USF® Muma Business Review
A publication of the Muma College of Business | University of South Florida

Volume 5, Number 4 | *Research Summary for Practice* | *31 DECEMBER 2021#*

Digital Identity: A Human-Centered Risk Awareness Study

By
Toufic Chebib, University of South Florida

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?* 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: 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 training to help manage the risks, 4) people want more transparency and control over their digital identity to help ease their concerns of the risks.

Cybersecurity breaches have been at the forefront of most news outlets, recently. People's Digital Identity has been at the epicenter of cybersecurity breaches. Defining digital identity, proper risk mitigation tools and the supporting guidance in standards and frameworks is key for risk mitigation.

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.

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

Findings

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.

Themes from the interviews served as a validator to the themes from the literature review. 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 training 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.

Discussion

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 matter 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 or artificial intelligence by helping people stablish end to end visibility in their interactions using their digital identity.

Methodology

The adaptive thematic analysis (ATA) framework was used to code my transcripts. I used it to generate the themes and key concepts in order to produce a report of the findings. First, I used a top-down approach, by reading through the transcripts, and developing an initial coding process and groupings, this step is also known as open coding. Second, I read through the transcripts from the bottom up, and generated an initial set of codes. I then identified my preliminary findings; this step is also known as Axial coding. The third step I took, was to connect the codes and group them into themes. I then validated the themes, to make sure they connect with each other cohesively. The last step, was to produce the report of my findings and analysis, based on the themes found in the interviews.

There have been different interpretations, variations, and adjustments, of Thematic Analysis throughout the years. Just like any good framework, I adapted a collective of the variations to my use case, to support this study. I decided to combine a few of the frameworks, that focus on thematic analysis, into my own adaptation. Notably, I took into consideration, the methodologies produced by Richard Boyatzis (1998) and followed by Braun and Clark (2006).

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 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 matter 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 safe keep people's digital identity and all of its related information and interactions online.

References

Boyatzis, R. (1998). Transforming qualitative information : thematic analysis and code development. Sage Publications.

Braun, V. & Clarke, V. (2006) Using thematic analysis in psychology, Qualitative Research in Psychology, 3:2, 77-101, DOI: 10.1191/1478088706qp063oa

Review

This article was accepted under the ***constructive peer review*** option. For futher details, see the descriptions at:

http://mumabusinessreview.org/peer-review-options/

Authors

Toufic Chebib is an IT and Cybersecurity leader. He serves as a Vice President at Citibank's Cybersecurity division, managing their Technology Risk & Controls portfolio. Prior to Citi, he was a cybersecurity program manager at the Centers of Medicare and Medicaid Services which is an organization with over a Trillion dollars in budget. Before his IT career, he was a senior executive in the retail industry, hiring over 4000 people and directing operations for a restaurant chain valued at over 45 Million dollars. He received his Doctor in Business Administration degree in December 2020.