International Journal of Cybersecurity Intelligence & Cybercrime

Volume 3 | Issue 1 Article 4

2-28-2020

A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults

digital divide, cybersecurity, generation Y, generation Z, online security behaviors and beliefs questionnaire (OSBBQ)

Recommended Citation

Debb, S., Schaffer, D., & Colson, D. (2020). A reverse digital divide: Comparing information security behaviors of generation Y and generation Z adults. International Journal of Cybersecurity Intelligence and Cybercrime, 3(1), 42-55. https://www.doi.org/10.52306/03010420GXUV5876

Debb, S. M., Schaffer, D. R., & Colson, D. G. (2020). *International Journal of Cybersecurity Intelligence and Cybercrime, 3* (1), 42-55.

A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults

Scott M. Debb*, Norfolk State University and Virginia Consortium Program in Clinical Psychology, U.S.A

Daniel R. Schaffer, Virginia Consortium Program in Clinical Psychology, U.S.A

Darlene G. Colson, Norfolk State University and Virginia Consortium Program in Clinical Psychology, U.S.A

Keywords; digital divide, cybersecurity, generation Y, generation Z, online security behaviors and beliefs questionnaire (OSBBQ)

Abstract:

Attitudes and behaviors toward cybersecurity best practices vary greatly across groups and generational context might impact how individuals conceptualize their accountability related to digital technology. There may also be age-based vulnerabilities resulting from personal perceptions about the importance of engaging in best-practices. However, age may not be as critical as experience when it comes to implementation of these behaviors. Using the Cybersecurity Behaviors subscale of the Online Security Behaviors and Beliefs Questionnaire (OSBBQ), this study compared the self-reported cybersecurity attitudes and behaviors across college-aged individuals from Generation Y and Generation Z. Data were derived from a convenience sample of predominantly African-American and Caucasian respondents (N=593) recruited from two public universities in Virginia, USA. Four of the eight OSBBQ subscale items demonstrated significant differences between Generation Y and Generation Z adults. Generation Y adults reported greater reviewing of privacy policies on social media, maintenance of antivirus updates, watching for unusual computer performance, and acting on malware alerts, but no significant differences on the other items. It is reasonable to assume that the observed elevated scores were accompanied by greater individual knowledge of information security simply because of being older as a cohort, suggesting that the group was also more experienced and less likely to perceive themselves as invulnerable to online victimization.

Introduction

The shared global cyberspace, encumbered within an increasingly digital world, is available to most people around the world. Although most individuals interact within this shared online cyberspace—likely multiple times per day—there is not necessarily a common standard regarding what is normal behavior online. There is an amazing amount of variability regarding personal attitudes, beliefs, and cybersecurity behaviors related to the protection of personal information and aggressors

*Corresponding author

Scott M. Debb, Ed.D., Department of Psychology, Norfolk State University, Brown Hall: 216, Norfolk, VA 23504, USA.
Email: smdebb@nsu.edu

tend to prey on unassuming individuals who can be more easily (socially) engineered relative to tech-savvier users (Mitnick & Simon, 2002; Parsons, Young, Butavicius, McCormac, Pattinson, & Jerram, 2015; Rezgui & Marks, 2008). That said, no individual or group is exempt from being targeted and victimized in cyberspace.

What happens online in cyberspace has real consequences in the offline world. Cybercrime is an increasingly looming threat not only to individuals, but governments as well, and publicly available information security safeguards and best-practices are disseminated to help protect the global citizenry from misuse, or unauthorized use, of their personal data and identity. This is exemplified by the investment in cybersecurity education and implementation provided by the United States Department of Homeland Security. Specifically, the Cybersecurity & Infrastructure Security Agency (CISA), housed within Homeland Security advises that with the interconnectedness of the world and the inherent advantages this affords, increased connectivity can yield increased risk of various forms of cybercrimes such as theft, fraud, and abuse, and that people who are (increasingly) reliant on digital technology need to be aware that this reliance makes our society as a whole more vulnerable to cyberattacks that take the form of corporate security breaches, spear phishing attempts, and social media fraud (CISA, n.d.). According to the National Cyber Awareness System, governments provide "a variety of information for users with varied technical expertise (and) those with more technical interest can read the Alerts, Analysis Reports, Current Activity, or Bulletins (whereas) users looking for more general-interest pieces can read the Tips" (National Cyber Awareness System, n.d.).

Unfortunately, awareness should not be mistaken for action, and it only represents the starting point for the process safeguarding oneself online. Inevitably, individuals must act with effective and consistent behavior corresponding to established best practices. As an example of where the breakdown between information and implementation often occurs, consider that CISA notes that user authentication is extremely important in the cyber world and that passwords are the most common way people authenticate, yet the effectiveness of passwords for information security is only high when guidance regarding complexity and confidentiality are followed (CISA, 2018). Research consistently demonstrates the ineffectiveness of password use as a cybersecurity safeguard when individuals do not adhere to established guidance for making passwords safe and secure, which is most easily accomplished by increasing complexity and adding multi-layered authentication. When standards are not met, individual (and often employer) efforts at information security become compromised (Jenkins, Grimes, Proudfoot, & Lowry, 2014; Sen, 2018; Zimmermann & Renaud, 2019).

Technological Divide

Given the omnipresence of digital technology embedded in daily life, it is essential to understand if generational gaps—typically expressed as the *digital divide*—continue to impact awareness, perception, and behaviors related to an individual's accountability for cybersecurity. In essence, everyone has a role in safeguarding the shared cyberspace; however, in an increasingly interconnected world, generational context might impact how someone perceives their role and responsibilities. The notion of a *digital divide* refers to the varying degrees of access to and proclivity toward use of technology across defined cohorts, although the phrase once offered reference to the distribution and value of (digital) information technology in society as a whole (Brants & Frissen, 2017). The generation to which an individual is chronologically associated may play a significant role in influencing this connection between knowing a best-practice and actually employing that practice in everyday life as a result of it becoming an internalized value.

Research suggests there is a general decline in what is generally understood as an age-based digital divide, most notably, in more developed nations (Holderness, 2013). Even though people with more experience tend to have more knowledge of security threats and therefore feel more confident in defending against cybersecurity threats (Huang, Rau, & Salvendy, 2010), generational differences may still play a significant role in how people perceive their ability to mitigate potential threats. For example, the notion of a grey divide posits that age-based obstacles might prohibit older adults from taking full advantage of digital avenues for communication and connectivity (Quan-Haase, Williams, Kicevski, Elueze, & Wellman, 2018), and that older adults may be less familiar with nuances of newer digital forms of interaction (Comunello, Ardèvo, Mulargia, & Belotti, 2016). On the other hand, evidence suggests that older individuals are fully capable of engaging in digital activities online (Pratt, 2018). Overall, it is still possible that different generations of technology users are more or less vulnerable to having their data misused due to their personal habits, learned throughout their own lives including the time period when they were first faced with being aware of digital safety needs.

When considering the attitudes and behaviors of digital immigrants relative to digital natives as an example, differences can be seen between individuals whose technology was singularly analog compared to those who were born into a world that was almost exclusively reliant on digital technology (Campos-Castillo, 2015). The divide can therefore be conceptualized as being fueled by many factors, including but not necessarily limited to age and experience. The terms *digital native* and *digital immigrant* were coined by Prensky (2001), referring to *natives* born around 1980 or late (highly associated with being greater and more proficient users of technology) and *immigrants* who are typically older adults not born into today's digitally-engaged world (and therefore assumed to be both less proficient and less frequent users of technology). What differentiates natives and immigrants is also qualitatively different relative to the distinction separating, for example, Baby Boomers (those born in the mid 1940's through the early 1960's) and subsequent generations. That said, those born over the past two decades are not simply natives to the digital world, they are seemingly more reliant upon it being present and operational as a fixed structure embedded within their environment (Colbert, Yee, & George, 2016). However, this does not necessarily assume these individuals have greater competence with regards to minimizing individual vulnerabilities that accompany the increased reliance and usage.

"The digital divide is not simply an issue of access, but also of obstacles to ... use" (Kennedy, Wellman, & Klement, 2003, p. 73). In general, the knowledge of, and behaviors related to, information security for older adults may outrank those of younger adults who are no more than a few years their senior. While this could lead to a perception of decreased vulnerability when operating in online spaces, any differences need not be solely reliant on age. For example unsolicited disclosure online is often motivated by the desire for convenience and a desire to maintain relationships (Krasnova, Spiekermann, Koroleva, & Hildebrand (2010), neither of which is necessarily age dependent.

There is also the say-do gap that exists between the acquisition of knowledge and implementation of a behavioral practice (Daud, Rasiah, George, Asivatham, & Thangiah, 2018; Hoppa, 2018; Noble, Haytko, & Phillips, 2009). Simply having access to important information does not guarantee internalization of the significance of that information, nor the corresponding actions pursuant to those internalizations. It is also possible that experience using digital technology is more essential than chronological age, especially as people mature over the course of their life (Eshet-Alkalai & Chajut, 2009). Attitudes, access, proficiency, and reasons for using any form of digital technology are all critical components when trying to understand the 'say-do' gap (van Deursen & van Dijk, 2014)—referring to the continuum of possible behaviors existing between knowledge and action. As an example, consider that personal information concerning your whereabouts in real-time should be kept private in order

to minimize the chances of being victimized resulting from the various forms of cybercrime aggressors typically engage in, yet many people expose themselves to unnecessary risk by publicly posting their daily activities online for everyone to access.

In terms of cyber-related security practices, there may even be a reverse digital divide impacting the integrity of society's information security infrastructure at a macro level. At face value, it may seem that older individuals who are adapting to newer technologies exert increased stress on the inherent limitations of the typical cybersecurity infrastructure found in home or organizational settings, but age does not always dictate vulnerability. This directly speaks to the human element—where there may be an automatic and biased assumption that as age increases so does risk—but in fact, it may be that "the most intractable aspects are in fact sociotechnical" (Jeong, Mihelcic, Oliver, & Rudolph, 2019, p 2). Developmental issues unique to the individual may be more important regarding what contributes to specific generational groups' engagement (or lack thereof) in essential cybersecurity practices.

Generations X, Y, & Z

Who belongs to which generation is not exact, although there is general agreement of the approximate distinctions. One cause for this is in how the generations are defined across studies (Reisenwitz & Iyer, 2009). Both Generations X and Y are considered to be high adopters of digital technology, most notably the Internet (Lissitsa & Kol, 2016), yet there are subtle differences given what types of digital tools and products were being introduced at specific times throughout the past sixty years. According to Gurau (2012), Generation X—arguably those born between 1961 and 1979—are characterized by technological savviness, and Generation Y—those born between 1980 and 1999 are the Millennials who have the distinction of being the first generation born into a digitally high-tech world (Desy & Wolanskyj, 2017; Norum, 2003). Because each generation is defined by unique collective experiences and values, differences in attitudes and behaviors are often visible despite the often small and seemingly inconsequential differences in year of birth. According to DelCampo, Haggerty, and Knippel (2017), although generational differences have always been present, the increase in life expectancies has resulted in most recent several generations "working side by side" (p. 1).

Consider that emerging adults have used technology in almost all aspects of their lives and from a very early age. This is exemplified by the staggering number of users of the Internet and social media. In one recent study of the general population in the United States, results showed that well over 80% of young adults ages 18-29 actively interacted with at least one social media site, and that nearly 100% of young adults use the Internet (Perrin, 2015).

Generation Z represents the current wave of individuals entering and exploring emerging adulthood. This is a unique period of development between adolescence and mid-late twenties characterized by significant developmental changes that promote movement toward becoming self-sufficient and independent (Arnett, 2000). It is also a time where perceived invulnerability is likely to be greater. Accordingly, these individuals may be less concerned about cybersecurity threats that might result from omission of basic security practices (Lapsley & Hill, 2010). Research has demonstrated that young adults are at greater risk of victimization from cybersecurity attacks (Algarni, Xu, & Chan, 2015; Rezgui & Marks, 2008), possibly resulting from the amount of personal information disclosed online (Fogel & Nehmad, 2009; Litt, 2013).

It seems that for some people, it is not until after being victimized that perceived invulnerability begins to change; however, simply being victimized may not necessarily motivate an individual to engage in more frequent cyber security best-practices (Chen, Beaudoin, & Hong, 2017). Research examining Generation Z in particular has demonstrated this cohort's collective knowledge and understan-

ding regarding the need for cyber security, but with poorer consistency compared to other generations (Kim, 2014). In one study, college students under 20 years of age demonstrated the lowest scores on knowledge of information security awareness when assessed using a self-report questionnaire (Farooq, Isoaho, Virtanen, & Isoaho, 2015).

In addition, distinctions between what constitutes Generation Y versus Generation Z appear to be somewhat arbitrary. Cilliers (2017) defines Generation Y as individuals born between 1980 and 1995, and Generation Z as individuals born from 1996 and on. Jiří (2016) also considers Generation Z as beginning in 1996 but Generation Y as beginning in 1977. Nagy (2017) defined Generation Y as 1977-1994 and Generation Z as 1995-2012. Goh and Lee (2018) defined Generation Y as individuals born 1980-1998 and Generation Z as individuals born 1995 through 2009. Other authors suggest that Generation Y includes individuals born 1977-1994 and Generation Z as individuals born in 1995 and later (Morton, 2002; Noble et al., 2009). For the purposes of this study, Generation Y was defined as individuals born 1977-1994, and Generation Z was defined as individuals born 1995 and later.

Rapid growth and changes in technology are also impacting social attitudes toward cybersecurity as a general facet of an increasingly global society (Colwill, 2009). Research suggests that an individual's perception of information security significantly impact behaviors and decision-making (Huang, Rau, Salvendy, Gao, & Zhou, 2011). Despite this, the human component inherent to all cyber security still suffers from gaps between an individual's intent and their actual behavior (Shropshire, Warkentin, & Sharma, 2015). One possible explanation for this 'say-do' gap is the presence of the hypothetical bias, which is defined as an overestimation of willingness (intent) or an inaccurate estimation of positive (behavioral) outcomes when examining a given behavior (Ajzen, Brown, & Carvajal, 2004). Notwithstanding, there is evidence to suggest that knowledge of information security policies and procedures predict positive attitudes towards these policies, and further, that information security knowledge and attitudes are positively related to self-reported behavior (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).

In a study investigating perceptions of information security towards security threats such as viruses, spam, and password attacks, researchers have demonstrated that a person's knowledge of threats to information security, the impact of the threat (e.g., the duration and scope), perceived severity of the threat (e.g., degree of harm and consequences), and past exposure to threats relate to participants' perceptions of the overall danger associated with specific threats (Huang, et al., 2010). Interestingly, perceptions of information security threats were dependent upon the types of losses associated with those threats, and people seemed to be more concerned by a threat if it was likely to result in potential financial loss or personal inconvenience. This suggests that people might be more motivated to engage in specific practices only in circumstances where they perceive the threat as directly related to some aspect of their personal or professional well-being, rather than a more overarching urgency pervading daily life.

Purpose of Study

Although young adults may be known for their tech savviness (as evidenced by their ability to navigate the Internet and engage on social media), there is a potential area of weakness regarding perceived information security awareness and corresponding behaviors that differ based on generational cohort. It seems reasonable to assume significant differences would exist between the attitudes and behaviors of older generations (Baby Boomers and Generation X compared to Generation Z for example); however, there is less understanding about the differences that might exist between the two most recent digitally native generations. As such, the current study sought to compare the information

security attitudes and behaviors of Generation Y Millennials born between 1977 and 1995 and Generation Z adults born after 1995 to help examine potential differences in information security awareness and practices. Having a better understanding of these relationships can provide insight into the online behaviors of digitally native emerging adults.

Methods

Sample

Data were obtained from students recruited from two public universities—one a large and culturally diverse research oriented school and the other a smaller Historically Black university—in a semi-urban area of southern Virginia. Collecting data as part of convenience sampling was approved by the Institutional Review Boards at both institutions. Participants at the larger school were recruited through the university's research pool database for psychology students, and participants at the smaller school were granted access to the survey via a secure hyperlink provided via email announcements. All participants provided informed consent prior to accessing the surveys. Participants had to be born between 1977 and 1999, ensuring they were from Generation Y or Z and at least 18 years old.

Data from 688 respondents were collected during the 2017-2018 academic school year. Of these, 67 respondents were removed prior to further analyses for not reporting their year of birth. Further, 28 respondents were removed for not answering items other than the demographics questionnaire. The resulting sample for this study was 593 respondents, with an average age of 22.06 years (SD = 4.80). When examined by generation, the average age of Generation Y individuals was 27.48 years (SD = 5.02, median = 25.50) and 19.52 years for Generation Z (SD = 1.33, median = 19.00).

Measures

Demographic information.. A demographics questionnaire created for this study asked participants to self-report their age, gender, race, and ethnicity. The majority of the sample were African American or Caucasian female undergraduate students, approximately 65% of whom were born between 1995 and 1999. These data are itemized in Table 1.

Table 1. ***Sample Demographics and Descriptive Statistics***

	N	%
Generational Classification		
Generation Y (1977-1994)	209	35.20%
Generation Z (1995-1999)	384	64.80%
University Affiliation		
Larger Research Institution	493	83.10%
Liberal Arts HBCU	100	16.90%
Gender		
Male	119	20.10%
Female	472	79.60%
Other	2	0.30%
Race		
African American	250	42.20%
Alaskan Native	1	0.20%
American Indian / Native American	3	0.50%
Asian / Asian American	24	4.00%

Continued on next page

Table 1. Continued from previous page

	N	%
Caucasian / White	229	38.60%
Latino/a	42	7.1%
Hawaiian Native / Pacific Islander	5	0.80%
Multiracial	39	6.60%
Ethnicity		
Hispanic	59	9.90%
Non-Hispanic	521	87.90%
[Unreported]	13	2.20%
Current Academic Status		
Freshman	130	21.90%
Sophomore	107	18.00%
Junior	141	23.80%
Senior	202	34.10%
Graduate Student	13	2.20%

Information Security Behaviors.. The current study utilized a portion of the items from the Online Security Behaviors and Beliefs Questionnaire (OSBBQ), which is a Likert-scaled questionnaire consisting of 75 items assessing perceptions of information security awareness and associated self-reported behaviors (Anwar, He, Ash, Yuan, Li, & Xu, 2017; Li, He, Ash, Xu, Anwar, & Yuan, 2014; Li et al., 2019). Initially developed for use within a corporate employee population, items ask respondents to rate their degree of comfort with specific information and cybersecurity-related tasks and to evaluate their computer and Internet abilities. For the purpose of this study, only the subscale assessing self-reported cybersecurity behaviors were included (see Table 2), as other items regarding computing skills and proficiency are more directly related to vocational environments and were therefore not relevant to the research question of this study.

Table 2. ***Cyber Security Behavior Items of the OSBBQ***

1	I use different passwords for my different social media accounts (e.g., Facebook, Twitter, LinkedIn).
2	I usually review privacy/security settings on my social media sites (e.g., Facebook, Twitter, LinkedIn).
3	I keep the anti-virus software on my computer up-to-date.
4	I watch for unusual computer behaviors/responses (e.g., computer slowing down or freezing up, pop-up windows, etc.).
5	I do not open email attachments from people whom I do not know.
6	I have never sent sensitive information (such as account numbers, passwords, and social security number) via email or using social media.
7	I back up important files on my computer.
8	I always act on any malware alerts that I receive.
9	I don't click on short URLs posted on social media sites unless I know where the links will really take me.

Results

The data were first assessed for missingness in response patterns. A missing values analysis was performed using SPSS (version 25) on each of the nine cyber security behavior items on the OSBBQ. All items demonstrated less than 1% missingness with the exception of item 5 ("I do not open email attachments from people whom I do not know"), which demonstrated 16% missingness. The missingness response pattern on item 5 was found to be significantly correlated with response patterns on two other items (item 3, $p = .029$; and item 8, $p = .007$). As a result, item 5 was removed from further analyses.

Response data for the remaining eight items were assessed for normality of response distribution. All items fell within the acceptable range for both skewness and kurtosis (< |1.96|; Sheskin, 2011). A series of independent samples t-tests were performed to assess for response differences in each item between Generation Y and Generation Z adult participants. Of note, the distribution of Generation Y and Generation Z adults in this sample lead to an oversampling of Generation Z adults. As a result, the sample in these analyses could not claim relative equality in group sample sizes (Generation Y = 35.20% of sample; Generation Z adults = 64.80% of sample). Levine's Test of Equality of Variances was non-significant for all comparisons, indicating satisfactory levels of homogeneity in between-group variances. All other assumptions of independent samples *t*-tests were met. Results of the analysis are provided in Table 3.

Table 3. ***Independent Samples t-Test Results***

				95% CI	
Item #	*t*	*df*	*MD*	Lower Bound	Upper Bound
1	1.70	591	-0.26	-0.57	0.04
2	2.53 *	591	-0.38	-0.67	-0.09
3	4.37 ***	591	-0.59	-0.86	-0.33
4	3.73 ***	591	-0.40	-0.61	-0.19
5	--	--	--	--	--
6	-0.12	591	0.02	-0.25	0.28
7	0.61	591	-0.08	-0.33	0.17
8	2.95 **	591	-0.41	-0.68	-0.14
9	1.73	591	-0.25	-0.52	0.03

* $p < .05$ ** $p < .01$ *** $p < .001$

Four of the eight subscale items demonstrated significant differences between Generation Y and Generation Z adults: item 2 (*reviewing privacy/security policies on social media accounts*), item 3 (*maintaining anti-virus software updates*), item 4 (*watching for unusual computer behaviors/responses*), and item 8 (*acting on malware alerts*). Generation Y participants endorsed greater cyber security practices compared to Generation Z adults specifically for these four items (see Table 4). Statistical significance was observed for items 3 and 4 at the $p < .001$ level, item 8 at the $p < .01$ level, and item 2 at the $p < .05$ level.

Table 4. ***Generation Y and Z Adults, OSBBQ Cybersecurity Behaviors Subscale Response Averages***

Item #	Generation Y Response Mean	Generation Z Adults Response Mean
1	4.95	4.68
2*	4.86	4.48
3***	5.36	4.77
4***	5.81	5.41
6	5.48	5.49
7	5.22	5.14
8**	4.94	4.53
9	4.99	4.74

* significant *t*-test difference, $p < .05$
** significant *t*-test difference, $p < .01$
*** significant *t*-test difference, $p < .001$

Discussion

This study considered the potential role of generational cohort as an influencer of information security attitudes and self-reported practices of college student adults from Generation Y and Generation Z—individuals born between 1977 and 1999. Results showed that the younger, Generation Z adults from this sample demonstrated less endorsement of widely known cybersecurity best practices. This was observed in items specifically focused on reviewing privacy policies (item 2), noticing unusual computer performance (item 4), and having an awareness of antivirus and malware automatic notifications (items 3 and 8). Data suggest that Generation Y individuals from this self-report sample being engaged in safer information security practices compared to their Generation Z counterparts. It is reasonable to assume that the safer practices the older group self-reported is accompanied by greater knowledge of information security simply because of the additional years of being engaged in a digital-technology world. Specifically, it was hypothesized that Generation Y would rank higher than Generation Z adults on the OSBBQ Cybersecurity Awareness subscale, and significant differences were observed for half of the items included in the analysis.

In 2015, then President of the United States Obama compared the current state of the collective cyberspace to the *Wild West*, implying that it needed a sheriff to consistently safeguard this publicly shared space (NPR, 2015). Given that Generation Z adults were barely adolescents at that time, it is understandable that Generation Y adults may comparatively seem to be more hypervigilant to potential risks. As a general perception of how the two cohorts may perceive their online presence, Generation Y adults may be less likely to perceive themselves as invulnerable in this 'wild west', yet the pervasiveness of digital technology in our society appears to be increasing digital literacy, ultimately leading towards the thinning of the generationally-based digital divide.

From a developmental perspective, it is possible that the normal adaptations that occur throughout one's life impacted how individuals in this study perceived the literal meaning of the items. This could be due to cultural differences inherent to their generational cohort and the individual experiences that occur over time with age. For example, people tend to lose their sense of invulnerability as they age (Denscombe & Drucquer, 1999) and generation Y adults grew up in a world where adapting to privacy and cybersecurity threats were first becoming more commonplace. These individuals are now at an age where the realities of (online) risk have become part of their conscious awareness as it relates to their lack of invulnerability.

We can assume that "digital immigrants... have progressed rapidly in moving into the digital world – adapting to and relying more on technology for work and personal use," (Autry & Berge, 2011, p. 461), potentially making them more vigilant as a generational cohort. Participants report of what was internally motivated them to be vigilant and behave in accordance with best-practices could have been negatively impacted. Research suggests that people who have not been personally affected by a significant cybersecurity breach tend to not have the urgency that motivates people to engage in best-practices consistently (Dodel & Mesch, 2017). In essence, when external motivators to behave are minimal, there is a stronger possibility of succumbing to the say-do gap. It is possible that individuals from this sample may become more motivated if they had been severely victimized at some point in their lives; however, this data was not collected. Data from this study did suggest that these participants were motivated by some, but not all, cybersecurity-related factors (as identified by the OSBBQ).

Despite this, the digital divide continues to close as a result of the omnipresence of technology across our globally connected society. Future generations are likely to experience an entirely different cyberspace with different types of threats that cannot necessarily be quantified by traditional

self-report instrumentation pertaining to isolated events such as opening email attachments and reviewing social media policies. The future digital divide may actually reflect how each of us perceive our interconnected accountability for the portions of cyberspace we dynamically occupy from a sociodemographic perspective, rather than generational.

Limitations & Future Directions

Although this study provides useful insights about the presence of and nature surrounding generational differences in cyber security attitudes and behaviors, it is not without its limitations. First, this was a cross-sectional study that did not allow for the examination of change in perceptions over time. Second, all data were derived from participant self-report and therefore do not speak to possible differences between Generation Y and Generation Z's intended behaviors and their actual behaviors. Third, while the sample was ethnically diverse, it primarily consisted of African American and Caucasian female undergraduate students from a convenience sample, which was expected given the student populations at both schools. Accordingly, inferences between results from this sample and hypothesized results from other populations cannot be taken for granted. Future studies should aim to bridge the gap on information and online security attitudes and behaviors between corporate environment employees and other cohorts, specifically emerging adults. As such, the range of ages included could be increased in future studies in order to make more meaningful comparisons between the generations.

Conclusion

This study examined the cybersecurity attitudes and self-reported behaviors of Generation Y and Generation Z adults. Data suggest that there was a statistically significant difference between how these two groups of adults were conceptualizing specific components of cybersecurity—most notably the direct feedback from their computer's software. As the sociotechnological divide overtakes any remaining digital divide, researchers should continue to assess the interrelationships between human performance and the ever-increasing automation embedded within society in order to better understand and subsequently mitigate the negative effects of the knowledge (say) – performance (do) gap.

Acknowledgments

The authors would like to acknowledge the Cybersecurity Research Complex and Center of Excellence in Cybersecurity at Norfolk State University for supporting this research.

Declaration of Interest Statement

The authors declare that they have no conflicts of interest.

References

Ajzen, I., Brown, T., & Carvajal, F. (2004). Explaining the discrepancy between intentions and actions: the case of hypothetical bias in contingent valuation. *Personality & Social Psychology Bulletin, 30*, 1108-1121.

Algarni, A., Xu, Y., & Chan, T. (2015, December). Susceptibility to social engineering in social networking sites: The case of Facebook. In 36th International Conference on Information Systems (ICIS 2015), Fort Worth: Texas. Retrieved from http://eprints.qut.edu.au/89392/

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443.

Arnett, J.J. (2000). Emerging adulthood: A theory of development from the late teens through the twenties. *American Psychologist, 55*, 469-480.

Autry Jr, A.J., & Berge, Z. (2011). Digital natives and digital immigrants: Getting to know each other. *Industrial & Commercial Training, 43*(7), 460-466.

Brants, K., & Frissen, V. (2017). Inclusion and exclusion in the information society. In R. Silverstone. (Ed.). *Media, technology, and everyday life in Europe* (pp. 39-50). Routledge.

Campos-Castillo, C. (2015). Revisiting the first-level digital divide in the United States: Gender and race/ethnicity patterns, 2007–2012. *Social Science Computer Review, 33*(4) 423-439.

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.

Cilliers, E.J. (2017). The challenge of teaching Generation Z. *PEOPLE: International Journal of Social Sciences, 3*, 188-198.

CISA: Cyber Infrastructure Security Agency (n.d.). Combating cyber crime. Retrieved from https://www.dhs.gov/cisa/combating-cyber-crime\#

CISA: Cyber Infrastructure Security Agency (2018). Creating and managing strong passwords. Retrieved from https://www.us-cert.gov/ncas/current-activity/2018/03/27/Creating-and-Managing-Strong-Passwords

Colbert, A., Yee, N., & George, G. (2016). The digital workforce and the workplace of the future. *The Academy of Management Journal, 59*, 731-739.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? *Information Security Technical Report, 14*, 186-196.

Comunello, F., Ardèvo, M., Mulgaria, S., & Belotti, F. (2016). Women, youth and everything else. *Media, Culture & Society, 39*(6), 798-815.

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations? *International Journal of Business & Society, 19*(1), 161-180.

DelCampo, R.G., Haggerty, L.A., & Knippel, L.A. (2017). *Managing the multi-generational workforce: From the GI generation to the millennials*. New York, NY: Routledge.

Denscombe, M., & Drucquer, N. (1999). Critical incidents and invulnerability to risk: Young people's experience of serious health-related incidents and their willingness to take health risks. *Health, Risk & Society, 1*(2), 195-207.

Desy, J.R., & Wolanskyj, A.P. (2017). Milestones and millennials: A perfect pairing—competency-based medical education and the learning preferences of Generation Y. *Mayo Clinic Proceedings, 92*(2), 243-250.

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human behavior, 68*, 359-367.

Eshet-Alkalai, Y., & Chajut, E. (2009). Changes over time in digital literacy. *CyberPsychology & Behavior, 12*(6), 713-715.

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015, August). Information security awareness in Educational Institution: An analysis of students' individual factors. *Trustcom/BigDataSE/ISPA, 2015 IEEE*, 352-359.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*, 153-160.

Goh, E. & Lee, C. (2018). A workforce to be reckoned with: The emerging pivotal Generation Z hospitality workforce. *International Journal of Hospitality Management, 73*, 20-28.

Gurau, C. (2012). A life-stage analysis of consumer loyalty profile: Comparing Generation X and Millennial consumers. *Journal of Consumer Marketing, 29*(2), 103–113.

Holderness, B. (2013). Toward bridging digital divides in rural (South) Africa. In D. Buckinghma & R. Willett (Eds.), *Digital generations: Children, young people, and new media* (pp. 251-272). New York, NY: Routledge.

Hoppa, M. A. (2018). Automating ethical advice for cybersecurity decision-making. *Proceedings of the International Conference on Information and Knowledge Engineering (IKE)*, 170-171.

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security.*Behaviour & Information Technology, 29*, 221-232.

Huang, D. L., Rau, P. L. P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies, 69*, 870-883.

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development, 20*(2), 196-213.

Jeong, J.J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards and improved understanding of human factors in cybersecurity (No. 2032). EasyChair. Retrieved from https://yahootechpulse.easychair.org/publications/preprint_download/XRKm

Jiří, B. (2016). The employees of Baby Boomers generation, Generation X, Generation Y, and Generation Z in seleceted Czech corporations as conceivers of development and competitiveness in their corporation. *Journal of Competitiveness, 8*(4), 105-123.

Kennedy, T., Wellman, B., & Klement, K. (2003). Gendering the digital divide. *IT & Society, 1*(5), 72-96.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security, 22*, 115-126.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*(2), 109-125.

Lapsley, D. K., & Hill, P. L. (2010). Subjective invulnerability, optimism bias and adjustment in emerging adulthood. *Journal of Youth & Adolescence, 39*, 847–857.

Li, L., He, W., Ash, I., Xu, L., Anwar, M., & Yuan, X. (2014). Does explicit information security policy affect employees' cyber security behavior? A pilot study. *Second International Conference on Enterprise Systems 2014*, 169-173.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-19.

Lissitsa, S., & Kol, O. (2016). Generation X vs. Generation Y–A decade of online shopping. *Journal of Retailing & Consumer Services, 31*, 304-312.

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior, 29*, 1649-1656.

Meredith, S. (2018, April 10). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. Retrieved from https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Hoboken, NJ: John Wiley & Sons.

Morton, LP. (2002). Targeting Generation Y. Public Relations Quarterly, 47(2), 46-48.

Nagy, S. (2017). The impact of country of origin in mobile phone choice of Generation Y and Z. *Journal of Management & Training for Industries, 4*(2), 17-29.

National Cyber Awareness System (n.d.). Alerts and tips. Retrieved from https://www.us-cert.gov/ncas

Noble, SM., Haytko, DL., & Phillips, J. (2009). What drives college-age Generation Y consumers? *Journal of Business Research, 62*, 617-628.

Norum, P.S., 2003. Examination of generational differences in household apparel expenditures. *Family Consumer Science Research Journal, 32*(1), 52–75.

NPR (2015, February 13). Obama: Cyberspace is the new 'Wild West'. Retrieved from https://www.npr.org/sections/thetwo-way/2015/02/13/385960693/obama-to-urge-companies-to-share-data-on-cyber-threats

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering & Decision Making, 9*, 117-129.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176.

Perrin, A. (2015). Social networking usage: 2005-2015. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2015/10/08/2015/Social-Networking-Usage-2005-2015/

Prensky, M. (2001). Digital natives, digital immigrants. *On The Horizon, 9*(5), 1-6.

Pratt, T. C. (2018). The myth of the tech-savvy teen and the clueless senior citizen: Revisiting technology-based victimization over the life course. *Criminal Justice Review, 43*(3), 360-369.

Quan-Haase, A., Williams, C., Kicevski, M., Elueze, I., & Wellman, B. (2018). Dividing the grey divide: Deconstructing myths about older adults' online activities, skills, and attitudes. *American Behavioral Scientist, 62*(9), 1207-1228.

Reisenwitz, T. H., & Iyer, R. (2009). Differences in Generation X and Generation Y: Implications for The organization and marketers. *Marketing Management Journal, 19*(2), 91-103.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*, 241-253.

Sen, R. (2018). Challenges to cybersecurity: Current state of affairs. *Communications of the Association for Information Systems, 43*(1), 22-44.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security, 49*, 177-191.

Sheskin DJ. (2011). *Handbook of Parametric and Nonparametric Statistical Procedures* (5th ed.). Boca Raton, FL: Chapman and Hall CRC.

van Deursen, A. J., & van Dijk, J. A. (2014). The digital divide shifts to differences in usage. *New Media & Society, 16*(3), 507-526.

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies, 131*, 169-187.