate the risks this spike has caused.

The full story that the themes found in the literature review convey starts with the increased usage of the internet that created a gap that needed to be filled by personal online identifiers and digital identity to facilitate the expansion and ease of use of the online medium. There have been many definitions of digital identity. The broadest term definition is synonymous with the physical identity but in the digital world, along with a series of attributes that make it more valid and unique. With the rise of digital identity and online personal data, there were different thoughts and perspectives that sprouted to try to justify and promote the use of digital identity. With more usage over time, personal identifiers online created a plethora of privacy risks that affected people and their digital identity as well as physical properties and value-based personal property. To mitigate those privacy risks, governments and private organizations tried to

establish a set of rules and regulations to support and help protect people's privacy and personal data. That set of rules and regulations created the need for a group of best practices and appropriate training. The training in the workplace and best practices published for end-users made people unconsciously acquire habits and form behaviors in their risk-based decisions when using the internet and its peripherals or internet of things (IoT) devices. Those newly formed habits and best practice behavior needed to be complemented and enabled with a series of tools and training to help support and make the end-user more aware of the risks and mitigations available on the market to safe-keep personal digital information.

The seven themes from the literature review findings are illustrated in the figure below:

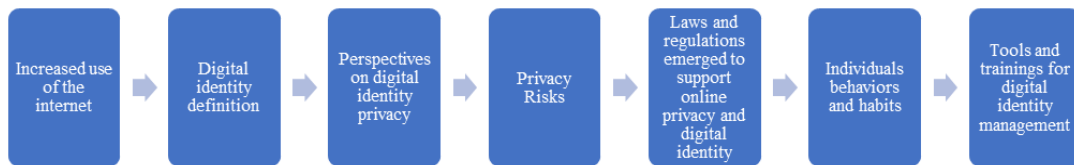


Figure 4. The Seven Themes from the Literature Review.

Theme 1: Increased Use of the Internet

The increase in internet usage enabled the facilitation of daily life tasks. According to Mueller and Sullivan, participating in societal activities requires people to use the internet in some way, shape, or form to facilitate everyday life (Mueller et al., 2006; Sullivan, 2014). This increased usage of the internet created a need for an enabler in the form of a unique identifier of people, and thus, digital identity came to be (Mueller et al., 2006). The internet has created the need for a medium to help in managing people's digital identity and online interactions. Hence, it caused the creation of digital identity as a solution to enable the boost of the full use of the capabilities of the internet (Sullivan, 2014).

As technology became an integral part of life, whether people are waiting at the doctor's office, in a public area for a friend, or for a football game to start, people tend to want to be connected through mobile phones or other IoT devices (Colbert, Yee, & George, 2016). With this increased usage of the internet and IoT devices came the increase of digital interactions and the need for digital identity. To enable this unavoidable medium called the internet, people have to use some sort of a unique identifier, like a username and password, to be able to be authenticated online and use email, bank accounts, bill payment platforms, and different services available online (Mueller et al., 2006). This increased internet usage caused the rise of risks and challenges to maintain information privacy (Sullivan, 2014). The rapid expansion and wide use of the internet, and every peripheral attached to it called IoT, caused new challenges to privacy and security protection (Choi et al., 2020). People knowingly or unwittingly disclose their personal information, but whether they are aware of the risks is further discussed in this study.

To help in solving the problems that sprouted from the use of digital identity, a proper definition is needed to help understand digital identity.

Theme 2: Definition of Digital Identity

To properly define digital identity, there is a common consensus among academics and practitioners that properly bridging between the physical and digital worlds is very important (Camp, 2004; Papangelis et al., 2020). To authenticate that connection, the digital has to be associated with the appropriate physical identity to validate that connection. Similar to digital identity, physical identity has a series of identifiers and attributes that associate with an individual (Mueller et al., 2006). To use the internet safely, there needs to be authentication and continuous authorization in place, between the physical and the digital, to mitigate some of the risks in wrongfully associating the proper physical person to their digital identity (Camp, 2004).

The way we identify a digital object as being what it purports to be and the criteria to continuously identifying it over a period of time is essential to maintain its credibility in the digital world; it is an ongoing authentication process (Allison, Currall, Moss, & Stuart, 2005). To understand the composition of digital identity, as illustrated in figure 2, there needs to be a better definition of identifiers, attributes, and digital relationships.

An identifier is something specific and uniquely associated with an individual. In some cases, identifiers can be a Social Security number, a birth certificate, a passport number, or any other type of identifier that is unique to the individual and can distinctly identify a person if that identifier is disclosed (Camp, 2004). Identifiers are only valid and meaningful when they are associated with the person they identify. A set of identifiers can be associated with an individual. In most cases, identifiers are difficult or impossible to alter (Mueller et al., 2006).

An attribute is a characteristic associated with an individual. Some of those characteristics involve hair color, eye color, vehicle identification number (VIN), make and model of vehicle driven, and home address. Any other group or series of behaviors attributed to an individual are also part of attributes. The series of behaviors can be the act of merely visiting the same websites daily in a particular sequence, credit card purchasing patterns, or a group of places frequently visited (Camp, 2004).

There is a common perspective that a person and his or her identity have a one-dimensional relationship (Gunasinghe et al., 2019). A person's privacy directly relates to the privacy of his or her identity; this uniform relationship between the privacy of the person and the privacy of the person's identity creates multiple levels of complication in privacy protection efforts. Three different levels emerge in the literature when defining identity (Alashoor et al., 2016); the first level is the individual; the second level is the relationships associated with the

individual, and finally, the relationship of the individual to a group. The individual can be placed within the identifiers' category, and the other two under the attributes category. To manage the different types of identities; there is a relationship between the physical, the personal, the social, and digital identities that should be considered and are essential to understand the relationship of privacy between the different layers (Alashoor et al., 2016).

The different definitions found of digital identity from the perspective of academics and practitioners manifest in the association of the physical to the digital world, taking into consideration the different identifiers, attributes, and behaviors of the individual. After identifying the basis of what is digital identity, there is a need to understand how people and organizations perceive digital identity and its impact on privacy.

Theme 3: Perspectives on Digital Identity and Privacy

With the increased and wide use of digital identity, there was a consensus among academics and practitioners that digital identity had impacted people's lives as well as organizations and governments. Digital identity impacted the privacy of people, organizations as well as societies and governments, notably from a reputation and financial aspect with potential legal repercussions.

Sullivan, a prominent researcher on the matters of digital identity and law from Georgetown University Law Center, states that the misuse of digital identity attributes affects the integrity of digital identity. That impact can cause long term damage to a person's reputational, legal, and commercial standing, online as well as offline (Sullivan, 2016). To help in understanding the potential implications of a digital identity compromise, it is helpful to understand the categories of personal information.

As part of digital identity, online personal information got segmented into three categories that are notably identified and discussed in the industry. Personal identifiable information, or PII, is a category associated with unique information about an individual (U.S. Department of Labor [DOL], 2020). Some Digital identity attributes, as well as identifiers, fall within this category. Another major category is personal protected health information, or PHI, which deals with the health records of individuals (U.S. Department of Health & Human Services [HHS], 2015). Finally, financial information is covered under the category of personal financial information, or PFI, which is mainly a category that includes unique personal information on individuals' banking information, data of credit, debit, or other transactional payment related personal data available online (Federal Trade Commission [FTC], 2012). The compromise of PII, PHI, and PFI can have a very undesirable effect on people's lives.

Hence, people are wary about using the internet. There is a common perspective among people that their online personal data, activities, and behavior are being tracked by unwanted parties. Whether it is from hackers, organizations, or governments, people are wary that their online data and digital identity are being misused, and they feel that they cannot do much about it (Auxier et al., 2019). Organizations realized that the cybersecurity threats they constantly deal with are, in one aspect, tied to their employees.

As individuals, for the most part, are associated with organizations that they belong to. Whether their workplace or some other organizations they are affiliated with, the digital identity and online interactions attributed to individuals indirectly affect the organization (Horn et al., 2015). Therefore, organizations started to take action and put together a set of rules and guidelines for their members, affiliates, or employees to try to give them guidance, awareness, and best practices on how to behave online to reduce the risk that can impact those organizations

from a reputational or financial perspective (Paulsen, McDuffie, Newhouse, & Toth, 2012). As a result, governance plays a role in managing the risks pertaining to digital identity.

As digital identity is further adopted, governments from around the world are using it to leverage the increased usage of e-government applications to streamline their services (Sullivan, 2016). Countries from around the world, like the United States, Estonia, and several others, started initiatives to switch most of their services to e-government platforms to facilitate the access and ease of the usage of government services (Dutil, Howard, Langford, & Roy, 2007). This effort will reduce the levels of corruption in countries facing that problem. With the increased usage of online services, there is an increased need for privacy and tighter security to protect people's data and keep it secure (Woodhouse, 2007).

Privacy becomes essential as digital identity use widens (Sullivan, 2014). Digital identity is impacting the way the government and the private sector operate. Introduced by Sullivan, The term "transaction identity" surfaced as using digital identity as a medium of digital transactions between individuals and governments as well as companies in the private sector (Sullivan, 2016). Transactional identity is important in leveraging digital identity as a medium to authenticate and validate the different parties involved in a transaction (Sullivan, 2016).

Just like any information system, using digital identity for conducting transactions online and trusting those transactions requires understanding its ontology to reduce the risks (Alsaedi, Stefanidis, Phalp, & Ali, 2019). The ontology of trusting personal data and digital identity in cyberspace is a subject that scholars, like Katzan (2011), have explored. For information to be secured and trusted for its authenticity in cyberspace, the CIA triad security model is identified in the IT security industry as a framework to keep personal data secure. The balance between the three focuses, confidentiality, integrity, and availability of data (known as the CIA triad), is

important to maintain information security (European Union Agency for Cybersecurity, 2020). Confidentiality relates to the limitations on information access and disclosure. Integrity refers to the controls that limit information modification. Availability is timely and reliable access to information whenever it is needed on a system (Katzan, 2011). With identities migrating to digital platforms, organizations and citizens need to be able to transact with reduced friction as more counter-bound services move to online delivery (Wolfond, 2017).

Digital identity created some legal concerns for maintaining online privacy. To help frame the problem to solve it better, practitioners segmented personal data into PII, PHI, and PFI in order to address the concerns in a more structured, efficient approach. This structure created an understanding and helped appease people who are always afraid that their personal data is continuously tracked online by unwanted parties. The increase in electronic government services created a demand for a more secure digital identity and raised privacy concerns as well. To ensure that online data is secure, confidentiality, integrity, and availability are essential characteristics of ensuring information accessibility, privacy, and security. Once the ontology of trusting digital identity in cyberspace is understood, privacy risks need to be explored further.

Theme 4: Privacy Risks

The different perspectives discussed in the literature with regards to digital identity privacy and the more widespread use of digital identity and online personal data sprouted a wave of risks and concerns around securely using the web and interacting with online platforms while limiting privacy risks.

To put online privacy risks in context, academics like Daeen Choi (2020) stated that the concern of online privacy risks created a substantial need for defining and measuring privacy risks. Practitioners, including Chen, Beaudoin, and Hong (2017), define online privacy risk by

who you are, what you do on the internet, and the risks associated with who you are and what you do that impacts your digital behavior negatively. When measuring risk, practitioners like Rossi (2007) try to quantify it in a way that can be measured tangibly. Risk is calculated using the formula of the probability of the risk occurring multiplied by how much it would cost in damages to mitigate against the risk. Properly measuring risk is a step towards building awareness to adequately form mitigation measures. Even without proper measurement of risks, people do not seem to be deterred by the threats to digital identity.

Researchers like Hsu and Lin (2016) agree that privacy and security risks do not appear to influence consumers' behavior in purchasing internet-connected devices. People will still perform risky actions online, even if they know the harm (Choi et al., 2020). The challenges in privacy-related decision making related to being misinformed about privacy risks make privacy and security protection difficult. The lack of cognitive ability and various cognitive biases regarding privacy risks also pose a threat to proper risk mitigation (Choi et al., 2020). Digital identity risks can be caused by multiple avenues online, with online social networks being a major cause of concern.

Some researchers (Kim, Baskerville, & Ding, 2018) assert that the owners of online social networks do not hold much data that cause risk with regards to the privacy of the individuals or the social groups they are affiliated with. Others (Granville, 2018) disagree with this assertion because of recent events from multiple social media platforms, including Facebook, that sold their users' data to unwanted, undesired parties that misused people's information and caused worldwide scandals. Also, some risks are caused by bad actors online.

In addition to people's information being shared online by different online platforms, risks arise from hackers stealing people's information from the various online platforms; this

information includes credit card information, Social Security numbers, and personal health records. Practitioners express that this information can be sold on the dark web, which equates to the illegal online trading or commerce medium and can sometimes total several thousands of dollars, depending on the value of the information and who it belongs to (Stack, 2017).

Individuals can get their identity stolen online; as a repercussion, they can incur financial, reputational losses or cause harm to others via the groups they are associated with, like organizations they work for or belong to. The goal of some hackers is to steal personal information of important people via compromising other individuals who belong to the same group as those public figures. Sometimes, these risks can cause significant damage to organizations as well as nations (Kahn & Liñares-Zegarra, 2016).

As a consequence of the manifested risks, governments like the United States and the European Union had to ask the people in charge of online social media platforms, Facebook being the most notable, to testify and justify what they are doing, to the extent of imposing hefty fines to offset their wrongdoings (“US fines,” 2019). In 2018, Amazon, one of the world's largest companies, launched an internal investigation into some of its employees, offering subscribers’ data to some merchants to help them increase their sales on the website without subscribers’ consent (Emont, Stevens, & McMillan, 2018).

According to researchers, consumers did not change their behavior after learning that some of their online interactions can cause them harm. Hence, people's perspectives regarding their digital identity created a need for the industry to define and measure personal privacy risks. A contradiction of opinions between academics sprouted regarding the risks related to online social networks while considering the scandals that Facebook and Amazon encountered by misuse of people's personal data. A gamut of other risks, including financial and reputational

risks, come into play when considering personal digital identity. Many of the most prominent companies in the world were reprimanded by governments like the United States and European Union for mistreating people's personal online data. Governments in various countries passed a range of laws to help protect people and organizations against online risks.

Theme 5: Laws and Regulations Relating to Privacy and Digital Identity

Due to the various privacy risks that emerged from the misuse of digital identity, as well as online identifiers, governments had to react to provide some guidelines in the form of laws, rules, and regulations to help protect people's privacy. Multiple governments around the world, including the United States and the European Union, started to establish rules and regulations that would limit the abuse of people's personal data and give individuals more leverage by consenting to those organizations to disclose their personal data (Schwartz, 2013). With the increase of electronic government services and transactions, governments had to intervene and solidify their positions with laws that help create some standards for rules of engagement to reduce the compromise of the integrity of an individual's digital identity (Sullivan, 2015).

A notable initiative from a government organization is the European Union general data protection regulation (GDPR). For years, the European Union (EU) data protection laws have been ahead of the rest of the world. In 2016, the European Union adopted GDPR as an upgrade to their previous Data Protection Directive, which was adopted in the early stages of the internet. At its launch, GDPR gave the different EU members until May 2018 to comply.

GDPR increases the level of an individual's privacy protection with regards to how the data is collected, stored, processed, and used by different online platforms and organizations (European Union, 2016). GDPR gives individuals more control over their online data by emphasizing the need for transparency when companies retain personal data; it also gives

individuals the right to obtain confirmation that their data is being used. Additionally, the GDPR provides individuals more control over the personal data that organizations store on their behalf. These organizations would not be able to use the data without the individual's consent, or details are provided to individuals regarding how their data was used, and their approval is obtained on how it was used. GDPR is definitely a step forward towards a more user-centric internet (Sobolewski, Mazur, & Paliski, 2017).

The U.S. government also passed laws to protect privacy. The first law with regards to data privacy was passed and published in 1974; it was the U.S. privacy act of 1974 (Privacy Act, 2014). This law was geared towards data held by U.S. government agencies and the right of U.S. citizens to access that data as well as limitations on sharing data with other federal and non-federal agencies. Then, the government passed HIPAA, which is the Health Insurance Portability and Accountability Act, in 1996; it was targeted towards the regulation of health insurance as well as ensuring the privacy and protection of individual's health records. HIPAA had some important sections on data privacy and security as well as defining PHI in its Privacy Rule section.

In the late 1990s, the Gramm-Leach-Bliley Act (GLBA) passed through legislation; it was mainly geared towards banking and financial institutions' regulations. The GLBA protects nonpublic personal information or personal identifiable information (PII). The GLBA forced banks and other financial institutions to regularly mail out privacy notifications to their customers along with special opt-out instructions if they do not like their personal information being shared with non-affiliated third parties (Gramm-Leach-Bliley Act, 2002).

As a supplement to many federal laws, some states, like California, took the initiative to create their own regulations. One example is the California Consumer Privacy Act (CCPA),

which was signed into law in 2018. The CCPA gives consumers additional rights for privacy protection and holds businesses accountable to not sell personal information of their clients without providing a disclosure notice and giving them the opportunity to opt-out (California Consumer Privacy Act, 2018). Similar to the GDPR, the CCPA includes a "right to delete" clause, which allows people to request their data to be deleted or removed from certain online platforms. Other states, like Massachusetts, New York, Hawaii, and Maryland, have followed suit and passed their own laws to help protect individuals' online data and privacy as well as their digital identity (Green, 2019).

From a best practices guidance perspective, online personal data privacy became such an issue that NIST established a privacy framework that serves as a guide for organizations in helping them ensure their cybersecurity posture is robust enough to help protect individuals' online personal data (Legal Monitor Worldwide, 2020). This approach is a double-edge, where if organizational data gets compromised, that impacts the individuals associated with that organization, whether they are employees or customers, and vice versa. If employees or customers get their data stolen, it might affect organizations they belong to or interact with (Legal Monitor Worldwide, 2020). The National Institute of Science and Technology also published the cybersecurity framework, which gives guidelines to organizations on how to protect their data and the data of their employees and customers. Some of the main domains of this framework are the use of cybersecurity training and awareness to keep employees from compromising their company systems, which indirectly compromises their personal data and the personal data of customers. Some training is referred to as phishing protection training, password best practices, and proper cybersecurity behavior online (NIST, 2018a).

To protect people's digital identity and privacy, governments and the private sector have created a series of laws, regulations, and rules to help people know the right behavior and what is inappropriate to act on and disclose online. The hope is to set a benchmark for governments, organizations, and individuals to operate on with regards to personal online data and digital interactions.

Theme 6: Individuals Behavior and Habits

People have developed habits and expected behaviors that are formed from their regular use of the internet. That behavior is not always geared towards the best of their interest and the highest level of risk mitigation techniques, even after governments and private organizations issued guidelines and best practices for people to abide by. People normally struggle with changing their previous habits to adapt to new behavior to conform to best practices, rules, and regulations.

Over time, people who do not have a system to maintain and keep track of their multiple online accounts tend to forget how many accounts they have opened (Brown, Bracken, Zoccoli, & Douglas, 2004). People tend to forget online accounts that they do not continuously use and maintain. Every account opened online tends to have a username and a password associated with it (Gaw & Felten, 2006). Those unique identifiers are aimed to identify the individual users of the different platforms uniquely. As people forget the accounts they have online; there is a tendency to forget the passwords set up for the various online accounts (Florencio & Herley, 2006).

If they are not aware of the risks of clicking unsafe links online, people's online behaviors default to being overly trustworthy and clicking on phishing scams through their emails or different social media (Dhamija, Tygar, & Hearst, 2006). Phishing attacks happen when hackers

target users with emails and other messages as a mechanism for stealing people's personal information as well as login credentials. Phishing scams can be very harmful and damaging to people's digital identity (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010).

People have formed habits with regards to their online interactions. Like many other habits people form, some are to their best interest, and some aren't, which end up causing them financial or reputational loss. Privacy attitudes impact the kind of decisions individuals make regarding disclosing their personal information online and their willingness to use and interact with technologies that invade their privacy and share personal information with unwanted third parties. Why people continue to do so remains an uncharted topic (Bélanger & Crossler, 2011).

Theme 7: Tools and Training Enabling Digital Identity Management

To enable the proper use of the online medium and ensure the most amount of privacy and the least amount of risk to online personal information, a set of tools and essential training are needed to help users manage their online interactions with the proper behavior and an adequate toolset available to help properly manage their digital interactions.

For the internet to reach its full potential and enhance people's lives, practitioners like Charney agree that an enhanced end-to-end trust in digital interactions is needed, as illustrated in the figure below.



Figure 5. The End-to-End Trust Model in the Interactions Between the Digital and Physical Worlds.

The trust in online interactions and experiences is key to a thriving private, secure digital world (Charney, 2009). A consensus exists among scholars and practitioners around the need for

transparency and more control. Personal information management efforts in the digital world must be established through better awareness and tools to support the initiatives (Brunk, Mattern, & Riehle, 2019; Olivero & Lunt, 2004). Personal information available online should be treated as personal belongings. People need to deal with them with caution and care, which is where the need for tools to help with managing digital identity become essential (Zastrow, 2014).

Existing tools that help increase people's awareness are lacking; therefore, better methods for measuring privacy risks on an individual level to try to mitigate the risks are needed (Choi et al., 2020). The surge in technological innovations as well as the use of authentication technologies similar to blockchain for identity authentication and verification, create the need for regulated channels and laws for governing these types of new technologies that can help eliminate geographical boundaries and shift to a more global citizenship (Sullivan, 2018).

Digital identity is a major enabler for electronic government applications. Smart identity cards, similar to credit cards with an embedded programmable microchip, may serve as secure tokens that connect digital and physical identity, create trustworthy environments, and strengthen confidence in online transactions critical to the growth of the digital economy. Proper digital identity management and the user-centricity of the solutions are definitely needed to manage the online medium (Al-Khoury, 2014).

Many of the tools and training available on the market as well as research on information privacy tools and technologies, were started and conducted in isolation from the actual future users of the tools (Bélanger & Crossler, 2011). Hence, some of the tools and training solutions on the market do not consider the concept of user-centricity to facilitate and accelerate the adoption of these tools to enhance the experience of the digital interaction (Bélanger & Crossler, 2011).

In industry, tools and training emerged among practitioners as a way for risk mitigation or risk reduction regarding the use of online platforms and applications (Cooper, 2017). These tools include the use of strong passwords to leveraging multi-factor authentication techniques for adding an extra layer of security to passwords to using tools like password managers to facilitate and better track the use of username and passwords in a different online platform. These are some of the many ways the cybersecurity industry has reacted to add an extra layer of protection to online personal data and protect digital identity (Dourish, Grinter, Delgado de la Flor & Joseph, 2004).

To manage user credentials, the recommended industry best practices with regards to strong passwords involve a combination of uppercase and lowercase letters with a minimum of eight characters, including numbers (Brown et al., 2004). For an added layer of security, strong passwords need to be accompanied with some sort of a multi-factor authentication system for added security. A multi-factor authentication system enables the security of access to a platform with a minimum of two or more forms of validation. The first is usually a password, and the second is token validation that the user alone possesses; i.e: a number sent to a cell phone, a randomly generated number from a code generator similar to the Google Authenticator tool, or any other device measuring the biological aspect of the user (Anakath, Rajakumar, & Ambika, 2019). The use of password management systems integrated within internet browsers or mobile phones is becoming a technology solution to help keep track of the different usernames and passwords that people use and keep them centrally readily available whenever needed while the user only has to memorize one password to access all of their other passwords used for the different online platforms (Alkaldi, Renaud, & Mackenzie, 2019).

From a training perspective, practitioners have created a series of training and best practices for individual's consumption that train users on how to identify when hackers are trying to scam them to gain access to their data; the method is also known as phishing (Dhamija et al., 2006). Phishing training and awareness were created to make people more aware of hackers trying to get to their online data for harmful purposes (Higashino et al., 2019).

To reinforce the best practices and guidelines created by the different government and organizational initiatives around online data privacy, several sets of tools and training emerged to help in the proper use of the internet. There remains a lack of training available to the majority of online users and the adequate user-friendly tools being used to help minimize the risks of online interactions (Nurse, Creese, Goldsmith, & Lamberts, 2011).

Summary of Findings

Table 1 summarizes findings in the literature and categorizes them into themes that connect the literature together and sets the stage for a compelling argument that supports the need for this study.

Digital identity is the association of the physical to the digital world, taking into consideration the different identifiers, attributes, and behaviors of the individual. The increase in the use of digital identity created a plethora of concerns for maintaining online personal privacy. While dealing with online data, confidentiality, integrity, and availability are essential characteristics to ensure privacy and security. People's perspectives regarding their digital identity created a need for the industry to define and measure personal privacy risks. To protect people's digital identity and privacy, governments and the private sector have established a series of laws, regulations, and rules to help people know the right behavior and what is inappropriate to act on and disclose online. People have formed habits with regards to their online interactions.

Like any other habit people form, some are to their best interest, and some are not, which end up causing them financial or reputational loss. To reinforce the best practices and guidelines created by the different government and organizational initiatives around online data privacy, tools, and training emerged to help in the proper use of the internet. Questions emerged after going through the literature, from academics and practitioners. These questions pointed to a gap in the literature and formed the justification and motivation of this study.

This study aims to understand what people know about the risks pertaining to their digital identity and online interaction as well as explore how they are behaving and understand why they behave the way they do. The methodology followed to conduct this study is described in the next chapter.

Table 1. Literature Review Summary of Findings.

Theme 1: Increased Internet Usage	
Findings	<ul style="list-style-type: none"> - Increase in internet usage created a need for digital identity - Digital identity was a boost to the proper usage and interaction in the online medium
Supporting references	(Colbert et al., 2016; Choi et al., 2020; Mueller et al., 2006; Sullivan, 2014)
Theme 2: Digital Identity Definition	
Findings	<ul style="list-style-type: none"> - Bridging between physical and digital identity was essential to validate and authenticate online interactions - Digital identity constitutes online identifiers and attributes - Digital identity can have three levels of association: <ol style="list-style-type: none"> 1. The individual 2. Relationships associated with the individual 3. The individual's association to a group
Supporting references	(Alashoor et al., 2016; Allison et al., 2005; Gunasinghe et al., 2019; Camp, 2004; Papangelis et al., 2020)
Theme 3: Perspectives on Digital Identity Privacy	
Findings	<ul style="list-style-type: none"> - Digital identity impacted people, organizations, societies, and governments - Online personal data is categorized under PII, PHI, and PFI - People feel that they are always being tracked online - Governments are ramping up the deployment of digital identity initiatives - There is a need for increased security to keep people's data secure and ensure privacy - Confidentiality, integrity, and availability are important to keep personal data secure
Supporting references	(Alsaedi et al., 2019; Auxier et al., 2019; DOL, 2020; Dutil et al., 2007; FTC, 2012; HHS, 2015; Horn et al., 2015; Katzan, 2011; Paulsen et al., 2012; Sullivan, 2016; Wolfond, 2017)
Theme 4: Privacy Risks	
Findings	<ul style="list-style-type: none"> - People will still perform risky things even if they know the self-harm - Online social platforms hold limited personal information - Conflicting opinion to the previous bullet; online social platforms are a major cause for online personal data compromises - People's personal data can end up being sold on the dark web - Governments like the United States and the European Union are taking action against online social platforms to limit the privacy risk to the individuals
Theme 4: Privacy Risks	
Supporting references	(Choi et al., 2020; "US fines," 2019; Emont, Stevens, & McMillan, 2018; Hsu & Lin, 2016; Granville, 2018; Kim et al., 2018)

Table 1 (Continued)

Theme 5: Laws and Regulations Emerged to Support Online Privacy and Digital Identity	
Findings	<ul style="list-style-type: none"> - Multiple governments around the world started passing laws and regulations to protect online personal data and digital identity - GDPR in the European Union - Privacy Act of 1974, HIPAA, Gramm-Leach-Bliley Act, California Consumer Privacy Act in the United States of America - National Institute of Science and Technology put together several frameworks to help support the privacy of online data and to help with guidance on best practices of online behavior
Supporting references	(Green, 2019; NIST, 2018a; Legal Monitor Worldwide, 2020; Sobolewski et al., 2017; Sullivan, 2015; Sullivan, 2018)
Theme 6: Individuals Behaviors and Habits	
Findings	<ul style="list-style-type: none"> - People tend to forget their online accounts that are open and their passwords - Phishing attacks are on the rise - People can sometimes be over trustworthy with messages sent to scam them online - People are willing to disclose their information even when they know that some platforms will invade their privacy
Supporting references	(Bélanger & Crossler, 2011; Dhamija et al., 2006; Florencio & Herley, 2006; Sheng et al., 2010)
Theme 7: Tools and Training for Digital Identity Management	
Findings	<ul style="list-style-type: none"> - There needs to be a system that ensures end to end trust in the digital world - Existing tools and training are lacking - Multiple hardware and software solutions are surfacing to try to meet the need to secure digital identity - People need a system to keep track of their online data - People need proper cybersecurity training to know how to safe keep their data and mitigate some of their online interaction risks
Supporting references	(Alkaldi et al., 2019; Al-Khouri, 2014; Anakath et al., 2019; Bélanger & Crossler, 2011; Brown et al., 2004; Cooper, 2017; Choi et al., 2020; Dourish et al., 2004; Higashino et al., 2019; Nurse et al., 2011; Charney, 2009; Zastrow, 2014)

CHAPTER FOUR:

METHODOLOGY

Overview

This chapter details the methodology used in this research study. The research design section provides more details about the methodology used to analyze the interview data. It emphasizes the method used to collect data, which emphasized interviewing individuals until data novelty saturation. The data collection section describes how the interview participants were selected and why. Then, an explanation of the methodology of how the study invitation was solicited as well as IRB approval, is provided. The last section in this chapter delineates the coding methodology and coding results.

Research Design

Interview Until Data Novelty Saturation

To understand the risk perceptions of people pertaining to their digital identity, the first set of questions were geared towards discovering digital identity and online personal data. This discovery includes information on what data people share online, as well as their knowledge about their online personal data and online interactions. The second section discusses current behavior online, while the last set of questions addresses future and unmet needs. The interviews were conducted until data novelty was reached. Data novelty was determined to be saturated when the interviews started generating repetitive information. The data novelty was reached at approximately 20 interviews.

Process Followed

Using an inductive, interpretive approach, the interview transcripts were first analyzed using a “top-down” approach, where the transcripts were reviewed and analyzed for overall context. The second iteration was conducted using a “bottom-up” approach to try to determine the core findings and overarching themes to help answer the research question (Neck, 2015).

In the thematic analysis that supports this qualitative research, the process followed started with the literature review and the group of preliminary themes found in the academic and industry-focused literature. The next step involved composing a coherent qualitative questionnaire driven by the findings in the literature and exploring some of the causes and gaps of what was found in the literature. The goal was to inquire into the research population of people aged 55 to 75years-old, with no technical IT background to determine their awareness of the risks pertaining to their digital identity. The coding technique helped to uncover the scheme of the themes that this exploratory research sought at its essence.



Figure 6. Methodology Process Followed Thematic Analysis.

Thematic Analysis

Thematic analysis (TA) is a concept recognized as qualitative research that falls between grounded theory and social phenomenology (Braun & Clarke, 2006). Four authors highlight the use of TA: Boyatzis, Clarke, Braun, and Fereday. Boyatzis was one of the first researchers to document the mechanics of going through the analysis in his book *Transforming Qualitative Information* (Boyatzis, 1998; Braun & Clarke, 2006; Clarke & Braun, 2018; Fereday & Muir-Cochrane, 2006). As a result of performing a TA over a set of qualitative interview transcripts,

common themes were discovered and portrayed in a group of findings that tell a story that is compelling and answers the research question being investigated.

There have been different interpretations, variations, and adjustments of TA throughout the years. Just like any good framework, it is adapted to the investigator's use case and purpose of research. In his book *Transforming Qualitative Information*, Boyatzis (1998) described an inductive approach, which aligns with the grounded theory methodology described in Saldaña (2016). The inductive or grounded theory analysis approach aims to develop a theory as a result of the analysis of whether a deductive approach tends to go through the qualitative analysis with theory and hypothesis in mind and work to validate the theory (Hyde, 2000).

Considering this study falls in the category of exploratory research, an inductive approach is the more appropriate method of analysis. The goal of this analysis is to illustrate findings and themes from the qualitative interviews that led to the use of the underlying framework as described by Braun and Clarke in their six-step approach (2006). The six steps are:

- 1- Familiarize yourself with your data
- 2- Generate initial codes
- 3- Search for the themes
- 4- Review the themes
- 5- Define and name the themes
- 6- Produce the report

The adaptation of the thematic analysis illustrated in the diagram below reflects the adaptation of the thematic analysis methodology to the coding, illustration, and analysis of the findings in this research study. The Adapted Thematic Analysis (ATA) approach allows the coder to utilize the inductive approach used in grounded theory analysis with the blend of the

three steps of open coding, axial coding, and selective coding approach as outlined by Corbin and Strauss (2014). In this study, the three steps used in grounded theory, as well as the six steps used by Braun and Clarke in TA, led to the development of the ATA.

Why the ATA for this Study

The ATA is the most appropriate method for analyzing this research because it provides the simplicity of a structured approach in conducting the coding of the transcripts. This approach is simple enough to understand and fit the thematic analysis steps illustrated by Braun and Clarke in a clear sequence that is easy to use and replicate while limiting ambiguity that may cause confusion and uncertainty to some researchers. The ATA representation framework diagram is represented in the figure below:

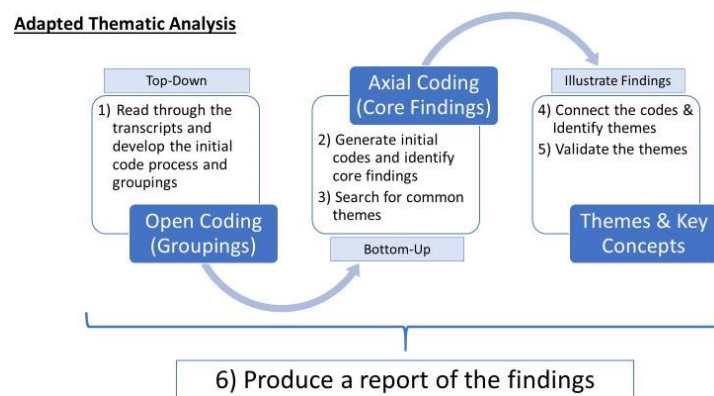


Figure 7. Adapted Thematic Analysis Framework.

Data Collection

The data collection process for this study occurred through a series of 15 to 30-minute interviews of individuals who were at least 55 years old. This age range was selected because those within this range tend to be closer to retirement and less computer savvy than the younger generation. The researcher interviewed participants from various professional backgrounds to over a wide range of populations and make the research study sample size as diverse as possible.

The interview questions were formulated in an open-ended qualitative way, with some specific follow up sub-questions, to ensure the individuals understood the questions and answered them adequately. The goal was to gauge their understanding and awareness regarding their online interactions and the associated risks, as well as their awareness of what online personal data they share that constitutes their digital identity footprint.

Interviews started in March 2020 and concluded in May 2020. The interviews were recorded via various software and hardware tools, then loaded into an online transcription service called Otter.ai to be transcribed. The lead researcher went through the transcription as well as the voice-over to verify accuracy. The researcher made the appropriate edits when the software did not translate accurately. The transcripts were then loaded into a coding template to perform the appropriate coding methodology.

Participant Selection

Participants in the study were solicited in various ways. The lead researcher placed flyers in various public places that attract the targeted population. Flyers were put up in several grocery stores and coffee shops. The researcher also leveraged his social media pages, LinkedIn and Facebook, as well as his personal connections to solicit interview participants. The originally intended approach was not as effective in recruiting participants. The recruitment of participants was derailed by the complete worldwide lockdown due to an unpredicted global event. As a result, the researcher transitioned to a referral approach, where a handful of original interviewees recruited served as a link to recruit their friends, colleagues, or family members. Participants were helpful and eager to help, especially during the tough times and the unprecedented event the world was experiencing. Interviews were conducted until novelty in the data was reached (Creswell & Poth, 2018; Saldaña, 2016; Seidman, 2013).

Interview Participants Characteristics

Twenty interview participants were involved in this study. They were from three different countries: 10% from the United Kingdom, 20% from Canada, and 70% from the United States.

From an employment perspective, 35% were retired, 65% were actively working with 25% working in education, and 30% being business owners.

Study Invitation

Every interview participant received an email with the solicitation flyer from Appendix A, the Interview questionnaire from Appendix C, and the IRB consent form from Appendix B. All participants provided verbal consent to participate in the interview, per the IRB protocol guidelines. Interviews were scheduled based on schedule availability and conducted via video conferencing software. The video conferencing software, Zoom, has a recording capability that was used to record the interviews; transcription occurred via a separate third-party software, Otter.ai.

IRB Approval

The Institutional Review Board (IRB) at the University of South Florida gave permission to conduct this study under *Study #000341*.

Data Analysis

Coding Method

Top-down open coding. In the first phase of the analysis, a top-down approach (Neck, 2015) was used to review all 20 interview transcripts. This first review was used to become familiar with the data; it helped to form an initial idea about the content and cohesiveness of the transcripts (Braun & Clarke, 2006). During this process, the fact that the investigator was also the person writing the analysis and the report helped tremendously. In this open coding section as

well, the transcripts were grouped by the topics that helped shape the interview questionnaire, which was the mechanism used to collect the transcripts' data. This initial set of groupings helped form categories of data points collected to be used in the analysis.

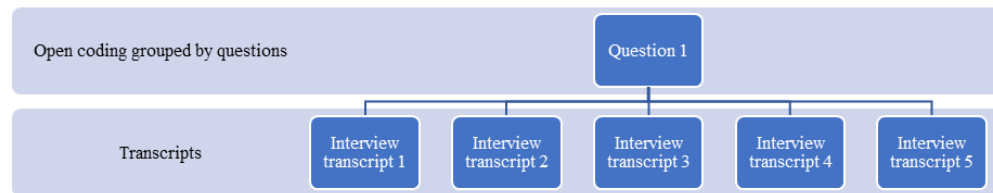


Figure 8. Transcripts to Open Coding Relationship.

Bottom-up axial coding. In the second phase of the analysis, after getting familiar with the data and identifying the grouping as well as the first level of condensed findings, axial coding was performed to generate the initial codes and identify the core finding from the consolidated interviews. These core findings units of analysis contributed to the discovery of the more general overarching themes.

In the third phase, after setting up the initial set of groupings and having the first set of codes produced, the search for common themes began. This phase helped to re-focus the analysis at the broader level of themes and thinking about sorting the different codes into potential themes as well as exploring the option of rearranging the grouping of the codes. This phase focused on the codes generated instead of the initial transcripts.

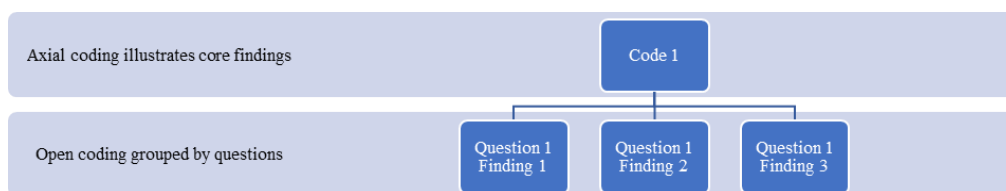


Figure 9. Open Coding to Axial Coding Relationship.

Illustrate findings by themes or key concepts. In the fourth phase, the second level of coding happened after the initial codes were already identified. In this phase, the first level codes

were reorganized and grouped based on the common themes found in the bottom approach. In this phase, a reorganization of the items identified in the axial coding phase occurred.

In the fifth phase, the high-level overarching themes found were refined and named appropriately to help reinforce and answer the research question guiding the study. In the sixth, or last stage, the themes found helped to guide the final analysis and write up of the report. This stage helped to tell a compelling story to convince the reader of the merit and the validity of the analysis (Braun & Clarke, 2006).



Figure 10. Axial Coding to Themes.

Coding Results

Open coding. Open coding is the initial line by line coding process of the interview transcripts. During this process, the first line of groupings was identified by the questions asked in the interview process. It served as a way for the investigator to start thinking about the different groupings.

The first set of groupings and the information coded from each question are displayed in the table below.

Table 2. Open Coding and Groupings.

Grouping	Open coding results from transcripts
Time spent connected online (Includes the use of email, messaging apps and surfing the web)	0 to 4 hours a day: 35% - Moderately Active 4+ hours a day: 65% - Active

Table 2 (Continued)

Grouping	Open coding results from transcripts
Online profiles adoption	<p>Online accounts in the last 5-10 years: 20+ Accounts: 13 people or 65% (The highest number being 100+) Less than 20 accounts: 7 people or 35% (The lowest number is 5) <i>Note:</i> People didn't remember all their online accounts from the past 5-10 years, even with the help of tools Email: 100% Social Media(Facebook, Instagram, LinkedIn...): Yes: 13 people - 65% & No: 7 people - 35% Online Banking: Yes: 85% & No: 15% Online Purchases: 100%</p>
Digital identity and online personal data composition awareness	All the interview participants think that their online digital identity is comprised of their online personal identifiers like name, address, phone number, birthday, as well as their online behavior and interactions
Level of comfort in entering personal information online	<ul style="list-style-type: none"> - Are hesitant or cautious when entering personal information online - Try to reduce their digital footprint when possible - Accept the risk when convenient and consider it part of their way of life
Have been, or knows someone, affected by the loss of online personal data	Yes: 17 - 85% No: 3 - 15%
Impact of online interactions risks identified on behavior change	Yes: 3 - 15% No: 17 - 85%
Reputational concerns around digital identity compromise	Yes: 11 people or 55% have reputational concerns People that have reputational concerns are mostly customer or student facing in their current jobs or influential in their societies and social groups No: 9 people or 45%, do not have any major concerns or have not thought about it much
Financial concerns around digital identity compromise	Yes: 9 people or 45%, have financial concerns (Most of the people that have concerns got affected or someone in their close proximity got affected by a financial hack) No: 11 people or 55% do not have any financial risks concerns (The majority of the interviewees that do not have financial concerns either do not actively bank online or have faith in their financial institutions to take care of their money)
Digital identity risks keeping you from fully using the internet	Yes: 4 people - 20% No: 16 people - 80%
Companies providing user-friendly information regarding their breaches	Yes: 4 people - 20% (2 people - Helpful, 2 people - Not helpful & Didn't know what to do with info provided) No: 13 people - 65% N/A: 3 people - 15%
Familiarity with online privacy rules and regulations	Yes: 17 people - 85% The majority heard of them, very few have encountered instances where they had to research them and are more aware No: 3 People - 15% never heard of them
Online companies being transparent with regards to personal information withheld	Yes: 5 people - 25% No: 8 people - 40% Don't Know what to look for: 7 people - 35%
Companies need to communicate to gain client trust	<ul style="list-style-type: none"> - Need to be more transparent with regards to personal information withheld: 2 people - 10% - Doesn't want more details: 2 people - 10% - Doesn't know what to look for: 7 people - 35% - Want more user-friendly information and disclosures: 7 people - 35% - Are interested in transparent details. Use third-party tools to manage online information (LifeLock seems to be popular) 2 people - 10%
Actions to keep online identity secure	<ul style="list-style-type: none"> - Don't know what to do: 4 people 20% - Change password more frequently: 9 people 40% - Research companies before using them online, and only deal with reputable companies - Be more cautious about clicking links from untrusted emails (Phishing) - Minimize online footprint - Take regular training to increase awareness - Only provide information to companies a person solicits - Use a password manager and various other available tools - Clean cookies and history regularly - Limit the use of public Wi-Fi - Monitor financial accounts regularly
Awareness of the availability of tools or training to keep digital identity more secure	Yes: 75% No: 25%
Had Cybersecurity training	Yes: 80% No: 20%

Table 2 (Continued)

Grouping	Open coding results from transcripts
Thoughts about training	<u>Helpful</u> : 7 people - 35% <u>Would like to be trained</u> : 2 people - 10% <u>Needs to be more user-centric and relevant</u> : 9 people - 45% <u>Does not care for it</u> : 2 people - 10%
Accounts & password management systems adoption	<u>Paper</u> : 25% <u>Electronic password manager or electronic manual system</u> : 30% <u>None</u> : 45%
Ideal solution to keep identity more secure	- Use websites in incognito mode: 1 person - 5% - Mask credit card information: 1 person - 5% - Don't know what to look for: 6 people - 5% - A tool to provide more transparency and control: 7 people - 35% - Digital Identity management tool (Keep track of passwords and websites): 6 people - 30% - A tool to provide what digital identity information out on the internet: 7 people - 35% - A tool to notify if anyone unauthorized used their digital identity: 7 people - 35% - Universal username and password with some way of authentication - A tool to eliminate complexity in accessing online accounts
Unmet needs to keep digital identity more secure	More transparency & control: 6 people - 30% No or doesn't know what to look for: 8 people - 40% Would like training and information about options: 6 people - 30%

Table 3. Open Coding to Axial Coding.

Open coding	Axial coding (Core findings)
Time spent connected online (Includes the use of email, messaging apps and surfing the web) 0 to 4 hours a day: 35% - Moderately Active 4+ hours a day: 65% - Active	Most people between the ages of 55 to 75 are active online
Online profiles adoption <u>Online accounts in the last 5-10 years</u> : 20+ Accounts: 13 or 65% (Highest number being 100+) Less than 20 accounts: 7 or 35% (Lowest number is 5) <i>Note</i> : People didn't remember all their online accounts from the past 5-10 years, even with the help of tools <u>Email</u> : 100% <u>Social Media(Facebook, Instagram, LinkedIn...)</u> : Yes : 13 - 65% & No : 7 - 35% <u>Online Banking</u> : Yes : 85% & No : 15% <u>Online Purchases</u> : 100%	Most of the population didn't readily know all the online accounts they used in the last 5 to 10 years
Digital identity and online personal data composition awareness All the interview participants think that their online digital identity is comprised of their online personal identifiers like name, address, phone number, birthday, as well as their online behavior and interactions	Acknowledged that their Digital Identity encompasses online personal data as well as online interactions, associations, and behavior
Level of comfort in entering personal information online - Are hesitant or cautious when entering personal information online - Try to reduce their digital footprint when possible - Accept the risk when convenient and consider it part of their way of life	Accept the risk as it is part of life right now, especially when the convenience outweighs the risks
Have been or knows someone affected by the loss of online personal data <u>Yes</u> : 17 - 85% <u>No</u> : 3 - 15%	Most people have been or know someone who has been affected by an online data breach
Impact of online interactions risks identified on behavior change <u>Yes</u> : 3 - 15% <u>No</u> : 17 - 85%	People's online behavior was not affected by experiencing or knowing about cybersecurity breaches
Reputational concerns around digital identity compromise <u>Yes</u> : 11 people or 55% have reputational concerns People that have reputational concerns are mostly customer or student facing in their current jobs or influential in their societies and social groups <u>No</u> : 9 people or 45%, do not have any major concerns or have not thought about it much	Risks about online presence and reputation being compromised mattered to individuals who are socially active, influential or their jobs get affected by a digital identity compromise

Table 3 (Continued)

Open coding	Axial coding (Core findings)
Financial concerns around digital identity compromise <u>Yes</u> : 9 people or 45%, have financial concerns (Most of the people that have concerns got affected or someone in their close proximity got affected by a financial hack) <u>No</u> : 11 people or 55% do not have any financial risks concerns (The majority of the interviewees that do not have financial concerns either do not actively bank online or have faith in their financial institutions to take care of their money)	Risks about online banking and financial losses mattered to people who have been directly or indirectly affected by a compromise. People seem to trust their financial institutions to protect them and their money
Digital identity risks keeping you from fully using the internet <u>Yes</u> : 4 people - 20% <u>No</u> : 16 people - 80%	Digital identity compromises and cybersecurity risks are not a deterrent for people fully using the internet for their needs
Companies providing user-friendly information regarding their breaches <u>Yes</u> : 4 people - 20% (2 people - Helpful, 2 people - Not helpful & Didn't know what to do with info provided) <u>No</u> : 13 people - 65% <u>N/A</u> : 3 people - 15%	In very rare occasions, companies are providing details about online data breaches
Familiarity with online privacy rules and regulations <u>Yes</u> : 17 people - 85% The majority heard of them, very few have encountered instances where they had to research them and are more aware <u>No</u> : 3 People - 15% never heard of them	There is a very high-level familiarity with the existence of online privacy rules, laws, and regulations Very rarely, people knew the details of these laws and regulations
Online companies being transparent with regards to personal information withheld <u>Yes</u> : 5 people - 25% <u>No</u> : 8 people - 40% <u>Don't Know what to look for</u> : 7 people - 35%	Companies are not transparent with people's personal data withheld or shared online. There is also a significant amount of people who are not properly informed enough to know what to look for
Companies need to communicate to gain client trust - Need to be more transparent with regards to personal information withheld: 2 people - 10% - Doesn't want more details: 2 people - 10% - Doesn't know what to look for: 7 people - 35% - Want more user-friendly information and disclosures: 7 people - 35% - Are interested in transparent details. Use third-party tools to manage online information (LifeLock seems to be popular) 2 people - 10%	People want companies to be more transparent and have user-friendly disclosure agreements and interactions with their users
Actions to keep online identity secure - Don't know what to do: 4 people 20% - Change password more frequently: 9 people 40% - Research companies before using them online and only deal with reputable companies - Be more cautious about clicking links from untrusted emails (Phishing) - Minimize online footprint - Take regular training to increase awareness - Only provide information to companies a person solicits - Use a password manager and various other available tools - Clean cookies and history regularly - Limit the use of public WIFI - Monitor financial accounts regularly	There seems to be a different level of awareness between the participants on what to do to keep their online identity more secure
Awareness of the availability of tools or training to keep digital identity more secure <u>Yes</u> : 75% <u>No</u> : 25%	For the most part, people are aware of the availability of tools to keep their identity more secure; very few knew all the options that are available for them to use and the difference between the utility of each tool
Had cybersecurity training <u>Yes</u> : 80% <u>No</u> : 20%	For the most part, people had some sort of cybersecurity awareness training, mainly due to their current or previous professions
Thoughts about training Helpful: 7 people - 35% Would like to be trained: 2 people - 10% Needs to be more user-centric and relevant: 9 people - 45% Does not care for it: 2 people - 10%	People thought that training is helpful but would like it to be more user-centric

Table 3 (Continued)

Open coding	Axial coding (Core findings)
Accounts & password management systems adoption <u>Paper</u> : 25% <u>Electronic password manager or electronic manual system</u> : 30% <u>None</u> : 45%	Low adoption of password management tools, due to the complexity of the tool or the distrust in the vendor due to lack of transparency
Ideal solution to keep identity more secure - Use websites in incognito mode: 1 person - 5% - Mask credit card information: 1 person - 5% - Don't know what to look for: 6 people - 5% - A tool to provide more transparency and control: 7 people - 35% - Digital Identity management tool (Keep track of passwords and websites): 6 people - 30% - A tool to provide what digital identity information out on the internet: 7 people - 35% - A tool to notify if anyone unauthorized used their digital identity: 7 people - 35% - Universal username and password with some way of authentication - A tool to eliminate complexity in accessing online accounts	Various ideas about solutions emerged, most of the responses geared towards more transparency and more control of their Digital Identity
Unmet needs to keep digital identity more secure - More transparency & control: 6 people - 30% - No, or Don't know what to look for: 8 people - 40% - Would like training and information about options: 6 people - 30%	People wanted more transparency and control over their online digital data. They want training and awareness about the options available and what to look for in keeping their digital identity more secure

Table 4. Axial Coding to Themes.

Axial coding	Themes
Most people 55 to 75 are active online	Qualifier to the study: high internet adoption & use of digital identity - Predominantly high internet usage, with over 20+ online accounts making people 55 to 75 a ripe target for cyber-attacks and digital identity compromises - Knowledgeable of what their digital identity entails 1) People accept the risk when it affects their convenience People are aware of some of the risks due to first-hand or second-hand exposure
Most of the people didn't readily know all of the online accounts they used in the last 5 to 10 years	
Acknowledged that their digital identity encompasses online personal data as well as online interactions, associations, and behavior	
Accept the risk as it is part of life right now, especially when the convenience outweighs the risks	
Most people have been or know someone who has been affected by an online data breach	
People's online behavior was not affected by experiencing or knowing about cybersecurity breaches	
Risks about online presence and reputation being compromised mattered to individuals who are socially active, influential or their jobs get affected by a digital identity compromise	
Risks about online banking and financial losses mattered to people who have been directly or indirectly affected by a compromise. People seem to trust their financial institutions to protect them and their money	
Digital identity compromises and cybersecurity risks are not a deterrent for people fully using the internet to their needs	2) People are concerned that companies are not being transparent with regards to being good custodians of their digital identity
In very rare occasions, companies are providing details about online data breaches	
There is a very high-level familiarity with the existence of online privacy rules, laws, and regulations. Very rarely people knew the details of these laws and regulations	

Table 4 (Continued)

Axial coding	Themes
Companies are not transparent with people's personal data withheld or shared online. There is also a significant amount of people who are not properly informed enough to know what to look for	2) People are concerned that companies are not being transparent with regards to being good custodians of their digital identity
People want companies to be more transparent and have user-friendly disclosure agreements and interactions with their users	
There seems to be a different level of awareness between the participants on what to do to keep their online identity more secure	3) People are aware of the availability of tools and trainings to help manage the risks. But they need more awareness education about their options and the utility of the tools and the training to use them properly while making an informed decision and staying user-centric
For the most part, people are aware of the availability of tools to keep their identity more secure; very few knew all the options available for them to use and the difference between the utility of each tool	
For the most part, people had some sort of cybersecurity awareness training, mainly due to their current or previous professions	
People thought that training is helpful but would like it to be more user-centric	
Low adoption of password management tools, due to the complexity of the tool or the distrust in the vendor due to lack of transparency	
Various ideas about solutions emerged, most of the responses geared towards more transparency and more control of their digital identity	4) People want more transparency and control over their digital identity to help them ease their concerns of the risks
People wanted more transparency and control over their online digital data. They want training and awareness about the options available and what to look for in keeping their digital identity more secure	

CHAPTER FIVE:

FINDINGS

Overview

This chapter illustrates the findings from this study based on the literature review that led to the creation of the questionnaire, which supported the qualitative interviews conducted with the target population of 20 individuals between the ages of 55 to 75 with no technical information technology background. By using the adapted thematic analysis framework for this study, the four themes illustrated in the diagram below emerged. The underlying data that led to the creation of the themes are explored in detail in this chapter.

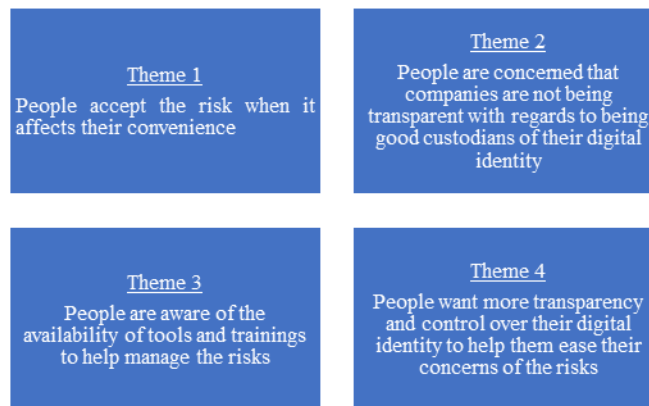


Figure 11. The Four Major Themes from the Interviews.

Findings from the Interviews

Qualifier to the Study: High Internet Adoption and Use of Digital Identity

The interviews with the 20 individuals between the ages of 55 to 75 led to the finding that there is a high degree of internet adoption among the interviewed population. Considering this

study was conducted during unusual circumstances when people were forced to socially distance and stay home, more people who were not usually active online had to adapt to the use of the technology to facilitate their daily lives while forced to stay home. A notable amount of people who, in normal circumstances, would not have shopped online or participated in social events via video conferencing were forced to learn the technology considering the circumstances.

Normally, only 68% of individuals between the ages of 55 and 75 use the internet (Vogels, 2019). However, digital adoption was near historic levels during this study, as discovered in the interviews, based on the need to connect to the internet to stay connected with the rest of the world during the unusual circumstances that affected this study.

There was also a high level of awareness amongst the interview participants that their digital identity is composed of multiple components. Interview participants were aware that their digital identity is composed of their personal information as well as their behavior and relationships online.

Most people 55 to 75 are active online. Examining the data gathered from the 20 interviews, the investigator found that 35% of study participants were not as active and only spent between one to four hours a day online.

Compared to 65% of study participants who were active but got divided almost evenly between the two categories: 1. four to six hours, which comprised 30% of the interviewees, and 2. six to twelve hours, which comprised 35% of the interviewees. The latter category includes the power users that spend most of their day connected online. Time spent connected online includes the use of email, messaging apps, connecting with friends, social media usage, and surfing the web.

Quoting participants from the two ends of the spectrum, one of the less active interviewees stated: “Online, including, research, emails, stuff like that. I would say, three to four hours.” One of the more active study participants stated: “I just wondered if it's like so out of 24 hours Yeah, my gosh, probably, like eight to ten hours, connected online.”

Online Accounts

Most of the people didn't remember all the online accounts they used in the last 5 to 10 years. The majority of study participants did not readily know how many online accounts they had created in the last 5 to 10 years.

Sixty-five percent of the interviewees had more than 20 online accounts. Without having exact figures, the participant with the highest number of accounts stated that they easily have 100 accounts, if not many more, that they could not recall. Conversely, only 35% of the interviewees estimated that they have less than 20 online accounts, with the lowest number of online accounts identified by an interviewee being approximately five accounts. Study participants still had a hard time remembering all their online accounts, even with the help of the tools they use to help manage their accounts.

All interviewees stated they have at least one email account, if not multiple. One of the interviewees stated: “You know, I guess none of us can escape email. And I have three different email accounts.” Another interviewee mentioned that the unpredicted event forced her to adapt to the digital world and have more of a formal digital identity presence. She stated that “I'm truly not an IT person, you know, because of the Coronavirus because of this COVID- 19, I've been forced to get online because everything is being done by streaming and by YouTube and Facebook and Zoom.”

Social media. Regarding social media, 65% of study participants stated they used some sort of a social media platform, whether Facebook, Instagram or LinkedIn, for business use to promote their businesses or personal use to keep up with their families and loved ones. The individuals who did adopt social media had more of a risk acceptance attitude or did not think about it much. The 35% of participants who did not use social media were not comfortable using the platform due to privacy concerns and worrying that their data would be lost or stolen, as it was a common thing happening with these platforms.

One of the interviewees who did not want to adopt social media stated that “The only thing I have is WhatsApp to chat with the family that's it. The rest, I don't trust it because when I read the fine prints for them for Facebook or other stuff to say, we have the right to share information with other study participants, so I said No, thank you. None of the social media accounts.” Another person stated that not using social media is the concern of their digital identity being compromised. They said, “Some of that is mental. It's a concern with identity theft, but not learned yet how to really negotiate this environment without being compromised.” One of the study participants who adopted social media stated that “I am comfortable with using it because that's the way of life now.”

Online banking. Going through the interviewee's answers about online banking, it seems that there is high adoption of 85% between study participants actively monitoring their credit cards online as well as paying their bills directly from their bank accounts. The 15% minority who was not actively using online banking systems provided to them by their banking institutions prefer to use manual transactions, like cash, where it is available, as well as mailing physical checks to pay their bills. They remained committed to this acquired behavior even after the unpredicted event's quarantine was fully implemented.

The investigator noticed that the unpredicted event was a big driver for participants to increase their adoption of the digital medium and become accustomed to making financial transactions online. One person stated, “I don’t know. I was reluctant at first to switch over to online accounts. But, um, so I'm sure I had fewer, and then now I've kind of embraced it completely. So, most of my accounts are online now.” This response indicated that this person embraced using the internet and the use of the digital world.

Online purchases. The majority of the study participants were forced to rely on purchasing items online due to the unexpected global event. Those purchases ranged from grocery store items through websites like Instacart to buying clothes and various household items via Amazon.com, Walmart.com, and others. An interviewee stated that “I signed up for Instacart when we all got locked down to get my food delivered,” which illustrates that the lockdown pushed study participants to use the internet for purchasing their essentials more and more.

Digital identity includes online personal data as well as online interactions. When asking study participants if they knew what constitutes their digital identity, most interviewees acknowledged that their digital identity encompasses online personal data, online interactions associated to their behavior online, their affiliation to online groups, and how those groups interact with other groups as well. The interview participants recognized that their online personal identifiers, like name, address, phone number, birthday, were just a part of their digital footprint and digital identity. One interviewee stated, “Well, I probably would just say things like addresses, birthdate, email accounts.” Another person described digital identity as “Everything that I do maybe on the internet or all the information about owning, like credit card, my social insurance, I guess, my behavior or where do I go which sites.”

As individuals increase their adoption of the internet, and awareness about their digital identity matures, further exploration of their risk awareness and tolerance is needed to understand their behavior. This first section in the themes from the findings serves as a qualifier for the study. Theme 1 below touches upon what people know and how they perceive cybersecurity threats relating to their digital identity.

Theme 1: People Accept the Risk When It Affects Their Convenience

Accept the risk as it is part of life right now, especially when the convenience outweighs the risks. Interviewees expressed that they are hesitant or cautious when entering personal information online. Multiple study participants expressed their discomfort in providing various websites with their personal information. One study participant stated: “My comfort level deals with how well I trust, and I know the brand, okay in that company.” Another participant stated: “I was comfortable inputting my information in only because I specifically use American Express. They have a lot more reps and warrants that basically protect the consumer.”

Study participants expressed that one of their risk mitigation techniques against having their online data being compromised is to try to reduce their digital footprint when possible. One study participant stated: “I do my little bit of my homework as far as trying to be sure the site I'm on has some measure of safety or encrypted side or selective with who I will give that information to online.” Study participants consider that accepting the risk when it is convenient to then is acceptable as interacting online is considered part of their way of life. One study participant stated: “When I purchase stuff online, I have to put my information online, I have to do it. It's not really a choice to provide my information online.”

Most study participants have been or know someone who has been affected by an online data breach. Reviewing the majority of study participants' responses, 85% of the study

participants, either experienced a data breach and loss of online personal data themselves, or they knew somebody affected by some sort of a breach. Whether it is a financial institution, a credit agency, or a large hotel chain, most of the responses received by the investigator indicated a level of awareness regarding breaches happening to prominent companies online. Only 15% of respondents believe they were never affected or did not know first-hand someone affected by an online breach. Their level of awareness of online breaches is rather high, considering what they read in newspapers and magazines and/or what they hear on the radio or see on TV.

One study participant stated: “I remember a work colleague lost her identity through her income tax. And so, she just shared that with me, but not in detail. Mostly, I was just left with the amount of frustration and work it was to try to straighten it out with the IRS.”

Study participants' online behavior was not affected by experiencing or knowing about cybersecurity breaches. Though the majority of the study participants mentioned they were exposed to some sort of an online breach, only 15% of the respondents mentioned that it affected the way they behave online. Eighty-five percent of the respondents stated that online behavior did not change even though they were exposed or heard of companies being breached online and losing millions of people’s personal information. One interview participant stated: “This was four years ago. I was not as aware of such things as I am now. And it was one of those from out of the country that actually when I clicked it, it just zapped my whole computer. And then it came up, click this, and we will link it will put you back in and then it said give us \$2,000, you know, all of that. It was really was a mess. But yeah, that I really learned a lot from that one experience.”

Study participants' concern about their online reputation. There seems to be a consensus among 55% of the interviewees around their concern for their online reputation. The

risks relating to online presence and reputation being compromised mattered specifically to individuals who are socially active and frequently interact with groups of people or if their actions influence the behavior of people around them. They might be influential in their societies due to their economic status or their jobs; some notable examples are company owners, presidents, or teachers. Those types of individuals are very concerned about being affected by a digital identity compromise due to the negative consequences that might cause their job or social surrounding.

One interview participant stated: “If someone zeroes in on you as an individual and decides they're going to go for it, it's very hard to resist. I mean, you know well, I'm aware of the, of the dark web and the data that's available on each and an individual. And I've, I've heard of demonstrations where people you know, type in your name, and then they say, this is what we know about you today. And you know, it's like a big spreadsheet, isn't it? There's your name, and then you've got address, passport number, blah, blah, blah, across the top, and it's just frightening. The data is out there. That's the thing. And if someone decides you're the one they're going to get, it's very hard to resist it.”

The other 45% of study participants did not have a concern, have not thought about it much, had no major concerns due to their limited online interactions, or simply accept the risk.

One interview participant, when asked if he has any concerns, replied: “No, not at all.”

People seem to trust their financial institutions to protect them and their money.

Online financial transactions seemed to have significantly increased during the quarantine. Out of the 20 people interviewed, 55% do not have any financial risk concerns. Out of that population, the majority who did not express that they had financial concerns, either do not actively bank online or the opposite is true; they frequently bank online but have significant faith

in their financial institutions to take care of their money and safely keep it. One interview participant stated: “The bank just gives you your money back, they somehow absorb the losses.” Another interview participant stated: “American Express has a lot more reps and warrants that basically protect the consumer. You know, if there is any kind of fraud, you can file something, and they will take it off your bill. I mean, most credit cards have that policy.”

Conversely, 45% of participants who did have financial concerns got exposed to some sort of financial compromise. That compromise might have represented itself in several forms. Most notably, a couple of the interviewees were scammed in the form of an online phishing attempt or got their credit card stolen from one of their online accounts and used in a malicious way. One interview participant stated: “Credit cards or bank accounts, No, I don't think I've actually opened them online. I've just had them opened in the brick and mortar.”

Cybersecurity risks are not a deterrence. Despite all the cybersecurity hacks, breaches, and various cybersecurity risks that affect the use of digital identity, 80% of the people interviewed stated that those risks are not keeping them away from using the internet to their liking. One interview participant said: “No, I have used the internet for everything that I want to use it for. They (the risks) are not keeping me from using it (the internet). They are making me more conscious of the things that I am doing. I am reasonably comfortable.”

Only 20% of the people interviewed expressed their concern about all the risks that come with their online interaction and its impact on their digital identity, which keeps them from fully using the internet to the level they want. One of the interviewees stated: “Some of my friends, they don't write letters. If I knew how to use Facebook and other electronic media properly, I would keep in touch. So, I am out of touch with them because I don't use Facebook, and the

same applies to my classmates. I am afraid I don't know how to use that without being victimized."

Theme 1 covered the awareness of participants of the threats that impact them and people around them as well as ignoring the risks when they affect their convenience. Theme 2 addresses people's concern that companies that manage online platforms are not being good custodians of their digital identity.

Theme 2: People Are Concerned That Companies Are Not Being Transparent with Regards to Being Good Custodians of Their Digital Identity

Companies are not providing details about data breaches. Most people interviewed in this study were not very happy with what companies provide them as far as user-friendly information regarding cybersecurity breaches. Specifically, 65% of the interviewees said that companies do not provide them with user-friendly, simplified communication about what happened and what they should do about cybersecurity breaches that affected their users. One study participant stated: "They are tracking data on how I shop, or how I go to a particular website to check something, I don't get that kind of information, don't get that kind of feedback on anything."

A small group, about 20% of the interviewed population, said they were happy with the information provided by those companies that were breached. Out of that 20%, only 10% thought the information was helpful; the other 10% stated that the information was provided, but it was not very hopeful, so they didn't know what to do with it or what actions to take as a consequence of those cybersecurity breaches. One study participant stated: "I think they can be transparent, but they haven't been proactive."

The remaining 15% of the people interviewed did not have much to say about companies' disclosures, or they simply did not know what to look for, which creates a gap in the diffusion of adequate information by the companies to keep people better informed.

One interview participant stated: "If they did, I don't know what to look for, to be honest."

There is a high level of familiarity with the existence of online privacy rules, laws, and regulations. When asked about privacy laws and regulations, 85% of people interviewed said they heard of online privacy laws as well as rules and regulations that govern online interactions and the minimization of the invasion of people's digital privacy. They were also aware that many companies had disclosure agreements associated with most of the creation of new online accounts as well as a regularly updated set of guidelines that define the way a company deals with people's personal data stored on their systems. Notably, the level of awareness of the content of those disclosure agreements, as well as the rules of engagement defined by those privacy laws, is still mysterious for most of the people interviewed.

One interview participant stated: "Oh, yeah, I mean do I know exactly what they are? No. but I am aware that there are some laws or rules but not specifically, exactly what they are."

Another interview participant stated: "I know a little bit about it, I guess, to be honest. The fact that probably 99.9% of people never read much of it. It was written by lawyers and is so complex that even that becomes open to interpretation by another lawyer or judge."

A small number of people, represented by 15% of the interviewed population, never heard of online privacy laws or any other rules and regulations that provide guidelines for best practices of online interactions and knowledge of people's rights with regards to company's

storing of their data online. One interview participant stated: “I don’t know much, I have never read anything about them, I am just minding my own business.”

Companies are not transparent with people's personal data withheld or shared online. Of the 20 people interviewed, 40% believe that companies are not being transparent or forthcoming with them regarding client’s personal data being tracked and stored on their systems. Or, they believe the information provided is not presented in a way that an average person can understand it. From the people interviewed, approximately 35% did not know what to look for or to ask companies about their data. Twenty-five percent of the interviewed population believe that companies are being transparent with them; some of them believe they just do not know what to look for in that information, but the companies are doing their part.

One study participant stated: “You get letters from banks that say this is what we do and retain from your information, and you get your annual statement. Does anybody really read that?”

Another study participant stated: “I don’t feel that they are open about it, the fact that you can ask Siri to search for something and all of a sudden somehow it knows. Yeah, I don’t think anybody is transparent of all of that big data stuff that is going behind the scenes, that everybody is sharing with everybody else.”

People want companies to be more transparent. Of the 20 people interviewed, 10% believe that companies need to be more transparent with regards to personal information data withheld on their systems. Thirty-five percent of participants want more user-friendly information and disclosures, so they feel more at ease while dealing online with companies. Ten percent of the interviewed population does not want more details from those companies, as it is not something relevant for them. Thirty-five percent of people interviewed say they do not have

enough education about what to look for, which creates a gap in communication in the disclosure of the proper information relevant to people. The last 10% of people interviewed expressed that they are interested in transparent details from organizations doing business online; these people tend to be users of third party tools, similar to LifeLock, to manage their online information; these platforms or tools provide them with a level of details that the original company they deal with does not usually provide.

One of the participants, when asked if companies are being transparent with regards to personal data, answered: “Oh, no, absolutely not, and I know that I know if they did. I didn’t recognize it for what it was.” Another participant was content with the information companies send her; she stated that: “They frequently will send me this is what we do with the information we gather from you, get that and read it. This will be usually when I have ordered online, they will tell me, and this is what we do with the information that we gather from you.”

Theme 2 highlighted participants’ concerns that companies are not being forthcoming and good custodians of their digital identity. Theme 3 covers participants’ awareness of tools and training that help manage their digital identity risks to try to reduce the risks and damage that companies may be causing to their digital identity.

Theme 3: People Are Aware of the Availability of Tools and Training to Help

Manage the Risks

Awareness to keep digital identity secure. When asked what actions to take to keep their online identity more secure, 20% of the interview participants did not know what actions to take or what to do. The rest of the interviewees had different thoughts of things to do to keep their digital identity more secure. Forty percent of the participants said they change or would like to change their password more frequently. Participants described other notable actions, like

researching companies before doing business with them online or only dealing with reputable organizations. Trying to minimize their digital footprint was another notable idea. An important action to take is to be more cautious about clicking on links from untrusted or unsolicited emails, also known as phishing emails, that the hackers use as a way to steal people's information off of their computers or various online accounts. Only providing information to companies a person solicits intentionally is also another way of making sure information does not get in unwanted hands. People also mentioned that they would like to regularly take training to see how hackers have evolved to try to steal their information and stay more aware. The last group of actions involves taking care of the technology used to access the internet, like the use of password managers and other various available tools, clearing cookies and browser history regularly, limiting the use of public Wi-Fi, and setting up monitoring alerts on most financial accounts used regularly.

One interview participant stated: "I wish somebody would tell me something more than what I am being told right now. But gosh, all I know is don't click it. Don't do it. And well, maybe that is all I need to know, I don't know. I would like to have a little bit more explanation of what's going on and how to avoid the problems." Another interview participant stated: "I keep my financial data off the internet, not on the computer as much as possible. Anything that is a legal document, I try to handle outside of the electronic environment." A third interview participant stated: "I don't know what I should do."

People's awareness of tools and training. There was a significant amount of awareness amongst people interviewed regarding the availability of platforms to help keep the digital identity more secure. Seventy-five percent of people mentioned that they know of various

software tools that help them use the internet more securely or are aware of some sort of training platform to help them stay abreast of those cybersecurity risks.

One of the interview participants stated: “Two-factor authentication, and then there is a text to my cell phone with a digital password to enter.” Another interview participant stated: “Once a year, we have to go through it [Cybersecurity awareness training], and if there are some issues during the year, that might be an update to the training.” Another participant stated: “I personally use a password manager, just to keep the passwords for the different accounts I have because some accounts I don’t use for a long period of time.”

Conversely, 25% of the population interviewed had no idea what relevant tools or training are available to help them manage their digital identity privacy and security.

People’s exposure to cybersecurity training. Most participants had some sort of cybersecurity awareness training, mainly due to their current or previous professions. Eighty percent of the interviewees said that they had cybersecurity training at some point as part of their jobs, compared to 20% that said that they were not exposed to any type of cybersecurity training. One study participant mentioned: “My workplace participates in a program called security mentor. So, you’re expected, and I think about once every month, you will get a training video that you have to take and complete.”

Cybersecurity training is helpful. Thirty-five percent of the people interviewed thought that training is helpful to keep them informed or would like to have the training to be better informed. They believe that training is the first step in building awareness. Ten percent of people mentioned that they would like to be exposed to training, whereas another 10% did not care about being trained.

Forty-five percent of participants expressed a desire for training to be more user-centric and relevant so that they can apply what they have learned. One interview participant stated: “That [Cybersecurity awareness training] has been very helpful reminding me of some things that I knew and then learning some safety measures.”

Low adoption of password management tools. From the interviewed population, 45% did not use any system, manual or electronic, to keep track of their accounts and passwords. Twenty-five percent used a paper system to keep track of their accounts and passwords, whether through sticky notes or on a special notebook. Thirty percent only adapted some sort of an electronic methodology for tracking, whether through a password manager or an encrypted password file.

One study participant stated: “I have an electronic system, an Excel sheet, and I have it password-protected.” When asked about password management tools, another study participant stated: “I do not know of any, and no one ever mentioned it to me.” One study participant stated: “Some of them I keep track of on paper, the rest I guess mentally without writing them down.” One study participant mentioned: “Apple keeps track of that. I have been using their software to keep track of things for a long time.”

Theme 3 highlighted participants’ awareness of management tools that help minimize their digital identity risks, which leads to Theme 4. The following theme addresses participants’ demand for more transparency and control over their digital identity from the companies they deal with online in order to ease their concerns about the potential risks these companies cause.

Theme 4: People Want More Transparency and Control Over Their Digital Identity to Help Them Ease Their Concerns of the Risks

People want more transparency and control over their online digital data. Regarding unmet needs to keep their digital identity more secure, the interviewees wanted training and awareness about the options available and what to look for to keep their digital identity more secure. Thirty percent of participants want more transparency from companies they deal with online as well as control over their online data. This transparency and control would allow them to give access permission to their online personal information selectively. One interview participant stated: “I think if there was something that would tell me what a hacker would know about me. What’s out there that people can use.” Another interview participant stated: “Transparency over my information out there, when it is readily available, will be helpful.”

Thirty percent of study participants would like more awareness and information about their options for protecting their online data as well as general information on best practices of how to be a good online citizen. This option can be in the form of training that highlights best practices and industry standards while maintaining user-centricity in the delivery of the information. One interview participant stated: “I would like to have more training to know what’s going on, why it’s going on, and what I need to do to respond.”

The remaining 40% of the people interviewed did not know what to look for or felt they do not have enough information to know what kind of unmet needs they should be seeking. This gap in knowledge connects to the problem of awareness that people have to know their options and how to think about the process. One interview participant stated: “I don’t know. Maybe I don’t know enough to know. I have done everything that I can think of; I read every article I can find. I listen to the experts to give me advice. I don’t know if that is enough.”

Solutions desired geared towards transparency and more control. Various ideas about desired solutions emerged from study participants; most responses focused on more transparency and control of their digital identity. Five percent of the interviewees would like a feature to use various websites in incognito mode. Another 5% of the interviewees wanted a way to mask their real credit card information while conducting transactions online. Thirty-five percent of the population expressed a desire for a tool to provide more transparency and control. Thirty percent of the interviewees wanted a tool for digital identity management that includes accounts and passwords management. Thirty-five percent of interviewees would like a tool that tells them what information is on the internet regarding their personal information; they also want the tool to notify them of any unauthorized use of their digital identity attributes somewhere online. Thirty percent of the interviewed population did not know what to look for and would like a higher level of awareness to make an informed decision.

Notably, a couple of individual requests requested that the tool provide a universal username and password to authenticate their digital identity, which should eliminate the level of complexity in accessing different online accounts. One study participant stated: “I definitely think it should have a password component because the whole idea of having a different password for every site is just too daunting.” One interview participant echoed a desire for that solution: “I wonder if having a universal username that we could use everywhere would be helpful.” Another participant mentioned: “It would be helpful if it would notify you if someone actually used your name or your address somewhere on the internet that you are not aware of.”

Theme 4 focused on interview participants’ demand for transparency and control over their digital identity and wish list of possible solutions to ease their concerns. The four themes derived from the interviews using the ATA led the investigator to identify findings that were

intriguing to explore and interpret. The next chapter compares the findings from the literature review with the findings from the ATA applied to the interviews. Also, it highlights the investigator's interpretations of this study.

CHAPTER SIX:

DISCUSSION

Overview

The purpose of the study was to answer the research question: “What are the risk perceptions of individuals, between the ages of 55 and 75, with no IT background, pertaining to their digital identity?” The study included the use of the adapted thematic analysis framework to pinpoint the understanding of the voice of the people. In this study, the interview participants consisted of a population of 20 non-IT career-oriented, 55 to 75-year-old individuals.

This chapter details the analysis of the findings from the interviews and how they compare to the findings from the literature review in order to identify gaps or commonalities between the findings of both chapters. This chapter also touches on the unpredicted event’s impact on participants’ behavior and the use of the digital medium. Additionally, it highlights the impact of this study from an industry and academic perspective.

Analysis

Qualifier to the Study: Increased Level of Internet Adoption Among People Caused the Wide Use of Digital Identity

As found in the literature review, the increase in internet usage created a need for digital identity to help enable, facilitate, and manage the use of the digital medium appropriately (Mueller et al., 2006). The themes discovered in the interviews indicate high adoption of the internet among the 55 to 75-year-old age group. Most interview participants expressed that they

cannot escape using the internet. With that high level of adoption comes the implied use of digital identity to help manage and facilitate online interactions.

Table 5. Internet Adoption Comparison.

Interviews	Literature Review
High adoption rate of the internet among 55 to 75-year-olds	The increase in internet usage created a need for digital identity (Mueller et al., 2006)

Interpretation. Despite the fact that the known average of only 68% of individuals between the ages of 55 and 75 use the internet (Vogels, 2019), this number significantly increased, as found in this research, due to circumstances when this study was conducted. The national quarantine forced people in this age group to use the internet to maintain social interactions, keep in contact with family and loved ones, and purchase their groceries and other items because most brick and mortar retailers were closed for in-person business.

Qualifier to the Study: People Are Aware of the Composition of Their Digital Identity

From the literature review, the definition of digital identity entails the association of personal identifiers and attributes as well as individuals' online relationships and interactions (Alashoor et al., 2016; Camp, 2004). This definition was validated; during the interviews conducted for this study, participants indicated that they are aware that their digital identity is a combination of their identifiers and attributes as well as their different online interactions.

Table 6. Digital Identity Composition Awareness Comparison.

Interviews	Literature Review
People are aware that their digital identity is a combination of their identifiers and attributes as well as their different online interactions	The definition of digital identity entails the association of personal identifiers and attributes as well as individuals' online relationships and interactions (Alashoor et al., 2016; Camp, 2004)

Interpretation. The level of awareness from individuals in the interviewed population regarding what constitutes their digital identity and how it is being used is very notable. The established awareness of the composition of their digital identity impacts the way people react to

risks associated with it. Identification is the first step in properly mitigating against risks as defined in the NIST CSF (NIST, 2018a). The definition of digital identity enables individuals to have a baseline of what they have that can be compromised and cause harm. Identifying the risks creates an awareness of the weak points to consider when trying to mitigate risk. This awareness of the composition of people's digital identity is a solid step towards answering one gap found in the literature review regarding the lack of a unified definition of digital identity. This gap in the literature can be clearly answered by defining digital identity as the collection of personal identifiers, personal attributes, and digital relationships and interactions.

Theme 1: Relationship Between Digital Identity Risks and People's Online Behavior.

The common perspective among people that their digital identity is constantly being tracked by unwanted parties, as uncovered in the literature review (Auxier et al., 2019), was reinforced by the interviews conducted in this study. Interview participants stated they are hesitant and cautious when entering personal information online. Some interview participants mentioned they try to reduce their digital footprint, when possible, to lower the risk of their information being exposed online in the case of a breach. With Phishing attacks and digital identity compromises being on the rise (Sheng et al., 2010), the majority of interview participants stated they were affected by the loss of online personal data or at least know someone who was affected. This personal impact creates the need for increased security to keep people's data more secure (Woodhouse, 2007).

The results of the interviews in this study indicated that the knowledge and experience about the risks of online interactions and loss of online personal data did not seem to impact or change the behavior of people online. To manage the problems caused by the risks associated

with online behavior and establish more trust, a framework found in the literature identifies confidentiality, integrity, and availability as pillars to keep digital identity and online personal data safe to use, easily accessible, and more secure (Katzan, 2011).

The interview participants were concerned about their identity being compromised or stolen to be used in a harmful way that would affect their families and social groups. The risk of losing financial assets was much less concerning to people than their reputational risk. There seems to be a higher degree of faith in the financial institutions taking care of clients and trying to keep their financial assets tied to online accounts secure among the group interviewed for this study. Conversely, as found in the literature review, people tend to forget the online account they have opened as well as the passwords they have created for those accounts (Florencio & Herley, 2007). The fact that people lose track of their online accounts and passwords creates a higher risk from a reputational and financial perspective. Online accounts can be compromised, and the user would not know if that password they had was used with other accounts that might show a higher level of risk attached to them, similar to personal checking accounts or credit lines. These security breaches can also be used by individuals or entities with a harmful intent to create fake personas that mimic other people's digital identity to cause harm to people in order for the bad actors to achieve their personal benefits and goals (Bélanger & Crossler, 2011).

Most interview participants stated that the risks of online interactions and the potential compromise of their digital identity do not hinder them from fully using the internet. The literature review uncovered that people would do risky things even when they know that it could cause them self-harm (Choi et al., 2020).

Interpretation. People are constantly cautious and wary that their digital identity is at risk of being tracked, misused, and compromised while they use the internet. Those risks

manifest in multiple shapes or forms: phishing, social engineering, and other tactics and procedures that criminals use online to steal people's digital identity. People are concerned about their digital wellbeing from a reputational and financial perspective as well as the safety of their families and social surrounding from the harm caused by online threats. Yet, people seem to disregard the risk, if it causes them an inconvenience or a roadblock to attain their want.

Table 7. Relationship Between Digital Identity Risks and People's Online Behavior Comparison.

Interviews	Literature Review
<p>Level of comfort in entering personal information online</p> <ul style="list-style-type: none"> - Are hesitant or cautious when entering personal information online - Try to reduce their digital footprint when possible - Accept the risk when convenient and consider it part of their way of life <p>Have been or knows someone affected by the loss of online personal data</p> <p>Yes: 17 - 85%</p> <p>No: 3 - 15%</p> <p>Impact of online interactions risks identified on behavior change</p> <p>Yes: 3 - 15%</p> <p>No: 17 - 85%</p> <p>Reputational concerns around digital identity compromise</p> <p>Yes: 11 people or 55% have reputational concerns</p> <p>People that have reputational concerns are mostly customer or student facing in their current jobs or influential in their societies and social groups</p> <p>No: 9 people or 45%, do not have any major concerns or have not thought about it much</p> <p>Financial concerns around digital identity compromise</p> <p>Yes: 9 people or 45%, have financial concerns</p> <p>(Most of the people that have concerns got affected or someone in their close proximity got affected by a financial hack)</p> <p>No: 11 people or 55% do not have any financial risks concerns</p> <p>(The majority of the interviewees that do not have financial concerns do not actively bank online or have faith in their financial institutions to take care of their money)</p> <p>Digital identity risks keeping you from fully using the internet</p> <p>Yes: 4 people - 20%</p> <p>No: 16 people - 80%</p>	<ul style="list-style-type: none"> - People feel that they are always being tracked online - Phishing attacks on the rise - There is a need for increased security to keep people's data more secure - Confidentiality, integrity, and availability are important to keep personal data secure - People tend to forget their online accounts that are open and their passwords - People will still do risky things even if they know the self-harm - People can sometimes be over trustworthy on messages sent to scam them online (Auxier et al., 2019; Bélanger & Crossler, 2011; Choi et al., 2020; Florencio & Herley, 2006; Katzan, 2011; Woodhouse, 2007; Sheng et al., 2010)

The impact of people disregarding the risks can be very costly, especially if there is no methodical way of evaluating the risk-benefit analysis through a best practice benchmark method that helps people make informed decisions when choosing to overlook the risk identified. With an informed risk-based decision, people can take quick action if any sort of harm was caused by their decision to overlook the risk. People's online behavior and cognitive ability to identify risk have to be driven by an informative, easy to use framework similar to the best practices guidance

that NIST created for organizations to make risk-based decisions regarding their cybersecurity posture, as manifested in the NIST Risk Management Framework (RMF) (NIST, 2018b). The development of a methodology to serve as a benchmark for personal digital identity risk management will help answer the gap found in the literature pertaining to the lack of user-centric benchmarks to help manage digital identity risks and establish the proper behavior to manage those risks. This study validated the need for such a framework, which is a needed topic for future research.

Theme 2: Online Platforms Are a Risk to People's Digital Identity

The literature review uncovered that multiple governments around the world, including the United States and the European Union, passed laws and regulations to protect online personal data and digital identity (Sullivan, 2015). Notably, the GDPR in the EU (Sobolewski et al., 2017) and HIPAA in the United States (HHS, 2015) are laws that resonate with individuals interviewed in this study. Interview participants expressed their familiarity with online privacy rules and regulations. The majority of interviewees stated that they have heard of them but do not know much about their details or what these laws and regulations empower individuals to do. NIST established several frameworks, like the NIST privacy framework (Legal Monitor Worldwide, 2020), to help with awareness and best practices about digital identity and online interaction management. The gap seems to exist in the user-centricity of these frameworks and the appropriate propagation of the awareness of their existence for the average individual to use adequately.

The literature review highlighted that online social platforms are a major contributor to digital identity compromises (Granville, 2018). A significant group of the interview participants in this study stated that online platforms are not being transparent with regards to what

information they record and store about their users. The literature review identified that people feel that they are constantly being tracked online (Auxier et al., 2019); this assertion reinforces the finding from the interviews about online companies not being transparent with their users about data they track about them.

The literature review stated that some people's online data might get sold on the dark web (Kahn et al., 2016). Thus, the interview participants expressed that online companies do not provide user-friendly, informative information if their systems were breached and what users need to know to take appropriate action on the information provided. The interview participants stressed the need for companies to provide user-centric information when communicating with their clients, specifically when there is a breach that caused harm to their systems and the data of their users. To reduce the risk and hold online companies and platforms accountable; governments like the United States and the European Union are taking action against those companies to limit the privacy risks to people's digital identity (Emont et al., 2018).

Table 8. Online Platforms are a Risk to People's Digital Identity Comparison.

Interviews	Literature Review
<p>Familiarity with online privacy rules and regulations <u>Yes</u>: 17 people - 85% The majority heard of them, very few have encountered instances where they had to research them and are more aware <u>No</u>: 3 People - 15% never heard of them</p> <p>Online companies being transparent with regards to personal information withheld <u>Yes</u>: 5 people - 25% <u>No</u>: 8 people - 40% <u>Don't Know what to look for</u>: 7 people - 35%</p> <p>Companies providing user-friendly information regarding their breaches <u>Yes</u>: 4 people - 20% (2 people - Helpful, 2 people - Not helpful & Didn't know what to do with info provided) <u>No</u>: 13 people - 65% <u>N/A</u>: 3 people - 15%</p> <p>Companies need to communicate to gain client trust - Need to be more transparent with regards to personal information withheld: 2 people - 10% - Doesn't want more details: 2 people - 10% - Doesn't know what to look for: 7 people - 35% - Want more user-friendly information and disclosures: 7 people - 35% - Are interested in transparent details. Use third-party tools to manage online information (Lifelock seems to be popular) 2 people - 10%</p>	<ul style="list-style-type: none"> - Multiple governments around the world started passing laws and regulations to protect online personal data and digital identity - GDPR in the European Union - Privacy Act of 1974, HIPAA, Gramm-Leach-Bliley Act, California Consumer Privacy Act in the United States of America - National Institute of Science and Technology put together several frameworks to help support the privacy of online data and to help with guidance on best practices of online behavior - Online social platforms are a major cause for online data compromises - People feel that they are constantly tracked online - People's personal data can end up being sold on the dark web - Governments like the US and the EU are taking action against online social platforms to limit the privacy risks to individuals (Emont et al., 2018; HHS, 2015; Kahn et al., 2016; Granville, 2018; Legal Monitor Worldwide, 2020; Sobolewski et al., 2017; Sullivan, 2015)

Interpretation. Online platforms have been known to be a risk to people's personal data and digital identity. Governments and organizations started establishing laws and rules to help manage the risks of these online platforms. Though many controls have been created as guidance and best practice to help manage that risk, people are still unsure of what to do to help mitigate potential threats. Once a level of awareness and maturity has been reached amongst individuals on how to interact with online platforms, the potential risks caused by these platforms will be attenuated and become more manageable in the case of a compromise or digital identity misuse.

The efforts of reducing the risks to digital identity compromises should also be integrated into the business controls that the online platforms operate with in order to reduce the gap and help people protect their digital identity. The companies operating the online platforms should be more user-centric in their communication and disclosures to their clients, which will help ease people's concerns and establish more trust in the organizations operating the platforms. This effort will help in increasing people's risk awareness and ease their concerns regarding their digital identity compromises. The roles of government entities should also not be discounted in setting proper regulations and controls to prevent the harm caused by online platforms; this recommendation addresses a gap found in the literature of laws and regulations being outdated in the United States and needing to be communicated in a user-friendly way to people so that their level of awareness of their rights and government protection is increased. This issue is an important segue into future research on what laws need to be in place and how they need to be presented to support the proper use of digital identity.

Theme 3: Tools to Manage Digital Identity Risks

Most interview participants were aware of the tools and training available to help manage their digital identity and teach them the best practices to keep their online interactions more

secure. The gap uncovered in the interviews from the awareness of the availability of tools and training is that the content and utility of those tools are not that well communicated. Interview participants were aware of the tools, but which ones are the best to suit their needs and how to properly use them are missing. The literature review uncovered that multiple hardware and software solutions are constantly being added to the market to try to meet the need of the consumers and help manage and secure people's digital identity, yet these tools lack user-centricity and streamlined delivery (Choi et al., 2020).

The literature review uncovered that people need proper cybersecurity training to know how to safe keep their data and mitigate some of their online interaction risks (Nurse et al., 2011). Interview participants mentioned that many of them had cybersecurity awareness training, but as cybersecurity threats that cause a major risk to digital identity evolve, the exposure to the training needs to be constant as the risks continuously evolve. The need for the training to be user-centric is also a noticeable request. The interview participants noted several different ways to keep their digital identity secure online. Rarely did consistency exist in the knowledge of what to do to keep their digital identity safe and how. The most consistently stated action was to regularly change their password, which is supported by the literature that people have the tendency to forget their passwords (Florencio & Herley, 2006).

The literature review found that people need a system to keep track of and manage their digital identity and online data (Cooper, 2017). The interviews uncovered that only a small group of participants use a digital tool to manage their online accounts and passwords. The majority of interview participants did not use a digital tool. They still use a pen and paper system.

Table 9. Tools to Manage People’s Digital Identity Comparison.

Interviews	Literature Review
<p>Awareness of the availability of tools or training to keep digital identity more secure <u>Yes:</u> 75% <u>No:</u> 25%</p> <p>Actions to keep online identity secure - Don't know what to do: 4 people 20% - Change password more frequently: 9 people 40% - Research companies before using them online and only deal with reputable companies - Be more cautious about clicking links from untrusted emails (Phishing) - Minimize online footprint - Take regular training to increase awareness - Only provide information to companies a person solicits - Use a password manager and various other available tools - Clean cookies and history regularly - Limit the use of public Wi-Fi - Monitor financial accounts regularly</p> <p>Had Cybersecurity training <u>Yes:</u> 80% <u>No:</u> 20%</p> <p>Thoughts about training Helpful: 7 people - 35% Would like to be trained: 2 people - 10% Needs to be more user-centric and relevant: 9 people - 45% Does not care for it: 2 people - 10%</p> <p>Accounts & password management systems adoption <u>Paper:</u> 25% <u>Electronic password manager or electronic manual system:</u> 30% <u>None:</u> 45%</p>	<ul style="list-style-type: none"> - Multiple hardware and software solutions are surfacing to try to meet the need to secure digital identity - People need proper cybersecurity training to know how to safe keep their data and mitigate some of their online interaction risks - People tend to forget their online accounts and their password - People need a system to keep track of their online data (Cooper, 2017; Choi et al., 2020; Florencio & Herley, 2006; Nurse et al., 2011)

Interpretation. Many tools and trainings are available on the market that help with digital identity management. The available market tools vary in their value proposition to their users. Tools range from specifically dealing with password management to only focusing on training and user awareness to managing multiple aspects of digital identity. The newer tools offer added functionality, like continuously scanning the internet for user-specific abnormal behavior, which can be beneficial if the information is provided to the end-user appropriately. The problem with the user-centricity of these tools remains a roadblock to their mainstream adoption. Price point and learning curve can also be relevant barriers of wide accessibility to the tools.

With the increase in popularity and advancement of machine learning and artificial intelligence, digital identity management tools might be transformed to be much more user

friendly. Removing the human factor of doing the backend analysis and informing the user in real-time to threats affecting their digital identity can significantly reduce risk by increasing the response time to potential threats. Automation in threat responses can help in mitigation and remediation by reducing the impact of compromises on the end-user. This reduction will help people in dealing with the repercussions of a clean up due to a digital identity breach aftermath. The study of the effect of new technologies impacting digital identity management tools can be the right step to reduce the gap created by these tools and training as well as the lack of user-centricity, which is identified as a gap in the literature review.

Theme 4: People Want More Transparency and Awareness to Keep Their Digital Identity Secure

The literature review uncovered that existing tools to manage digital identity and cybersecurity-related training are lacking (Nurse et al., 2011). The interview participants in this study identified several different opinions to keep their digital identity more secure.

Transparency was at the forefront of people's wish lists. Transparency builds more trust in information systems (Alsaedi et al., 2019). The interview participants also emphasized wanting to know what information is available about them online, and they want to be notified every time someone tries to access their digital identity information. These requests are reinforced by the findings in the literature review that a system to ensure an end to end trust in the digital world is needed (Charney, 2009). To try to satisfy some of the needs discovered, multiple hardware and software solutions similar to LifeLock emerged to help manage and secure digital identity and build trust in the online medium (Cooper, 2017).

Notably, interview participants expressed that they do not know what to look for to keep their digital identity more secure. This gap is where training and awareness about industry best

practices need to be provided on a broader, more open scale to anyone wanting the information. Similar to the efforts that the NIST cybersecurity framework tailored for organizations (NIST, 2018a), there needs to be a version of the cybersecurity framework geared towards individuals and best practices with regards to their digital identity and online interactions.

Table 10. People Want More Transparency and Awareness to Keep Their Digital Identity Secure Comparison.

Interviews	Literature Review
Ideal solution to keep digital identity more secure - Use websites in incognito mode: 1 person - 5% - Mask credit card information: 1 person - 5% - Don't know what to look for: 6 people - 5% - A tool to provide more transparency and control: 7 people - 35% - Digital Identity management tool (Keep track of passwords and websites): 6 people - 30% - A tool to provide what digital identity information is out on the internet: 7 people - 35% - A tool to notify if anyone unauthorized used their digital identity: 7 people - 35% - Universal username and password with some way of authentication - A tool to eliminate complexity in accessing online accounts Unmet needs to keep digital identity more secure - More transparency and control: 6 people - 30% - No, or Don't know what to look for: 8 people - 40% - Would like training and information about options: 6 people - 30%	<ul style="list-style-type: none"> - Existing tools and training are lacking - There needs to be a system to ensure an end to end trust in the digital world - Multiple hardware and software solutions emerged to secure digital identity - National Institute of Science and Technology put together several frameworks to help support the privacy of online data and to help with guidance on best practices of online behavior (Alsaedi et al., 2019; Cooper, 2017; NIST, 2018a; Nurse et al., 2011; Charney, 2009)

Interpretation. The lack in cybersecurity training and awareness created unmet needs with digital identity users. This lack of awareness sprouted the need for more training, transparency in information systems, and the ability to control digital identity aspects. The increase in awareness with regards to digital identity management leads to a reduction in risks as a result of people being more aware and vigilant. The increase in transparency with online information systems leads to a more robust end-user to end-user confidence as well as trust in authenticity and validity of transactions performed online using people's digital identity. The end to end trust with information systems using digital identity can be manifested by leveraging distributed ledger technology systems similar to blockchain, that exist for the purpose of

promoting end-to-end trust in online transactions as well as transparency and openness in transaction history.

Artificial intelligence can also play a role in reducing the need for training by helping in the automation of some of the actions people have to take to manage the risks pertaining to their digital identity, as well as help in building a robust solution to manage digital identity.

Conclusions

Cybersecurity threats and their impact on people's digital identity has been a significant topic discussed in the news as well as in social settings. The impact of these threats has affected a great number of people in all age groups. This study focuses on the 55 to 75-year-old age group, as this category of people is close to retirement or already retired; therefore, a notable compromise impacting their digital identity can cause their financial well-being to be tremendously affected as well as cause a major impact on their life and well-being.

The principal investigator of this study has always perceived that risk awareness of individuals is a step in building a more educated population that is resilient to cyber threats. His experience in the cybersecurity industry and dealing with cyber threat mitigation techniques at the organizational level had him concerned about people. In cybersecurity, individuals are considered a weak link in the cybersecurity mitigation ecosystem. Therefore, building awareness among individuals and making the tools and techniques used to help them mitigate the risks in a user-centric way are essential risk mitigation techniques. To help guide the research; the following research question was formulated, "What are the risk perceptions of individuals, between the ages of 55 and 75 with no IT background, pertaining to their digital identity?"

The literature review conducted resulted in seven themes summarized as follows: 1) Increased internet usage, 2) Digital identity definition, 3) Perspectives on digital identity privacy,

4) Privacy risks, 5) Laws and regulations emerged to support online privacy and digital identity, 6) Individuals' behaviors and habits, 7) Tools and training for digital identity management. The study's interview questionnaire was derived from these themes to help serve as a guide to conduct the interviews. Twenty interviews were conducted with individuals between the ages of 55 and 75 with non-technical IT backgrounds. The interviews were transcribed and coded following the ATA, which resulted in four themes that answer the research question and a qualifier theme.

The themes from the interviews are summarized as follows, first is the qualifier theme that talks about high internet adoption and the use of digital identity. The other themes answering the research question are: 1) People accept the risk when it affects their convenience, 2) People are concerned that companies are not being transparent with regards to being good custodians of their digital identity, 3) People are aware of the availability of tools and trainings to help manage the risks, 4) People want more transparency and control over their digital identity to help them ease their concerns of the risks. The themes from the interviews served as a validator to the themes from the literature review.

The interpretations of the findings from the literature review and the interviews give a perspective on the gaps found and are summarized as follows: 1) The unexpected event quarantine forced an all-time high usage of the internet in the 55 to 75 age group, which required people to understand their digital identity and its composition in order to understand the risks associated with it, 2) The fact that people disregard the risks to their digital identity when it affects their convenience demands that there needs to be a methodology to benchmark and assess personal risk, 3) Online platforms have been the cause of many digital identity breaches, which causes governments to intervene to help protect individuals; thus, many laws seem to be outdated

or not written in a manner to be understood by a non-specialist and require government intervention to help fix that problem, 4) Most of the tools and trainings on the market that manage digital identity are not user-centric; the rise of machine learning and artificial intelligence can help make these tools more wholesome and robust as well as help reduce the end user impact on their efficacy, 5) The demand for more transparency and awareness from people can be solved by leveraging distributed ledger technologies like blockchain or the use of artificial intelligence by helping people establish end to end visibility in their interactions using their digital identity.

The implications of this study state that with the increased adoption of digital identity and its usage, individuals need to be aware of the different risks associated with using the online medium and efficient ways to manage these interactions to help facilitate online interactions.

As with any type of new system to be used, there needs to be enough information to help properly utilize the system. Thus, the system needs to be efficient, informative as well as a user-centric personal risk management framework to follow to use and manage digital identity effectively and with low risk. The proper rules and regulations need to be in place to help set the standards and best practices on how to use digital identity and manage it efficiently.

Governments as well as the private sector, need to place more emphasis on end-user controls and protection and communicate it properly to people. Once the laws and regulations are established, user-friendly tools are needed to enable the proper management of digital identity; tools are a great enabler once built successfully around users' needs while considering their adaptability to help support the rules and the regulations put in place by governments and private industry.

Some new technologies on the market, like blockchain and artificial intelligence, may be an enabler as well as an enhancer of tools that help support end-users in managing their digital identity by simplifying the user's dependency and automating the processes that help people stay protected.

With the right rules and regulations as well as the proper tools in place, training and awareness become essential in making sure the rules are communicated efficiently and in a user-friendly manner to individuals. They are also important to understanding the different options in tools on the market to help enable compliance with these rules and regulations to enhance the management of digital identity. The distinction between the different tools on the market and their utility to satisfy the specific use cases they were built to support needs to be communicated to the masses to help people choose the tailored solutions they need to keep their digital identity secure.

End users truly need transparency, control, and user-friendliness as characteristics of information systems. Since digital identity is part of information systems, those characteristics are essential and have to be baked in the process of developing mechanisms to help promote, manage, and safely keep people's digital identity and all of its related information and interactions online.

Contribution to Academics and Practitioners

The themes of the findings in this study as well as the study details generated from the interviews and compared to the literature review, are empirical findings that are useful to individuals and organizations trying to solve the problem of managing digital identity and keeping it secure.

From the perspective of individuals, most study participants expressed their eagerness to learn the study results once the study was complete. The investigator received several requests from interview participants regarding the status of the research and whether the results were generated and ready to be shared. The results of this study will help people understand where they stand with regards to other people in the population studied, individuals between the ages of 55 and 75 with a non-career IT technical background. This information is important for people to see the diversity of perspectives that similar individuals in their studied population have; this information also shows the variety of perspectives generated from different life events and experiences as well as the different level of awareness that individuals have regarding risks pertaining to their digital identity and online interactions.

From an academic perspective, this study sets the foundation for trying to understand people's perspectives with regards to digital identity risks, which was lacking in the literature review conducted with regards to academic articles and existing research.

Limitations and Future Research

Multiple limitations are associated with this study. The first limitation and a notable one is the fact that this study was conducted during an unpredictable event. When the investigator was preparing to solicit interview participants for the study, the COVID-19 pandemic started and forced people to be quarantined in their homes. This event was a global pandemic that affected the way people interact. As a result, conducting interviews in person, which was the original intent of the investigator, was no longer possible. To generalize this phenomena; it can be considered that any major event, similar to this one, will cause a shift in people's behavior and make them adapt to certain circumstances, that might force them to be more avid users of the internet.

To accommodate the situation, the investigator transitioned to using video conferencing via Zoom as the medium to conduct the interviews. Even though video conferencing was the best option to keep the study going, this approach made the interviews less personable, where the investigator was not able to read the interviewees' perspectives similar to what could have been done when interviews are conducted in person. This approach also might have omitted some people who are not users of the internet and would have been part of this study in different circumstances.

The second limitation is the sample population studied; interview participants were from various backgrounds and, in some cases, lived in different countries. Interview participants were recruited from the United States, Canada, and the United Kingdom. People with diverse backgrounds living in different countries and environments do not have consistent perspectives on the risks pertaining to their digital identity, considering the milieus that they live in as well as the rules, laws, and regulations promoted and enforced in three countries with three different types of governance systems and corporate environments.

The third limitation, and an excellent avenue for future research, is the number of participants. In the future, the findings of the themes of this study can be used to build a survey for a significantly larger audience to test the validity of the results in more of a census type of perspective and research. Those types of studies usually involve hundreds of people as part of the targeted population for research and can help validate or prove wrong some of the themes and the findings from this study.

The fourth limitation, and also an excellent venue for future research, is the population interviewed. This population can be expanded beyond non IT career-oriented people between the

ages of 55 and 75 to include IT career-oriented individuals in the same age group and compare the difference in the answers between both groups.

The fifth limitation and an intriguing avenue for future research is to generation. This study can be expanded to inter age focused groups. It would be fascinating to see the perspectives of risks pertaining to digital identity in a comparison between the different age groups: Centennials, Millennials, Gen Xers, and Baby Boomers.

Multiple other interesting areas of future research also include studying each of the risks found in the interviews in more depth in details, studying the tools available on the market that help in managing digital identity, and trying to determine their effectiveness as well as generating specific suggestions on how to improve them. Another interesting area for future study is the cognitive ability and mental aspect of technology users and its impact on digital identity, which touches on cognitive ability, information delivery, and processing aligned with the behavioral information system analysis.

REFERENCES

- Alashoor, T., Baskerville, R., & Zhu, R. (2016). Privacy and identity theft recovery planning: An onion skin model. doi:10.1109/HICSS.2016.461
- Alkaldi, N., Renaud, K., & Mackenzie, L. (2019). Encouraging password manager adoption by meeting adopter self-determination needs. Retrieved from <http://eprints.gla.ac.uk/169744>
- Al-Khouri, A. M. (2014). Digital identity: Transforming GCC economies. *Innovation: Management, Policy & Practice*, 16(2), 184-194. Retrieved from <https://search.proquest.com/docview/1645743237?accountid=14745>
- Allison, A., Currall, J., Moss, M., & Stuart, S. (2005). Digital identity matters. *Journal of the American Society for Information Science and Technology*, 56(4), 364-372. doi://dx.doi.org/10.1002/asi.20112
- Alsaedi, T., Stefanidis, A., Phalp, K., & Ali, R. (2019). Social transparency in enterprise information systems: Peculiarities and assessment factors. *2019 6th International Conference on Behavioral, Economic and Socio-Cultural Computing (BESC)*, 1-4. doi:10.1109/BESC48373.2019.8963048
- Anakath, A. S., Rajakumar, S., & Ambika, S. (2019). Privacy preserving multi factor authentication using trust management. *Cluster Computing*, 22(S5), 10817-10823. doi:10.1007/s10586-017-1181-0
- Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and privacy: Concerned, confused and feeling lack of control over their personal information. 85, 88-93. Retrieved from <https://statistical.proquest.com/statisticalinsight/result/pqpresultpage.previewtitle?docType=PQSI&titleUri=/content/2019/R8588-93.22221.xml>
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age. *Management Information Systems*, 35(4), 1017-1041. Retrieved from <http://www.econis.eu/PPNSET?PPN=675839327>
- Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. SAGE Publications. Retrieved from https://books.google.com/books?id=_rfCIWRhIKAC

- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. doi:10.1191/1478088706qp063oa
- Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology*, 18(6), 641-651. doi:10.1002/acp.1014
- Brunk, J., Mattern, J., & Riehle, D. M. (2019). Effect of transparency and trust on acceptance of automatic online comment moderation systems. 429-435. doi:10.1109/CBI.2019.00056
- California Consumer Privacy Act. (2018). Retrieved from <https://oag.ca.gov/privacy/ccpa>
- Cambridge English Dictionary. (2020). Identity. In *Cambridge English dictionary*. Retrieved from <https://dictionary.cambridge.org/us/dictionary/english/identity>
- Camp, J. L. (2004). Digital identity. *IEEE Technology and Society Magazine*, 23(3), 34-41. doi:10.1109/MTAS.2004.1337889
- Charney, S. (2009). The evolution of online identity. *IEEE Security & Privacy*, 7(5), 56-59. doi:10.1109/MSP.2009.140
- Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70, 291-302. <https://doi.org/10.1016/j.chb.2017.01.003>
- Choi, D. D., Wang, G. A., & Lowry, P. B. (2020). The design of personal privacy and security risk scores for minimizing consumers cognitive gaps in IOT settings. *Advances in Design Science Research*. doi:10.24251/HICSS.2020.624
- Clarke, V., & Braun, V. (2018). Using thematic analysis in counselling and psychotherapy research: A critical reflection. *Counselling and Psychotherapy Research*, 18(2), 107-110. doi:10.1002/capr.12165
- Colbert, A., Yee, N., & George, G. (2016). The digital workforce and the workplace of the future. *Academy of Management Journal*, 59(3), 731-739. doi:10.5465/amj.2016.4003
- Cooper, C. (2017, October 10). *Awareness training is key to reducing security risk*. Cybersecurity insights. Retrieved from <https://www.csoonline.com/article/3229969/awareness-training-is-key-to-reducing-security-risk.html>
- Corbin, J., & Strauss, A. (2014). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. SAGE Publications. Retrieved from <https://books.google.com/books?id=hZ6kBQAAQBAJ>

- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches*. SAGE Publications. Retrieved from <http://ezproxy.lib.usf.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cab00847a&AN=usflc.036209374&site=eds-live>
- Dhamija, R., Tygar, J., & Hearst, M. (2006). Why phishing works. *CHI '06 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/1124772.1124861
- Dourish, P., Grinter, R., Delgado de la Flor, J., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6), 391-401. doi:10.1007/s00779-004-0308-5
- Dutil, P. A., Howard, C., Langford, J., & Roy, J. (2007). Rethinking government-public relationships in a digital world: Customers, clients, or citizens? *Journal of Information Technology & Politics*, 4(1), 77-90. doi:10.1300/J516v04n01_06
- Emont, J., Stevens, L., & McMillan, R. (2018). Amazon investigates employees leaking data for bribes. *Dow Jones Institutional News*. Retrieved from <https://www.wsj.com/articles/amazon-investigates-employees-leaking-data-for-bribes-1537106401>
- European Union Agency for Cybersecurity. (2020). Security of personal data. Retrieved from <https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data>
- European Union. (2016). General data protection regulation. *Official Journal of the European Union*, L(31), 1-88. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1559428229433&uri=CELEX:32016R0679>
- Federal Trade Commission. (2012). Privacy choices for your personal financial information. Retrieved from <https://www.consumer.ftc.gov/articles/0222-privacy-choices-your-personal-financial-information>
- Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, 5(1), 80-92. doi:10.1177/160940690600500107
- Florencio, D., & Herley, C. (2006). A large scale study of web password habits. Retrieved from <https://www.microsoft.com/en-us/research/publication/a-large-scale-study-of-web-password-habits/>
- Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. *WWW '07 Proceedings of the 16th international conference on World Wide Web*. doi:10.1145/1242572.1242661 Retrieved from <http://dl.acm.org/citation.cfm?id=1242661>

- Gaw, S., & Felten, E. (2006). Password management strategies for online accounts. *SOUPS '06: Proceedings of the second symposium on Usable privacy and security*. doi:10.1145/1143120.1143127
- Gramm-Leach-Bliley Act (2002). Retrieved from <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act>
- Granville, K. (2018, March 19). Facebook and Cambridge Analytica: What you need to know as fallout widens. *New York Times*. Retrieved from <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>
- Green, A. (2019). Complete guide to privacy laws in the US. Varonis. Retrieved from <https://www.varonis.com/blog/us-privacy-laws/>
- Gunasinghe, H., Kundu, A., Bertino, E., Krawczyk, H., Chari, S., Singh, K., & Su, D. (2019). PrivIdEx: Privacy preserving and secure exchange of digital identity assets. *WWW '19: The World Wide Web Conference*. doi:10.1145/3308558.3313574
- Higashino, M., Kawato, T., Ohmori, M., & Kawamura, T. (2019). An anti-phishing training system for security awareness and education considering prevention of information leakage. *2019 5th International Conference on Information Management (ICIM), Cambridge, United Kingdom*, 82-86. Retrieved from <https://search.proquest.com/docview/2226169708>
- Hodge, R. (2019, December 27). *2019 Data breach hall of shame: These were the biggest data breaches of the year*. Cnet. Retrieved from <https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/>
- Horn, I. S., Taros, T., Dirkes, S., Hüer, L., Rose, M., Tietmeyer, R., & Constantinides, E. (2015). Business reputation and social media: A primer on threats and responses. *Journal of Direct, Data and Digital Marketing Practice*, 16(3), 193-208. doi:10.1057/dddmp.2015.1
- Hsu, C., & Lin, J. C. (2016). An empirical examination of consumer adoption of internet of things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior*, 62, 516-527. doi:10.1016/j.chb.2016.04.023
- Hyde, K. F. (2000). Recognising deductive processes in qualitative research. *Qualitative Market Research*, 3(2), 82-90. doi:10.1108/13522750010322089
- Identity Theft Resource Center. (2020). *ITRC 2019 end of year data breach report*. Retrieved from https://www.idtheftcenter.org/2019-data-breaches/?utm_source=web&utm_medium=sitewidenotice&utm_campaign=01282020_019DataBreachReport

- International Association of Privacy Professionals. (2020). What does privacy mean? Retrieved from <https://iapp.org/about/what-is-privacy/>
- Kahn, C., & Liñares-Zegarra, J. M. (2016). Identity theft and consumer payment choice: Does security really matter? *Journal of Financial Services Research*, 50(1), 121-159. doi:10.1007/s10693-015-0218-x
- Katzan, H. Jr. (2011). Ontology of trusted identity in cyberspace. *Journal of Service Science*, 4(1), 1-11. Retrieved from <https://search.proquest.com/docview/868857882?accountid=14745>
- Kim, J., Baskerville, R. L., & Ding, Y. (2018). Breaking the privacy kill chain: Protecting individual and group privacy online. *Information Systems Frontiers*, 1-15. doi:10.1007/s10796-018-9856-5
- Legal Monitor Worldwide. (2020, January 22). NIST publishes privacy framework version 1.0.
- Merriam-Webster. (2020a). Definition of privacy. In *Merriam-Webster.com dictionary*. Retrieved from https://www.merriam-webster.com/dictionary/privacy?utm_campaign=sd&utm_medium=serp&utm_source=js onld
- Merriam-Webster. (2020b). Identity definition. In *Merriam-Webster.com dictionary*. Retrieved from <https://www.merriam-webster.com/dictionary/identity>
- Mueller, M. L., Park, Y., Lee, J., & Kim, T. (2006). Digital identity: How users value the attributes of online identifiers. *Information Economics and Policy*, 18(4), 405-422. doi://doi.org/10.1016/j.infoecopol.2006.04.002
- Myers, M. (2013). *Qualitative research in business and management*. SAGE Publications.
- National Institute of Standards and Technology. (2017). *Digital Identity Guidelines*. Retrieved from <https://csrc.nist.gov/publications/detail/sp/800-63/3/final>
- National Institute of Standards and Technology. (2018a). *Framework for improving critical infrastructure cybersecurity*.
- National Institute of Standards and Technology. (2018b). *NIST risk management framework*. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>
- Neck, C. (2015). Disappearing women: Why do women leave senior roles in finance? *Australian Journal of Management*, 40(3), 488-510. doi:10.1177/0312896215578014
- Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for usable cybersecurity: Past and present. *2011 Third International Workshop on Cyberspace*

- Safety and Security (CSS)*, Milan. doi:10.1109/CSS.2011.6058566 Retrieved from <https://ieeexplore.ieee.org/document/6058566>
- Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, 25(2), 243-262. doi:10.1016/S0167-4870(02)00172-1
- Papangelis, K., Chamberlain, A., Lykourantzou, I., Khan, V., Saker, M., Liang, H., Sadien, I., & Cao, T. (2020). Performing the digital self. *ACM Transactions on Computer-Human Interaction*, 27(1), 1-26. doi:10.1145/3364997
- Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy*, 10(3), 76-79. doi:10.1109/MSP.2012.73
- Perlroth, N., Satariano, A., & Tsang, A. (2018, November 30). Marriott hacking exposes data of up to 500 million guests. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html>
- Privacy Act of 1974. (2014). Retrieved from <https://www.justice.gov/opcl/privacy-act-1974>
- Rossi, P. (2007). How to link the qualitative and the quantitative risk assessment. *Paper presented at the PMI® Global Congress 2007-EMEA, Budapest, Hungary*. Newtown Square, PA: Project Management Institute.
- Saldaña, J. (2016). *The coding manual for qualitative researchers*. SAGE Publications. Retrieved from <http://ezproxy.lib.usf.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cab00847a&AN=usflc.034045048&site=eds-live>
- Schwartz, P. M. (2013). The EU-U.S. privacy collision: A turn to institutions and procedures. *Harvard Law Review*, 126(7), 1966-2009. Retrieved from <https://www.jstor.org/stable/23415063>
- Seidman, I. (2013). *Interviewing as qualitative research : A guide for researchers in education and the social sciences*. Teachers College Press. Retrieved from <http://ezproxy.lib.usf.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cab00847a&AN=usflc.031021394&site=eds-live>
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *CHI '10: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/1753326.1753383

- Shin, L. (2014). 'Someone had taken over my life': An identity theft victim's story. Forbes. Retrieved from <https://www.forbes.com/sites/laurashin/2014/11/18/someone-had-taken-over-my-life-an-identity-theft-victims-story/>
- Sobolewski, M., Mazur, J., & Paliski, M. (2017). GDPR: A step towards a user-centric internet? *Intereconomics*, 52(4), 207-213. <http://dx.doi.org/10.1007/s10272-017-0676-5>
- Srivastava, A., & Geethakumari, G. (2013). Measuring privacy leaks in online social networks. *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Mysore*. doi:10.1109/ICACCI.2013.6637504
- Stack, B. (2017). Here's how much your personal information is selling for on the dark web. Retrieved from <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>
- Sullivan, C. (2014). Protecting digital identity in the cloud: Regulating cross border data disclosure. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 30(2), 137-152. doi:10.1016/j.clsr.2014.01.004
- Sullivan, C. (2015). *Protecting digital identity in the cloud*. In *The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues* (pp. 149-170). Boston: Syngress. doi.org/10.1016/B978-0-12-801595-7.00007-0
- Sullivan, C. (2016). Digital citizenship and the right to digital identity under international law. *Computer Law & Security Review*, 32(3), 474-481. doi.org/10.1016/j.clsr.2016.02.001
- Sullivan, C. (2018). Digital identity – from emergent legal concept to new reality. *Computer Law & Security Review*, 34(4), 723-731. doi.org/10.1016/j.clsr.2018.05.015
- U.S. Department of Health & Human Services. (2015). What is PHI? Retrieved from <https://www.hhs.gov/answers/hipaa/what-is-phi/index.html>
- U.S. Department of Labor. (2020). Guidance on the protection of personal identifiable information. Retrieved from <https://www.dol.gov/general/ppii>
- “US fines Facebook \$5 billion for privacy violations.” (2019, July 24). Deutsche Welle. Retrieved from <https://www.dw.com/en/us-fines-facebook-5-billion-for-privacy-violations/a-49730844>
- Vogels, E. A. (2019). Millennials stand out for their technology use, but older generations also embrace digital life. Retrieved from <https://www.pewresearch.org/fact-tank/2019/09/09/us-generations-technology-use/>
- Wolfond, G. (2017). A blockchain ecosystem for digital identity: Improving service delivery in canada's public and private sectors. *Technology Innovation Management Review*, 7(10),

35-40. Retrieved from
<https://search.proquest.com/docview/1963139579?accountid=14745>

Woodhouse, S. (2007). Information security: End user behavior and corporate culture. *Paper presented at the 7th IEEE International Conference on Computer and Information Technology (CIT 2007)*, 767-774. doi:10.1109/CIT.2007.186

Zastrow, J. (2014). The digital archivist: PIM 101: Personal information management. *Computers in Libraries*, 34(2).

APPENDIX A:

INTERVIEW SOLICITATION FLYER



**RESEARCH INTERVIEW
PARTICIPANTS NEEDED!**

Seeking individuals between the ages of 55 to 75 for a 30 minute interview to support a study conducted by a doctoral candidate at The University of South Florida regarding online interactions and digital personal data awareness.

Kindly contact Tom for more details:

Tom Chebib	Tom Chebib	Tom Chebib	Tom Chebib	Tom Chebib
tchebib@mail.usf.edu	tchebib@mail.usf.edu	tchebib@mail.usf.edu	tchebib@mail.usf.edu	tchebib@mail.usf.edu
(919)809-9686	(919)809-9686	(919)809-9686	(919)809-9686	(919)809-9686

APPENDIX B:
IRB VERBAL CONSENT FORM

Script for Obtaining Verbal Informed Consent Information to Consider Before Taking
Part in this Research Study **Title: Digital Identity: A Human Centered Risk Awareness Study**
Study # 000341

Overview: You are being asked to take part in a research study. The information in this document should help you to decide if you would like to participate. The sections in this Overview provide the basic information about the study. More detailed information is provided in the remainder of the document.

Study Staff: This study is being led by Toufic "Tom" Chebib who is a Doctor of Business Administration candidate at the University of South Florida. This person is called the Principal Investigator. Other approved research staff may act on behalf of the Principal Investigator.

Study Details: This **Interview** study is being conducted at a public location (Coffee shop, public library, or virtually) and is supported/sponsored by Doctor of Business Administration program at the University of South Florida, Muma College of Business. The purpose of the Interview/study is to explore the level of awareness of people with regards to the risks that come with their digital interactions in order to try to figure out why. The time commitment is around 30 minutes.

Participants: You are being asked to take part because you fit the profile of people targeted by the study. Individuals between the age of 55 and 75 with no career background in IT.

Voluntary Participation: Your participation is voluntary. You do not have to participate and may stop your participation at any time. There will be no penalties or loss of benefits or opportunities if you do not participate or decide to stop once you start.

Benefits, Compensation, and Risk: We do not know if you will receive any benefit from your participation. There is no cost to participate.. This research is considered minimal risk. Minimal risk means that study risks are the same as the risks you face in daily life.

Confidentiality: Even if we publish the findings from this study, we will keep your study information private and confidential. Anyone with the authority to look at your records must keep them confidential.

If you have any questions, concerns or complaints about this study, call Tom Chebib at (919)809-9686. If you have questions about your rights, complaints, or issues as a person taking part in this study, call the USF IRB at (813) 974-5638 or contact the IRB by email at RSCH-IRB@usf.edu.

Would you like to participate in this study? Yes/No (Verbal)

APPENDIX C:

INTERVIEW QUESTIONNAIRE

Three sections interview:

Section 1: *Background Information on individual online interactions*

- How much time do you spend online per day?
- What do you do?
- Tell me about the last time you used your email? Your social media account?
- Are you aware of how many online profiles you have?
- Do you keep track of them somehow? paper or electronic system?
- Have you ever had to enter your personal information like your physical address, phone number, age? social security number, credit card number etc. online? Tell me more about that experience?
- How comfortable were you providing this information?
- Have you or someone you know been affected by a loss of personal data due to a recent company data compromise (Target, Marriott, Experian...)?
- What do you know about it?
- Did the company responsible for the loss of data provide any details?
- Were they helpful for you or your friend to understand what happened?
- Did this have an impact on you or your friend's digital behavior?

Section 2: *Current behavior*

- What does your online personal data mean to you?

- What are your concerns around your online personal data and digital identity?
- Do you feel that there are potential reputation risks by being online?
- Do you feel that there are potential financial risks by being online, Loss of 401K, or money from your bank/trading accounts?
- What do you know about online privacy rules or laws or regulations?
- Tell me more about it
- Are companies you are interacting with online providing you any transparent information regarding your personal data?
- What do you think they should tell you?
- What do you believe you should do to keep your online data/digital identity secure?
- What are you currently doing to protect your online data?
- How are the risks of digital interactions keeping you from fully using the internet capabilities?
(optional)
- Do you know of any solutions, tools or trainings that help with protecting your online digital data?
- Have you considered using one of these?
- Do you have any friends who currently use these?
- What is your impression on the data privacy solutions to increase awareness? (i.e.: training, software/hardware solutions or guidelines on best practices)
- If an ideal solution existed to help you in managing your online data, what do you think it should tell you or allow you to do?

Section 3: *Future and unmet needs*

- Do you feel that you have unmet needs to keep your digital identity secure?
- Do you think that you need more resources to help manage the risk that come with your digital identity?

APPENDIX D:
IRB APPROVAL EXEMPT FORM



EXEMPT DETERMINATION

February 19, 2020

Toufic Chebib
4202 E. Fowler Avenue
Tampa, FL 33620

Dear Toufic Chebib:

On 2/18/2020, the IRB reviewed and approved the following protocol:

Application Type:	Initial Study
IRB ID:	STUDY000341
Review Type:	Exempt 2
Title:	Digital Identity: A Human-Centered Risk Awareness Study
Funding:	None
Protocol:	Protocol

The IRB determined that this protocol meets the criteria for exemption from IRB review.

In conducting this protocol, you are required to follow the requirements listed in the INVESTIGATOR MANUAL (HRP-103).

Please note, as per USF policy, once the exempt determination is made, the application is closed in BullsIRB. This does not limit your ability to conduct the research. Any proposed or anticipated change to the study design that was previously declared exempt from IRB oversight must be submitted to the IRB as a new study prior to initiation of the change. However, administrative changes, including changes in research personnel, do not warrant a modification or new application.

Ongoing IRB review and approval by this organization is not required. This determination applies only to the activities described in the IRB submission and does not apply should any changes be made. If changes are made and there are questions about whether these activities impact the exempt determination, please submit a new request to the IRB for a determination.

Sincerely,

Jennifer Walker
IRB Research Compliance Administrator

A PREEMINENT RESEARCH UNIVERSITY

Institutional Review Boards / Research Integrity & Compliance

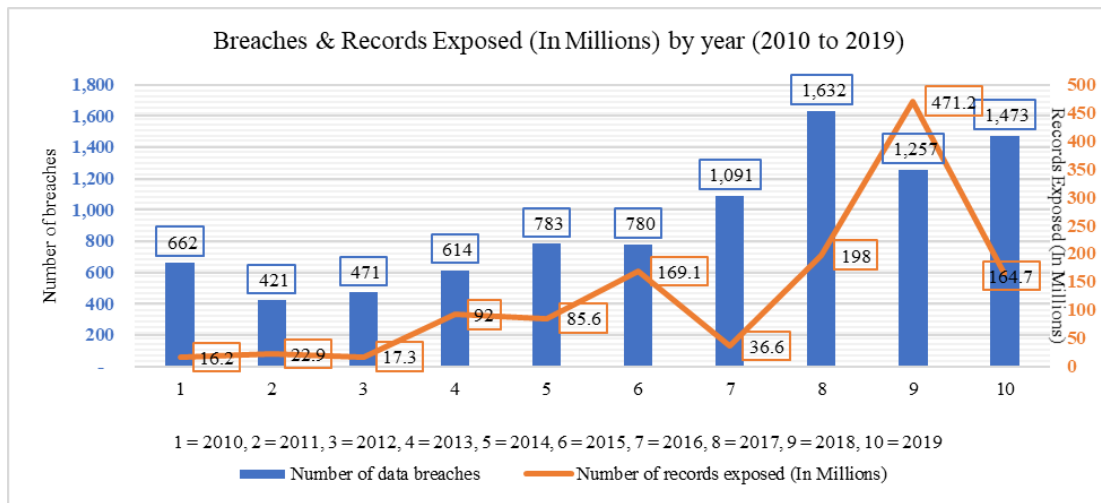
FWA No. 00001669
University of South Florida / 3702 Spectrum Blvd., Suite 165 / Tampa, FL 33612 / 813-974-5638

Page 1 of 1

APPENDIX E:

ITRC 2019 DATA BREACH REPORT STATISTICS

Table 1A. Breaches and Records Exposed (In Millions) by Year (2010 to 2019). *



* Source: Based on data from Identity Theft Resource Center (ITRC), [2019 End of Year Data Breach Report](#).