FROM INNOCENT IRENE TO PARENTAL PATRICK: FRAMING USER CHARACTERISTICS AND PERSONAS TO DESIGN FOR CYBERSECURITY

Kim, Euiyoung (1); Yoon, JungKyoon (2); Kwon, Jieun (3); Liaw, Tiffany (4); Agogino, Alice M. (5)

Organisations:
(1) Jacobs Institute for Design Innovation, University of California at Berkeley
(2) Department of Design and Environmental Analysis, Cornell University
(3) Human Factor and Ergonomics, University of Minnesota
(4) Bioengineering, University of California at Berkeley
(5) Mechanical Engineering, University of California at Berkeley

ABSTRACT
With the surging number of digital devices penetrating our daily routines, the risks inherent to cybersecurity—the protection of data on digital products connected to the Internet—have also increased since these devices (e.g., connected home devices, personal monitoring) collect, process, analyze and store users' sensitive personal information. Thus, there is a pressing need to assist users in being aware of and dealing with potential cybersecurity threats. With the proposition that fulfilling the need starts with developing an in-depth understanding of the user behaviors in the context of cybersecurity, an exploratory study was conducted that employed three mixed qualitative and quantitative research methods—a trend analysis, an interview study, and an online survey study. The paper reports the user characteristics on (1) awareness levels of cybersecurity issues, (2) uses of digital devices, and (3) means of dealing with the privacy issues in product use. The results of the studies were translated into eight personas that systematically reflect distinct characteristics of users, which can help designers empathize with their potential users vulnerable to cybersecurity risks.

Keywords: Human behaviour in design, User centred design, Ethics, Early design phases

1 INTRODUCTION

We live in the world of high-tech devices—from small mobile devices to large home electronics. As newly developed devices increasingly interact with such daily devices connected to the Internet, an immense quantity of information and physical infrastructures are becoming intertwined and inseparable (Ten et al., 2010 & 2008). The growth trend of such communication webs has surged and the number of Internet of Things (IoT) devices surpassed the number of people on Earth in 2011 (Gubbi et al., 2013; Piyare, 2013). The US National Intelligence Council predicts that by the year 2025, our non-digital artifacts will be integrated into the IoT applications across food packages, furniture and even paper documents (Atzori et al., 2009).
One side-effect of the emergence and popularity of everyday connected devices is that our lives are inadvertently becoming dependent on cyberspace, in which many people can be potentially in danger of cyberattacks and cybercrimes (Bruijn and Janssen, 2017). The forms of cyberattacks vary from simple identity theft to take-over of governmental systems, and medical equipment, to automatic driving/flight controls. The types of these dangers have been increasingly shifted from online to offline: the collection of online data such as age, gender and geological location to offline user data such as activities, environment, and affective states (Rosner and Kenneally, 2018). The extent of the damage is not trivial. Indeed, former US President Barack Obama pointed out that cybersecurity risks have become "the most serious challenge" in the 21st century. In response, several initiatives have been taken in various areas to build a robust network and ecosystem of cybersecurity professionals, e.g., national cybersecurity division in the US Department of Homeland Security and National Initiative for Cybersecurity Education (National Institute of Standard and Technology, 2018; Singer and Friedman, 2014).
Despite such efforts to prevent (or minimize) cyberattacks, the majority of the population seems to remain vulnerable because of the complex and nuanced nature of cybersecurity problems. One

noteworthy issue is that the problems cannot always be solely attributed to technology failures. In fact, many cybersecurity risks are associated with human factors concerns, e.g., unforeseen user errors in the interactions with products (Marble et al., 2014). This implies that state-of-art security technologies alone would not be sufficient in protecting users, given the fact that in most cases of cyberattack, they are the ones who make the decisions in the instances that leak their personal information (Abawajy, 2014). To render users amenable to protect their privacy from the potential cyberattacks, cybersecurity campaigns are among the most common interventions to influence users to increase their cybersecurity awareness and change their behaviors (Harknett and Stever, 2011). However, Bada and Sasse (2014) reveal that the most current cybersecurity campaigns have not led to improved cybersecurity awareness and desirable behavior change. Comparably, designers who create new products, including services and systems, tend not to pay much attention to potential users' situated needs around cybersecurity in their design process (Kim et al., 2018).

We postulate that such campaign interventions do not adequately reflect the diversity of user groups and their situated needs, thus failing to be integrated into everyday practice of technology use. To overcome this challenge, we propose to identify characteristics of users and their real-life behaviors, and to develop personas accordingly. The resulting outcomes would help designers to increase their understanding of their potential users vulnerable to cybersecurity risks and create tailored design solutions. Personas are representations of intended users' characteristics (e.g., demographics, behaviors, and knowledge) and their values and needs (Cooper, 1999; Miaskiewicz and Kozar, 2011; Pruitt and Adlin, 2010). Personas have been proven to be effective in identifying design opportunity spaces especially when the accessibility to potential user segments are restricted (Chang et al., 2008; Faily and Flechais, 2011; McKenna et al., 2015; Kim et al., 2013). Personas in conjunction with other user-design methodologies allow designers to identify characteristics of specific users in the target group (e.g.., users vulnerable to cybersecurity risks). Persona developments assist designers to focus design decisions to meet the needs of the intended target audience (Massanari, 2010).

In the literature of cybersecurity, several personas have been proposed that focused on the characteristics of stakeholder's roles involved in preventive cybersecurity solutions, e.g., IT managers, software developers, data analyst (McKenna et al., 2015; Faily and Flechais, 2011). These personas are valuable to develop tools that reflect the needs of cybersecurity development teams (Stoll et al., 2008). However, they do not particularly help designers understand when and how users become susceptible to cybersecurity issues. The goal of this research is to develop user personas by investigating characteristics of users in relation to user perceptions of cybersecurity risks, when and how they encounter cybersecurity issues and how they respond to cybersecurity risks. We adopted the approach of data-driven persona development (for an overview, see McGinn and Kotamraju, 2008).

The paper describes the research approach taken to identify user characteristics (Section 2), followed by a summary of the results (Section 3). Section 4 presents the formulated user personas and discusses their characteristics. The paper ends with general findings, discussions, including limitations, and future research directions.

2 METHODS AND DATA SOURCES

Three qualitative and quantitative research methods were triangulated: a trend analysis, interviews, and online surveys. The mixed-methods were meant to compare and complement the data collected from different sources and ensure the comprehensiveness and expressiveness of the personas (Adlin and Pruitt, 2010; Faily and Flechais, 2011). These three methods determine the general stages of the research, in which the research findings from each method are associated with the progress of developing personas, which is illustrated in Figure 1.

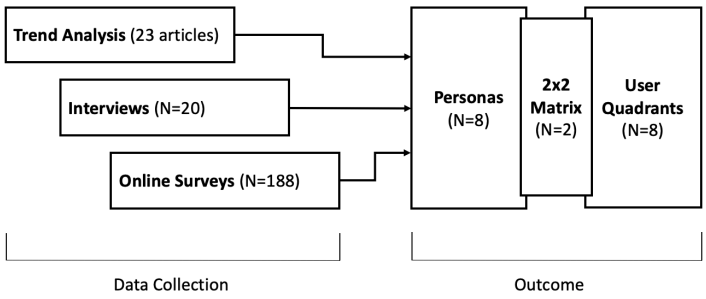

Figure 1. A sequence of the research approach and outcomes

Trend analysis. The trend analysis included a study of emerging cybersecurity threats reported in the media press that was published in the last ten years to frame the scope of research, identifying the where and when users encounter cybersecurity attacks. Online articles reporting recent large-scaled

cybersecurity breach incidents were identified that covered various business sectors, e.g., social media, telecommunication, and retail stores. Only articles that specified the types of cybersecurity issues, the causes, and the extent of the damages were considered for further examination, resulting in 23 articles (e.g., Armerding, 2018; Newman, 2018). With the 23 articles on cybersecurity breach incidents, we examined the cybersecurity problem types by distinguishing two factors: cyberattacks on information and hardware. 'Cyberattack on information' refers to the attacks resulting in information breach or lost (e.g., the leak of a customer's credit card information). 'Cyberattack on hardware' refers to the impact of the attacks on the operation and safety of the physical artifact (e.g., the driving paths of rail trains changed by a hacker's attack). The numbers of the victims were categorized as either smaller than one thousand, or larger than one thousand. The results indicated that among the collected incidents, each cyberattack on information tended to victimize more than one thousand people taking 71.4 % of the cases, more than half of which were on information breaches. Each cyberattack on hardware resulted in less than one thousand victims (28.6%) (e.g., Tesla Model S stolen by a hacker's cloned key fob). Although the severity of the attacks may vary for information breach and physical attack, the number of the victims was the highest for all cases of cyberattacks on information and hardware. Given the results, it appeared to be of importance to explore the possible attack points in daily device use, while also examining the cybersecurity awareness of the users. Taken together the government reports and popular media reports (e.g., Newhouse et al., 2017; Rosner and Kenneally, 2017), it was decided to look into the characteristics of vulnerable populations who are more prone to cybersecurity breach and create representative personas coupled with user characteristics identified herein.

Interviews. The goal of conducting semi-structured interviews (N=20, 10 males, 10 females) were to learn users' perspectives on cybersecurity problems and to examine general cybersecurity awareness. The ages of the participants ranged from 19 and 70 years old (M= 44, SD=17). Age breakdown of the interviews were: 18-29 range (6 participants), 30-49 range (4 participants), 50-64 range (8 participants), 65+ (2 participants). There were 10 participants who had children. Participants were recruited at public areas including cafés, airports, or references from peers. The interview questions were guided by the research prompts associated with: (1) the perception on cybersecurity issues, (2) the contexts in which cybersecurity attacks occur, and (3) users' responses and concerns. The data from these interviews were compiled and analyzed by observing underlying patterns amongst certain characteristics, such as demographics, cybersecurity awareness, having children with access to their devices or other unique factors. The interviews were carried out individually and took about 15-30 minutes each. The preliminary insights gained from the interviews informed the online survey in terms of the questionnaire items and characteristics of the initial personas.

Online survey. Building on the results of the trend analysis and interview study, an online survey was carried out in which participants (N=188) reported (1) their awareness of cybersecurity issues, (2) their ways of using digital devices and services of their own and (3) their ways of dealing with the cybersecurity issues. This was, with a randomized large-group data, to grasp a large picture of the relationship between user characteristics (e.g., gender, age, device usage environment, etc.) and usage behavior related to cybersecurity risks.

3 RESULTS

This section summarizes the results from each of the primary methods used to develop the personas.

3.1 Interview analysis

In addressing research questions around digital device and services usage, we noted what digital devices each participant owned. All participants owned a computer (desktop or laptop) and a smartphone, with an exception of one participant who had a flip phone with no access to the Internet. The participants who owned these devices reported the main use for their computer was for work and occasionally entertainment or reading the news. All participants reported that they mainly owned their phones as a necessity to communicate with family members, coworkers or friends. Other uses for their phones included entertainment or social media. Five participants reported owning an IoT device (e.g., Google Home, Alexa, smart TV), but only two participants actively use the devices for reasons of security (e.g., smart lock) or for driving their car efficiently (e.g., Tesla dashboard). Regarding methods of dealing with privacy issues, we found that there were some common methods among the participants in protecting their privacy on their devices. Most participants reported protecting their data through password-related actions such as using complex passwords, recording passwords on an external source or creating different passwords for different accounts. We also found that those that have previously or

currently worked in the field of technology performed more technological-related methods of protecting their data, including use of a Virtual Private Network (VPN), firewalls or an encrypted hard drive. Most of these participants also tended to provide minimal personal data and would even falsify their personal data or refuse services if they required too much data.

When analyzing the results from the interviews, age was an important factor for characterizing the general public since unique cybersecurity behaviors and trends were present amongst the different age groups. Some unique behaviors were also present for the participants who had children old enough to own and use a digital device. These characteristics and trends were used in order to formulate the eight personas further explored in section 4. Here are main characteristics of users by age groups. Due to the insufficient number of participants in an age group 31-40, the discussion of that group is excluded.

- Two significant subgroups were present in the participants between 19-30 years of age, typically college students. One subgroup was well aware of the risks of cybersecurity, most likely due to their high exposure to the field of technology as they studied computer science or have worked in a tech-related job. Because of their high awareness and methods (e.g., firewalls and VPN) to protect their data, they were vigilant in protecting their data and providing minimal personal information. If they did provide information, they oftentimes would falsify their personal information to get access to the service. The other subgroup that emerged amongst this age group was those with moderate knowledge of cybersecurity. They understood that there were risks with providing personal data on their devices, but they only take protective action depending on their peer's cybersecurity behaviors or if they hear news of a cybersecurity incident. They did not care much about protecting their personal information, as long as they were able to get access to the service.
- Cybersecurity awareness of the participants in the age group of 40-59 varied from either very high (because their jobs deal with sensitive information) or very low (because they do not need cybersecurity knowledge in their day-to-day lives). Regardless of their awareness level, the age group tended to be very protective in preventing cybersecurity breaches and hiding their personal data. Those with high awareness knew several methods to protect their data, oftentimes having complex passwords or providing limited personal information. Those with low awareness would use similar methods because their spouses or coworkers would encourage these behaviors.
- Two participants who were 65+ years tended to own few digital devices and mainly used them for communication purposes. They admitted to their low awareness of risks of providing personal data or even how their devices worked. Because they did not depend on these devices on a daily basis, they did not take much action to protect their information.
- Ten participants had children old enough to use digital devices on their own. Although their levels of cybersecurity awareness varied, the majority were concerned about their children's cybersecurity risks. Despite their concerns, only two participants actively monitored their children's usage behaviors. The other participants reported that they either already warned their children of cybersecurity risks or they expected their children to be familiar with potential harm.

3.2 Online survey

Data from a total of 206 participants were collected through Amazon Mechanical Turk (hereafter referred to as MTurk). Among the dataset, six incomplete surveys were excluded from analysis. Of the remaining 188 participants, (male: 122), age breakdown was as follows: the 19-30 range (133 participants), the 31-40 range (47 participants), the 41-64 range (19 participants), and the 65+ range (three participants. There were 94 participants who answered 'single', and 95 who answered 'married' or 'married with children'.

3.2.1 Survey design and analyses

The survey consisted of three parts, each inquiring (1) general frequency of device use (e.g., how often do you check/use your device?), (2) cybersecurity awareness and proactive-ness (e.g., how familiar are you with cybersecurity/information security?), and (3) demographics (e.g., age range, gender, family status, and employment status) respectively. The survey used a mixed design involving multiple choice, Likert scale, and open-ended questions. The survey included 29 items (part 1: 5 items, part 2: 16 items, and part 3: 8 items). The first part was measured by a 3-level categorical scale (high: more than I can count, medium: 5-20 times a week, low: less than 5 times a week) and the ratings of the items were averaged. The second part was rated based on a 3-point Likert scale (-1= hardly aware and 1=highly aware) and the scores were averaged. For analysis, we identified a relationship between cybersecurity awareness score (-1 to 1) and user environment (single versus married/partnered or married/partnered with children). To build a framework from this relationship, we positioned these two variables in a 2x2 framework (see Figure 2). The x-axis shows user environment group in which -1 represents single-user environment and 1 represents multi-user environment (e.g., married/partnered or married/partnered with children). The y-axis is the cybersecurity awareness score that showed if user is proactive towards cybersecurity (high score) or passive towards cybersecurity (low score). Although the y-axis is a scale-based variable and x-axis is a categorical variable, we found this framework effective to grasp a quick overview of the population distribution.

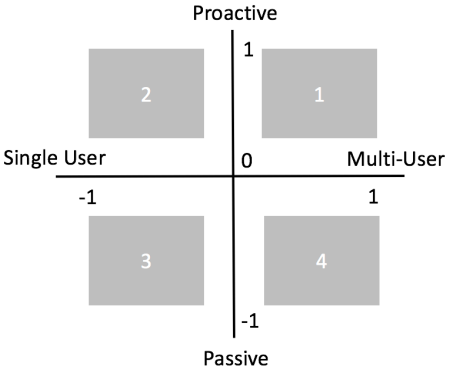

Figure 2. Framework for cybersecurity awareness and user environment

3.2.2 Categorization of survey results

After establishing this framework, we examined if there are population differences among the four quadrants with respect to (1) how individuals perceive cybersecurity issues and (2) who the most vulnerable people would be and their characteristics. We also interrogated the participants who were close to zero in their scores of cybersecurity awareness (i.e., neutral). Table 1 summarizes the survey results organized by the participants in the four quadrants and those who were neutral in cybersecurity awareness. The characteristics of participants in each quadrant are examined and briefed below.

Table 1. Summary of the online survey results of cybersecurity awareness

User groups	N	Awareness	Top age range	Gender		Frequency of digital device use			Cyberattack experience	
		Mean		Male	Female	High	Med	Low	Yes	No
Quadrant 1	37	0.49	19-30 (65%)	51%	49%	51%	35%	14%	24%	76%
Quadrant 2	61	0.44	19-30 (50%)	70%	30%	30%	49%	21%	64%	36%
Quadrant 3	27	-0.32	19-30 (93%)	59%	41%	43%	50%	7%	30%	70%
Quadrant 4	17	-0.29	19-30 (65%)	29%	71%	35%	47%	18%	35%	65%
Neutral awareness	46	0.06	19-30 (83%)	63%	37%	30%	43%	27%	47%	53%
Total	188	0.18	19-30 (68%)	60%	40%	36%	45%	19%	44%	56%

- **Characteristics of participants in quadrant 1: Multi-user, Proactive**
  Participants in quadrant 1 showed the highest frequencies of using digital devices with the highest level of cybersecurity awareness. They also showed the lowest cyberattack experience rate (24%) compared to other quadrants. There were nearly an even number of males and females. The top age range of this group was 19-30 (65%).
- **Characteristics of participants in quadrant 2: Single-user, Proactive**
  Participants in quadrant 2 showed moderate frequencies of using digital devices with the second highest level of cybersecurity awareness with higher male percentage (70%). This quadrant had the highest cyberattack experience rate (64%), and highest number of people (61 participants). The top age range of this group was 19-30 (50%).
- **Characteristics of participants in quadrant 3: Singer-user, Passive**
  In general, participants in quadrant 3 had high device use frequencies (high: 43%, medium: 50%). The cybersecurity awareness score was the lowest among four quadrants (-0.32). There were

slightly higher number of male (59%), and 30% of the participants in this group reported to have cyberattack experience. This quadrant showed the highest proportion of the age group 19-30 (93%).

- **Characteristics of participants in quadrant 4: Multi-user, Passive**
  Participants in quadrant 4 showed moderate frequencies of using digital devices and also had a high female percentage (71%). The number of participants was the lowest among the four quadrants (17 participants). Forty-five percent of the participants had experienced at least one cyberattack. The top age range of this group was 19-30 (65%).

3.2.3 Findings and Discussion

Previous literature on building personas is heavily structured upon interpretation of data from qualitative research methods. Our aim for using the online survey was to follow a data-driven persona building approach (McGinn and Kotamjaju, 2008) to balance the different data sources. The data in the online survey were sufficient to draw the characteristics of user segments in different perspectives.

Lower cybersecurity awareness level in female and multi-user groups. As can be seen from Table 1, the average cybersecurity score of all 188 participants was very low (0.18), while the range of the score was between -.75 and 1 (implying some awareness of cybersecurity issues). Quadrant 1 had the highest cybersecurity awareness level while quadrant 3 had the lowest awareness level. When the participant characteristics were compared by which quadrant they were in, we found a noticeable difference with quadrant 4. For example, while all three quadrants (1,2, and 3) had higher male percentage (which is predictable given the fact that overall male percentage was higher), only quadrant 4 had a higher female percentage (71%). Such results show that a high proportion of females are in the passive and multi-user group.

Inverse proportion between device use frequency and cyberattack experience. Quadrant 1 had the highest device use frequency (51%), yet the lowest cyberattack experience rate (24%). Quadrant 3 had the second highest device use frequency (43%) with the second lowest cyberattack experience rate (30%). Unsurprisingly, quadrant 2 that had the most 'low usage' participants, showed highest cyberattack experience rate (64%). The exact reason behind such pattern is unknown, yet it seems that device use frequency may be in inverse proportion to cyberattack experience.

Managing privacy concerns in product use. More than half of the participants responded that they had experienced cyberattacks before. As part of the survey, participants were asked to answer optional open-ended questions as to how they managed privacy concerns and what sorts of actions they took to protect private information while their personal device was in use. Below are examples of quotes from the survey participants. These answers were not included in the quantitative data analyses since it had significantly low response rate (<5%) and where only optional, but enough to provide insights into user behaviors associated with their data protection.

> *'Shredding documents that sensitive information, multiple types of malware protection, being aware of potential scam emails/websites' — Participant 163, Quadrant 2*
> *'I stored my personal information in the particular folder with protected password. Nobody can see my file. This is one way I follow regularly' — Participant 193, Quadrant 1*

These responses revealed that users have different personal preferences when it comes to securing their private information. Some participants talked about controlling their behavior while using the devices (e.g., only use reputable sites, refuse giving personal information on unauthentic websites), whereas others talked about executing extra steps to secure their information after their input (e.g., protect folders with password, download protective software). As such, managing privacy concerns may differ by not only the type of information, but also by personal characteristics and preferences. In the next section, we address such user differences and similarities by developing personas and user quadrants.

4 DEVELOPMENT OF PERSONAS AND USER QUADRANTS

Three of the co-authors independently coded, categorized and analyzed all data collected from the trend analysis, interviews and online surveys. Qualitative coding was used to extract core insights from the data sets and organize them in relevant clusters (McKenna et al., 2015). The results of the studies were translated into eight different personas that systematically reflect distinct characteristics of users — that fall into different quadrants of the user matrixes.

4.1 Personas

Eight archetypical personas were developed based on the induced data that differ in terms of the number of involved users, the degree of user control, and the degree of cybersecurity awareness. Although previous literature suggests that a cast between three to seven personas are reasonable for conducting a social research, more recent studies are using seven to eight personas depending on the scope of the study (Blomquist and Arvola, 2002; Friess, 2012; Siddall et al., 2011; Johnston et al., 2014). We present four examples of the developed personas (see Table 2) — Innocent Irene, Vigilant Victor, Responsive Rebecca, and Parental Patrick — that fall into different quadrants of the two matrixes in Figure 3.

Table 2. Sample Personas (The full description of the eight personas can be reviewed at http://bravo.berkeley.edu/wp-content/uploads/2018/12/Eight-archetypical-personas.pdf.)

Innocent Irene	Innocent Irene is an example of an 'extreme single-user' in matrix 1 with 'extreme low awareness' in matrix 2. As a single, elderly woman who is currently retired, she is the sole user of her devices, which includes a laptop and a non-smart phone. In terms of using the devices for social purposes, she uses the phone about once a week to communicate with her family and uses the laptop about twice a week for her volunteer work. She does not make much effort to manage her personal information from cyberattacks, other than relying on recommendations from the tech store when she bought her devices. *"I don't really understand technology."*
Vigilant Victor	Vigilant Victor is a persona of the 'transitional' group in matrix 1 and 'extreme digital' group in matrix 2. Victor is a university student who is an incoming software engineer. Victor uses his devices for primarily personal computer science-related work, gaming without the social media component and keeping up with the news, so he is completely the sole user of his devices. He is an example of a transitional user that is very vigilant about which of his information is provided in his devices and applications. *"I provide the minimum amount of information necessary to use the service."*
Responsive Rebecca	Responsive Rebecca is a Conditional Proactive user. She has a medium understanding of cybersecurity since her knowledge of cybersecurity is limited to what she sees on the news or hear from her peers. She is a Conditional Proactive user who varies her cybersecurity prevention actions depending on her perceived risk of the situation or the data being provided, but typically does not take action otherwise. *"I typically don't do anything to prevent cyber hacks unless I hear something on the news about data breaches or if I believe my information is too sensitive to provide."*
Parental Patrick	Parental Patrick is a persona of 'family protective' group in matrix 1 and 'conditional awareness' group in matrix 2. Patrick is a married father of two children who is currently working as a middle school teacher. He is an example of a Family-Protective user since he owns multiple devices in which he shares with his wife and children. His actions to secure his individual devices against cyberattacks depend on his "gut-feeling", unless his children are involved in using the devices. When his children are involved, he does not allow their personal information to be on these devices and is aware of his children's usage of the devices. For example, he does not allow his children to use social media. *"I don't allow my children to use social media… I use my gut feeling to decide what I put online."*

4.2 User quadrants

Iterative data analysis resulted in eight themes, each representing a different user group at large. The eight themes were subsequently mapped onto two types of 2x2 matrixes, which are delineated in Figure 3. The left matrix in Figure 3 is based on the number of people using a device (single versus multi-users) and the degree of user control of personal data (proactive versus passive). The distinction between proactive and passive users represents the likelihood of taking intentional actions to protect their data/privacy and prevent potential cyberattacks. As shown in Matrix 1, three user groups emerged: (1) extreme individual, (2) transitional, and (3) family protective. 'Extreme individuals' portray those who are the sole user of their device(s) and take few, if any, cybersecurity precautions. 'Transitional' users represent those who are typically the sole user of their device and have taken varied actions towards protecting their online privacy and data. 'Family protective' refers to users who have more than one user on their device(s) and have taken varied protective actions. The right matrix in Figure 3 is based on the degree of cybersecurity awareness (high versus low) and the degree of user control of personal data (proactive versus passive).

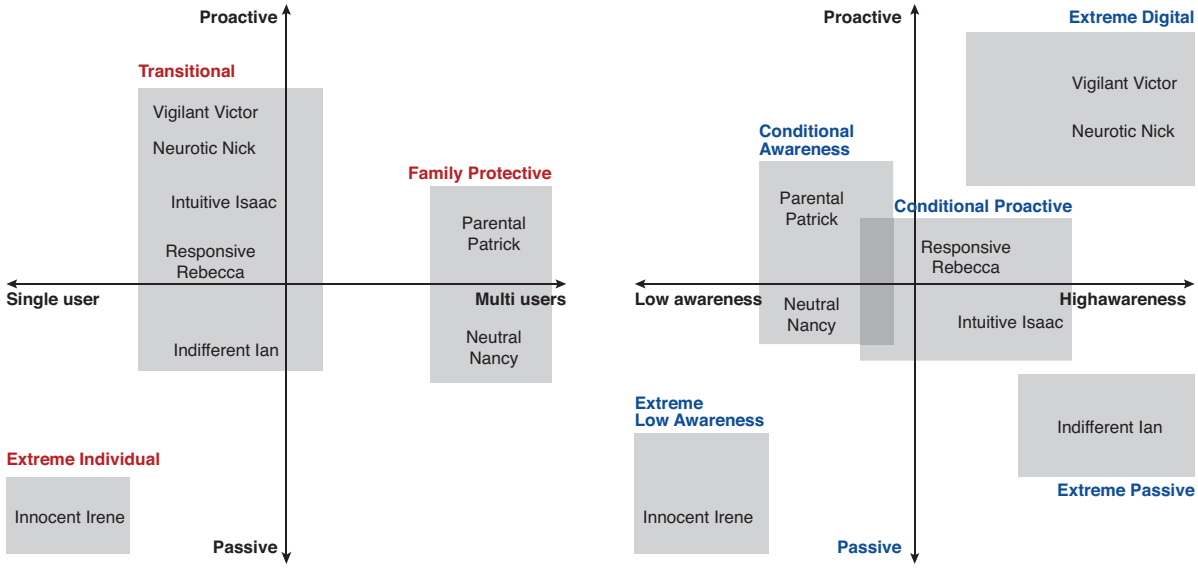

Figure 3. User quadrants: Matrix 1 (the number of involved users and the degree of user control: left) and Matrix 2 (the degree of awareness and the degree of user control: right)

The level of awareness indicates the extent a user has had education or exposure to the field of cybersecurity. Five user groups emerged in this space: (1) extreme digital, (2) extreme passive, (3) conditional proactive, (4) conditional awareness, and (5) extreme low awareness. 'Extreme digital' illustrates those who have high exposure to the cybersecurity area and actively utilize several strategies to protect their online privacy and data from cyberattacks. 'Conditional proactive' portrays those with high (or medium) exposure to the cybersecurity field and take actions depending on their perceived cybersecurity risks. 'Extreme passive' is about those who have high exposure to the cybersecurity field, but hardly take any protective actions. 'Conditional awareness' indicates those with medium (or low) exposure to the cybersecurity field and irregularly take protective actions. 'Extreme low awareness' is a group of those who have minimal exposure to the cybersecurity field and rarely takes protective actions.

5 GENERAL FINDINGS AND DISCUSSION

The main purpose of the present paper is to build a set of personas that represent different types of user's characteristics in the domain of cybersecurity. This is important in that while use of personas in user-centered design is prevalent, the use of the personas to identify the end-users' characteristics in the context of cybersecurity has rarely been addressed. The comparisons of the data sets from the three research methods—a trend analysis, interviews, and online surveys—have allowed us to deepen our understanding of user characteristics; e.g., the cybersecurity awareness levels and behaviors differ between single user and multi users. In line with McCormac et al. (2017), our research results confirm the idea that the level of cybersecurity awareness differs by age groups. By fusing the various types of data sources from interviews, trend analysis to online surveys we were able to extract different insights and pointers to identify user characteristics which made the process and resulting outcomes more methodical (McGinn and kotamraju, 2008). Below, we discuss the emerging themes and findings across three research methods implemented herein and resulting personas.

Single user vs. Multi users. According to both interviews and online surveys, we found that single-users and multi-users showed different patterns in terms of the level of cybersecurity awareness. The single-user group showed a bottom-heavy pattern, indicating a higher population distribution in the low-cybersecurity awareness area whereas multiple-user group (e.g., a family with children) showed a top-heavy pattern, implying that higher proportion of high cybersecurity awareness. The middle 'married' group, but with no children, showed no specific pattern, indicating an evenly distributed population in all cybersecurity awareness score range. The difference between the single- and multi-user groups may be due to the fact that parents are more interested in cybersecurity threats and preventions because their children may be especially vulnerable to cyber threats. Also, parents may have more opportunities to learn about cybersecurity in the process of child education (Bernd et al., 2015), whereas single-users may have to grasp and learn this information by will.

Cybersecurity awareness level by different age groups. Interviews and online surveys showed different cybersecurity awareness levels by different age groups. Among four distinct age groups: 19-30, 31-40, 41-65, and +65, the youngest group (an age range between 19-30) tended to show the highest cybersecurity awareness levels, followed by the 41-65 age group that showed a broad range from high to low depending on the type of occupation. The age group +65 tended to show the lowest cybersecurity awareness. This is unsettling as our society expects and encourages a growing population of elders to be engaged in new digital media such as Skype or other social media services (Pillemer, 2012). Thus, it is important to better understand elders' characteristics and digital device usages and potential vulnerability to cybersecurity breaches.

Research on cybersecurity from a users' perspective is challenging because cybersecurity is a subject that is intangible and is usually not a frequent event. By using a mixed research method approach we were able to extract emerging themes around cybersecurity issues. The proposed personas and user quadrants were results of the highlights and discussion upon the research implementation. We recognize that one limitation to our work is that we only have 20 interviews and most of the participants in both the interviews and online surveys fall under a young age group (19-30). We will involve a broader range of user testbeds in the future research. Another limitation is that while our research team tried to be as comprehensive as possible to select the titles on each axis on the 2x2 segmentations, we recognize this is a subjective process. In the future, we will experiment with a more data-driven segmentation method, i.e. clustering analysis or principal component analysis to generalize our work.

6 CONCLUSION

In this paper, we triangulated three types of research methods: trend analysis, interviews and online surveys to identify different user characteristics inherent to cybersecurity. Then, we compared the data points to examine the accuracy of our research outcomes, based on which personas were formulated. We propose that the developed personas can be used as a baseline of user characteristics in the cybersecurity context for future designers. These personas can help designers foresee how their target user groups would handle potential cybersecurity risks and related factors and envision their design solutions accordingly. In future research, we plan to further improve the personas by incorporating potential data breach scenarios identified in the survey study. The goal is to design more secure digital, mobile devices comprehending a better understanding of user segments through the proposed personas.

REFERENCES

Abawajy, J. (2014), "User preference of cyber security awareness delivery methods". Behaviour & Information Technology, 33(3), pp.237-248. ttps://doi.org/10.1080/0144929x.2012.708787

Adlin, T. and Pruitt, J. (2010), "The essential persona lifecycle: Your guide to building and using personas", Morgan Kaufmann.

Armerding, T. (2018). The 17 biggest data breaches of the 21st century. [online] Available at: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html (accessed date November 25, 2018)

Atzori, L., Iera, A., & Morabito, G. (2010), "The internet of things: A survey. Computer networks", 54(15), 2787-2805.

Bada, M., & Sasse, A. (2014), "Cyber security awareness campaigns: Why do they fail to change behaviour?". Global Cyber Security Capacity Centre.

Bernd, J., Gordo, B., Choi, J., Morgan, B., Henderson, N., Egelman, S., Garcia, D.D. and Friedland, G., (2015). Teaching privacy: Multimedia making a difference. IEEE MultiMedia, (1), pp.12-19.

Blomquist, Å. and Arvola, M. (2002), "Personas in action: ethnography in an interaction design team", In Proceedings of the second Nordic conference on Human-computer interaction (pp. 197-200). ACM.

Bruijn, H. and Janssen, M. (2017), "Building cybersecurity awareness: The need for evidence-based framing strategies", Government Information Quarterly. 34. pp. 1-7. https://doi.org/10.1016/j.giq.2017.02.007

Chang, Y. N., Lim, Y. K., & Stolterman, E. (2008), "Personas: from theory to practices", In Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges (pp. 439-442). ACM.

Cooper A. (1999), "The Inmates are Running the Asylum". In: Arend U., Eberleh E., Pitschke K. (eds) Software-Ergonomie '99. Berichte des German Chapter of the ACM, vol 53. Vieweg+Teubner Verlag, Wiesbaden. https://doi.org/10.1007/978-3-322-99786-9_1

Faily, S. and Flechais, I. (2011), "Persona cases: a technique for grounding personas". In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2267-2270. ACM. https://doi.org/10.1145/1978942.1979274

Friess, E. (2012). Personas and decision making in the design process: an ethnographic case study. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1209-1218).

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). "Internet of Things (IoT): A vision, architectural elements, and future directions". Future generation computer systems, 29(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010
Harknett, R.J. and Stever, J.A. (2011), "The new policy world of cybersecurity". Public Administration Review, 71(3), pp.455-460.
Johnston, J., Rodney, A., & Chong, P. (2014). Making change in the kitchen? A study of celebrity cookbooks, culinary personas, and inequality. Poetics, 47, 1-22.
Kim, E., Jensen, M. B., Poreh, D., & Agogino, A. M. (2018), "Novice designer's lack of awareness to cybersecurity and data vulnerability in new concept development of mobile sensing devices". In DS92: Proceedings of the DESIGN 2018 15th International Design Conference (pp. 2035-2044), Dubrovnik, Croatia. pp. 2035-2044. https://doi.org/10.21278/idc.2018.0461
Kim, E., Kocsik, V.S., Basnage, C.E. and Agogino, A.M. (2013), "Human-centric study of digital-paper transitions: framing design opportunity spaces", International Conference on Engineering Design (ICED13), The Design Society, Seoul, Korea, 19-22.08. 2013.
Marble, J., Lawless, W., Mittu, R., Coyne, J., Abramson, M. and Sibley, C. (2014), "The Human Factor in Cybersecurity: Robust & Intelligent Defense". Cyber Warfare, 56, pp.173-206. https://doi.org/10.1007/978-3-319-14039-1_9
Massanari, A. (2010), “Designing for imaginary friends: information architecture, personas, and the politics of user-centered design”. New Media & Society, 12(3), pp.401-416. https://doi.org/10.1057/palgrave.ivs.9500066
Miaskiewicz, T., & Kozar, K. A. (2011), "Personas and user-centered design: How can personas benefit product design processes?". Design Studies, Vol. 32(5), pp. 417-430. https://doi.org/10.1016/j.destud.2011.03.003
McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M., (2017), Individual differences and information security awareness. Computers in Human Behavior, 69, pp.151-156.
McGinn, J.J. and Kotamraju, N., (2008), "Data-driven persona development". In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1521-1524. ACM. https://doi.org/10.1145/1357054.1357292
McKenna, S., Staheli, D. and Meyer, M. (2015), "Unlocking user-centered design methods for building cyber security visualizations". Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on (pp. 1-8). IEEE. https://doi.org/10.1109/vizsec.2015.7312771
National Institute of Standard and Technology, NICE https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan
Newhouse, W., Keith, S., Scribner, B. and Witte, G. (2017), "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework". NIST Special Publication, 800, p.181.
Newman, L. H. (2018). The Worst Cybersecurity Breaches of 2018 So Far. [online] Available at: https://www.wired.com/story/2018-worst-hacks-so-far/ (accessed date November 25, 2018)
Pillemer, K.A., (2012). 30 lessons for living: tried and true advice from the wisest Americans. Penguin.
Piyare, R. (2013), "Internet of Things: Ubiquitous home control and monitoring system using Android based smart phone". International Journal of Internet of Things. 2(1): 5-11.
Pruitt, J. and Adlin, T. (2010), "The persona lifecycle: keeping people in mind throughout product design". Elsevier.
Rosner, G. and Kenneally, E. (2018), Privacy and the Internet of Things: Emerging frameworks for policy and design, https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf, The Center for Long-term Cybersecurity (CLTC), Berkeley, CA.
Rosner, G. and Kenneally, E. (2017), *Privacy and the Internet of Things*, Center for Long-Term Cybersecurity, Berkeley, CA.
Siddall, E., Baibarac, C., Byrne, A., Byrne, N., Deasy, A., Flood, N., ... & Wang, Y. (2011). Personas as a user-centred design tool for the built environment, Proceedings of the Institution of Civil Engineers-Engineering Sustainability Vol. 164 Iss. 1, March 2011, pp. 59-69 doi:10.1680/ensu.1000015
Singer, P. W., & Friedman, A. (2014), "Cybersecurity: What everyone needs to know". Oxford University Press. https://doi.org/10.5860/choice.188472
Stoll, J., McColgin, D., Gregory, M., Crow, V. and Edwards, W.K. (2008), "Adapting personas for use in security visualization design. In VizSEC 2007 (pp. 39-52). Springer, Berlin, Heidelberg.
Ten, C. W., Liu, C. C., & Manimaran, G. (2008), "Vulnerability Assessment of Cybersecurity for SCADA Systems". IEEE Transactions on Power Systems, 23(4), 1836–1846. https://doi.org/10.1109/tpwrs.2008.2002298
Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 40(4), 853-865. https://doi.org/10.1109/tsmca.2010.2048028

ACKNOWLEDGMENTS

This research was partially supported by a CLTC (Center for Long-term Cybersecurity) grant 2018 at the University of California, Berkeley.