2018

Gender and Cybersecurity: Consumer Awareness, Experience and Trust

M. Olguta Vilceanu
Rowan University

Kristine Johnson
Rowan University

Gender and Cybersecurity: Consumer Awareness, Experience and Trust

M. Olguta Vilceanu, Ph.D.
Kristine Johnson, Ph.D.
Rowan University

ABSTRACT

In light of the growing epidemic of cyberattacks, it is important to understand how different groups within the general population connect information with attitudes and behaviors. Internet transactions become less of an option and more of a requirement for consumers and the workforce. This study explored the connection between awareness, experience, and trust with the goal of identifying communication strategies that will ultimately steer consumers toward healthy cyberbehaviors. Consumer trust in government and business organizations is the desired status quo for everyone. Awareness and experience are important modifying factors and both are addressable through strategic consumer communication campaigns. Understanding the different ways men and women think, feel, and act around key issues in cybersecurity is key to organizational success. Furthermore, investing in promotion of educated trust can help organizations avoid massive loyalty shifts if or when the next data breach occurs.

INTRODUCTION

Each year brings another crop of major cybersecurity crises and incidents that affect millions of individual and organization, and perhaps much of the crisis can be attributed to lack of awareness, education, and experience that would help bridge cybersecurity and everyday life. The topics of cybersecurity and cybertheft are particularly relevant today, as society moves toward all-electronic information transactions. Data and communication technologies simplify our daily life (work, shopping, entertainment) even as they create the possibility for massive amounts of personally identifiable information about our health and financial records, tax information, and Internet usage to be accessed for nefarious reasons.

The average cost of a data breach ranges within a couple of millions of dollars (IBM-Ponemon Institute, 2017[1]), not including substantial share valuation decreases due to shareholders offloading victimized companies from their investment portfolio (Shields, 2015). Where a cyberattack with potentially compromised data is called an incident, a data breach represents confirmed data loss. In a confirmed data breach perpetrators captured entire databases full of highly sensitive personal information (social security numbers, credit card accounts, loans and

[1] http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

income statements, health records, etc.) associated with consumer accounts. In 2016 alone, there were over 1,500 data breaches reported by private and public organizations around the world (Verizon DBIR 2016).

Within the general population, anyone can enable hackers to implement systemic attacks if consumer behavior is driven by insufficient awareness and experience with cybersafety. Unnecessarily high or unreasonably low levels of consumer trust in the organizations who manage personally identifiable information--even those they work for--translate in decision-making and behaviors with a direct impact on the organizational effectiveness. A recent survey from the Pew Research Center found that 64% of the American adults have "personally experienced a major data breach" (Olmstead & Smith, 2017). Given the magnitude of the situation, it is worth looking into the possible characteristics shared by the affected population.

This study conceptualizes cybersecurity awareness, experience, and involvement from the perspective of consumer gender, attitudes, and behaviors. There is an abundance of reports confirming severe underrepresentation of women in science, technology, engineering and math (STEM) programs of study at all levels. Furthermore, this gender discrepancy continues into the information technology (IT) workfield, where women constitute less than 11% of the cybersecurity workforce (Kaspersky Lab, 2017; ISC, 2017) and a very small percentage of them hold managerial or executive positions. However, there is almost no research focused on gender and cybersecurity within the field of consumer behavior. Without extensive training, mentors and role models for women, it stands to reason that women may process and engage with cybersecurity incidents differently than men. If that is true, organizational communication management must address such facts in order to elicit the right type of consumer involvement and behaviors--both inside and outside organizations.

LITERATURE REVIEW

Cybersecurity, gender, and the workforce. Most cyberattacks have an enterprise rather than individual character (see Verizon DBIR 2016[2] and DBD 2017[3]), meaning that multiple publics inside and outside the organization impact the likelihood of success with each criminal attempt. Cybersecurity incident mitigation efforts should therefore also target the general population--only a small part of which comprises the active cybersecurity management and immediate response teams. Where the IT industry promotes organizational effectiveness, cybersecurity is substantially more specific, due to its focus on stopping security breaches and attacks. In cybersecurity, the ratio between time invested in prevention versus combat makes it, ironically, most vulnerable for budget cuts when organizations face difficult times (Bagchi-Sen et al., 2010). Given the continuous growth in the technological sciences coupled with the significant rise in number of corporate hacks (Equifax, Uber, Target, etc.), it is no surprise the demand for cybersecurity professionals has grown immensely (Mims, 2017; O'Neill, 2016).

[2] http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
[3] http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/

The need for broader communication strategies is emphasized by recent research reporting an acute shortage of qualified personnel to handle cybersecurity, a field where data exfiltration (unauthorized access or unintentional vulnerabilities) is the top concern for North American organizations (ISC, 2017). In addition, about one-third of the managers come from previous non-technical careers (p. 5) and they all need to staff their teams with growing numbers of highly skilled technical workers who tend to be relatively young, very well compensated, and highly mobile by choice (p. 6). The culture of male-dominated IT fields does little to encourage women to pursue an education in information technology when they are teenagers (Armstrong, 2007) or retain them once work-family balance becomes an issue (Trauth et al., 2004). In everyday life, outside of their immediate work environment, cybersecurity professionals may serve as role models and share their knowledge and opinions with friends and family, thus helping to propagate awareness of cybersecurity issues and healthy behaviors. On the other hand, an insufficient number of successful women role models and mentors in cybersecurity prevents younger women from even being interested in pursuing degrees and careers in cybersecurity (Bagchi-Sen et al., 2010).

When compared to their males counterparts, women in the sciences are twice as likely to leave a technology job (Mercer, 2017). Mistreatment in the workplace including unwanted behavior and unwanted sexual attention is also a contributor (Scott et al., 2017). Does this generalized gender imbalance in the professional field translate into substantial differences between the way men and women in general experience and understand cybersecurity? If such differences exist, they may translate into (or perhaps explain) long-term challenges in cybersecurity marketing and communication.

Awareness, experience, and trust. Arguably the most important function of *issue* communication (Seeger, 2006) is activating key audiences from lack of awareness to latent awareness and finally to operational status (Grunig, 2005). For the purposes of this study, awareness is conceptualized as individuals having heard of recent major cyberattacks. Experience with cybertheft is derived from consumers having noticed, or having received notice, that their consumer accounts were compromised in a cyberattack. Trust is conveyed via consumer confidence in the ability and preparedness of business or government organizations to (1) handle consumer information responsibly and safely; and (2) withstand a major cyberattack in the near future.

While cybersecurity departments are difficult to staff and fund, cybersecurity communication challenges marketing and communication efforts because the stakes are high, the topic is complex, and the size and frequency of cybersecurity incidents has exploded in the last decade. Every organization and every individual consumer are potentially vulnerable to cybersecurity failure. So, if we are all at risk, does anything we think, feel, or do really matter? Informed trust and judicious use of organizational resources could address this key factor in the relationship consumers have with government and business entities. Fatalism may translate in reckless behaviors, as was previously seen in medical bias among professionals, legislators, patients, and the general public in major medical epidemics such as AIDS, malaria, typhoid fever, and so on

(Stuber et al., 2008; Thiede, 2005). Cybertheft is not a medical issue, though it certainly qualifies as a social and financial epidemic (MacIntyre et al., 2017), due to its growing scope and scale.

A previous Pew Research Center survey on consumer awareness and understanding of data breach incidents had revealed that consumers rely on and have clear expectations that companies would safeguard personally identifiable information and use it appropriately, even as they are increasingly worried about the ease with which such information can be accessed. More importantly, fewer than 40% of the Americans would be confident in the ability of credit card companies to keep personal data "private and secure"—an attitude strongly and negatively influenced by the respondents' prior exposure to information about publicly reported government surveillance and data breach incidents (Rainie and Duggan, 2016). Would a similar effect be noticed in the broader context of not just data breaches, but cybersecurity in general? It is important to mention here that each of the cyberattack examples used in the Pew Cybersecurity survey was representative for at least one major cyberattack incident on several major companies within the same industry segment, within the last five years.

Trust and (mis)representation of cybersecurity issues. Individuals, companies, and news media struggle with the concept of trusting a variety of entities and networks (Constante et al., 2015). In the meantime, issues of cybertrust, internet policy and governance, as well as information stewardship for the common good, are competing forces in a tenuous yet unavoidable relationship with individual and organizational needs for autonomy, profit, and growth (Dutton et al., 2005). To compound issue complexity, many people are influenced by the 'misuser' mythology, where hackers and crackers are seen as valiant heroes aiming to overthrow material practices imposed by greedy governments and multinational corporations (Söderberg, 2010).

Cybersecurity communication depends on consumers' ability and willingness to trust in the ability of numerous organizations to safeguard the vast amounts of highly sensitive, personally identifiable information (PII). On the other hand, the criminal justice policy system is not entirely ready to define and address the concept of identity and information theft, which leads to difficulty in tracking the identity and strategies of cyberthieves (Morris, 2010). Victimized companies may have valid reasons to want to delay public disclosure of their status as injured parties for as long as possible, in order to avoid becoming vulnerable to more data theft while they are still working to address the problems raised by the most recent incident (Jenkins et al., 2014). Conversely, some individuals report their status as injured parties, either in anticipation of compensation packages to follow if and when companies settle the class action suits that follow each major cybertheft or data breach disclosure, or in attempts to support social media activism around cybersecurity issues.

Where consumers are facing issues that deeply impact their lives, trust and activism connect strongly with feelings of empowerment vs. fatalism (Radin, 2005). It could be argued that cybertheft can be likened to cancerous tumors, because they can take over the individual's life, starting a period of intense, costly, and painful procedures that may or may not remove the problem successfully. The complexity of cybersecurity incidents is further augmented by the

multiple layers of victims: those whose money or identity were stolen; those who may have been impersonated during the fraud and now have to prove their innocence; and the general public who bears the redistributed cost of incident recovery through fees, copays, and so on (Verizon, 2017)

Demographic parameters in cybersecurity marketing communication. The Pew Research Center conducted a cybersecurity survey in Spring 2016. At that time, several major data breaches had recently been broadly discussed by media and audiences not only in the United States, but around the world. At first glance, this study indicated that 64% of the Americans "have personally experienced a major data breach" and "roughly half of Americans do not trust the federal government or social media sites to protect their data" (Olmstead & Smith, 2017, pp. 2-3). Furthermore, "a substantial majority of Americans anticipate major cyberattacks in the next five years on our nation's public infrastructure, or banking and financial systems" (p. 6). Given the overwhelmingly negative tone of report findings, deeper questions need to be asked along key demographic variables such as gender, age, and education level; and behavioral variables such as type and frequency of cyberactivity.

RESEARCH QUESTIONS

From a corporate communication and consumer behavior perspective, it is essential to determine if the severe underrepresentation of women within the Information Technology and cybersecurity industries is reflected in substantial gender-based differences in attitudes, opinions, and behaviors. There is a noticeable absence of literature exploring connections between cybersecurity marketing communication and general audience demographics.

To effect a positive change in the way consumers trust, perceive, and behave regarding cybersecurity, we must first acknowledge the possibility of major differences in the way men and women think, feel, and act regarding cybersecurity. At an individual level, cybersecurity assumes both active and passive online presence. Active presence implies individuals access the Internet, establish accounts for utilitarian purposes such as bill payment, and accessing personal health records; or hedonic activities such as shopping, or using social networking sites. Passive presence refers to the variety of businesses and organizations who store, access, and manage highly sensitive PII online, as well as personal information disclosed in social networking sites, by various individuals and organizations.

Every instance of directly experienced cyberattack is harrowing on its own. While it is conceivable that a respondent may have heard of cyberattacks and still remain inactive, and trust business and government organizations to safeguard their personal sensitive information and handle it with care, the expectation is that personally experiencing the effects of a cyberattack may influence both awareness and trust. This study asks several important questions:

[RQ1] Does experiencing one or more instances of cybertheft significantly correlate with any internet behaviors or consumer characteristics?

[RQ2] What are the consequences of low overall awareness regarding major cyberattacks?
[RQ3] How does trust relate to experience, awareness, and other consumer characteristics?

METHOD

The focus of this study is to address gender and other demographic differences in awareness, experience, and trust, as they relate to gender and cybersecurity. This study used the original Pew Research Center Cybersecurity Survey (Olmstead & Smith, 2016) dataset. A total of 1,040 phone interviews were conducted with US adults age 18 or 18, nationwide, between March 30 - May 3, 2016. The dataset includes answers from a nationally representative sample of US adults. Phone interviews were conducted over cell phone (74.8% of completed surveys, response rate 10%; and landline (25.2% of surveys, response rate 8%).

Of the original set of 120 questions, only a subset were used for this study: basic demographics (sex, age, education level), internet behaviors (access email/internet, have online accounts, visit social media websites), trust/confidence in business and government organizations, direct/indirect experience with cybertheft incidents, and expectations about future cyberattacks. Some of these questions had binary setups (yes/no, male/female), while others had 3-point or 4-point Likert scale answers. Any other volunteered answers recorded separately (ex., 'don't know,' 'does not apply,' or 'refused') were recoded into missing-value.

Independent variables. Key independent variables included demographic and behavioral items. Respondent gender was used either as an independent variable for univariate statistics, and as a split-file variable for covariance analysis. Behavioral variables expected to have an impact on awareness, experience, and trust included: how often they used the internet (intfreq), whether or not respondents access the internet using a tablet or smartphone (intmob) and visit social media sites (snsint2), whether or not they use public wifi for various purposes such as checking email, shopping online, or even personal banking (wifi2), and the types of online accounts they have with various categories of businesses (acct).

Dependent Variables. Awareness, experience, and trust required input from several variables in the original study, as explained below. Experience is the most important variable.

Experience (based on survey items from (secur2) questions asked respondents if, to the best of their knowledge, they ever did (receive) notice that (a) their social security number had been compromised; (b) their other sensitive personal information, such as account numbers, had been compromised; (c) there were fraudulent charges on their debit/credit card; (d) someone had taken over their email account without permission; (e) someone had taken over their social media account without permission; (f) someone tried to open line of credit or apply for a loan using their name; or (g) someone attempted to receive a tax refund using their name. Index variable secur2sum counted the number of incidents reported by each respondent (count if answer is 1=yes; ignore if answer is 2=no or missing value).

Awareness (based on survey items from policy6) explored consumers' having heard of (a) the publication of company emails at the Sony Corporation, (b) the exposure of government security clearance information at the Office of Personnel Management, (c) the exposure of credit card data of customers who shopped at Target stores, (d) the disruption of the powergrid in Ukraine, and/or (e) the publishing of the identities of AshleyMadison.com customers. A new variable policy6mean generated a mean value to approximate awareness for all cases where at least three of the answers were valid (1=heard a lot, 2=heard a little, 3=not heard at all). Information from the new policy6mean variable measured consumer indirect knowledge of cybertheft: since the question asked them about having heard of each incident, not having been directly affected by it. Awareness correlations were calculated for gender and internet behaviors.

Trust explored respondents' confidence in the ability of different types of organizations to keep their records safe from hackers and unauthorized users. Different questions asked about trust in (1) other people in general, (2) friends and family, (3) government, or (4) business organizations. In direct measures, respondents expressed their current habits of holding accounts or sharing passwords (across websites or with family/friends), and considered the likelihood of occurrence and possibility of success for future cyberattacks. All government units and organizations were lumped together as "the federal government" (e). Trust in business organizations differentiated between (a) the company that manufactured cell phone; (b) the company that provides cell phone service; (c) the email provider; (d) the social media sites respondent visits; (f) the credit card company; and (g) the companies or retailers with which the respondents does business. Cases with valid entries (1=very confident, 2=somewhat confident, 3=not too confident, 4=not at all confident) for five or more of the seven questions were retained for analysis. A total of 90 cases (0.09% of data set) were omitted from this analysis step due to an insufficient number of valid responses per individual interviewee.

Within the communication process, trust functions as both a premise and a result of the interaction between awareness and experience. In the context of cybertheft, it is important to learn about critical incidents, or the tipping point that may trigger a major change in the type of situational public with which an individual identifies. Trust has a behavioral component that includes sharing passwords (either across websites or with friends or relatives) and choosing not to open account with an organization deemed insufficiently trustworthy. The attitudinal component assesses consumer confidence in the ability and preparedness of business and government organizations to protect their sensitive information on a daily basis and if faced with a major cyberattack.

FINDINGS

Sample demographic distribution along the coordinates of age and education level emphasized the importance of exploring survey results from the gender perspective. It appears that older males are substantially more likely than younger males to have completed a higher level of education (ρ=0.160, Sig.=0.000). This relationship is absent among older vs. younger women, and older women are also less likely than men to have completed a college or graduate degree

(see Table 1 below). Although this survey did not ask respondents about the field in which they attained their highest level of education, the underrepresentation of women in STEM college programs and professional fields further accentuates the knowledge gap in a way that is meaningful to the topic of cybersecurity.

Table 1. Demographics Summary: Age Range and Education*

Age Range	High School grad or less		Some college/ Associate degree		College graduate or more		Total	
Gender	M	F	M	F	M	F	M	F
18-24	19.3%	10.1 %	13.6 %	12.8%	4.3%	3.7%	10.9 %	8.2%
25-34	13.3%	9.4%	21.8 %	10.1%	14.1 %	18.5 %	15.6 %	13.4 %
35-44	10.7%	10.1 %	12.7 %	13.4%	18.8 %	15.7 %	15%	13.4 %
45-54	24.07 %	14.8 %	15.5 %	16.1%	17.1 %	14.4 %	18.8 %	15%
55-64	18%	24.2 %	20.9 %	22.1%	21.8 %	24.1 %	20.4 %	23.5 %
65+	14.7%	31.5 %	15.5 %	25.5%	23.9 %	23.6 %	19.2 %	26.5 %

*About 3.7% of respondents (N=15 male and N=17) offered 'Don't Know/Refused' answers for either age or education and were excluded from this calculation

Awareness. Generally speaking, respondents who had heard a lot about recent cyberattacks (lower mean values) tended to have more types of online accounts (sum value), which is good. Unfortunately, they also reported higher incidences of cyberattack experiences, which is not so good. Consequently, the more they knew about recent cyberattacks, the less they trusted government and business organizations to protect their personal information from cyberattack and unauthorized users--a finding that was statistically relevant for women, though not for men (see Table 2 below).

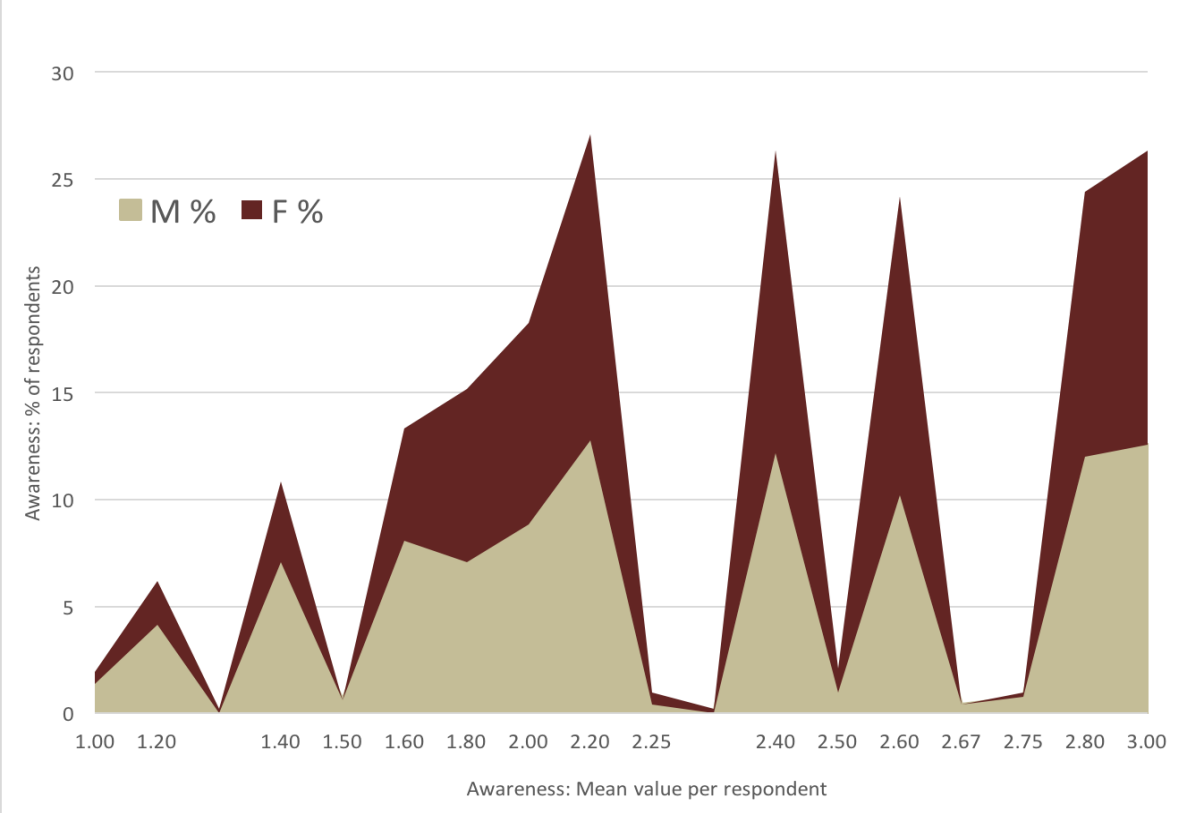
Table 2. Correlation of awareness with trust, experience, and various online accounts

Cyberattack Awareness (mean)	Trust in government and business orgz's (mean)	Online accounts (sum)	Experienced cyberattack directly (mean)
Male	0.003	-.422**	.207**
Female	-.098*	-.354**	.207**

Pearson's coefficient value listed for ρ*<0.05 and ρ**<0.01

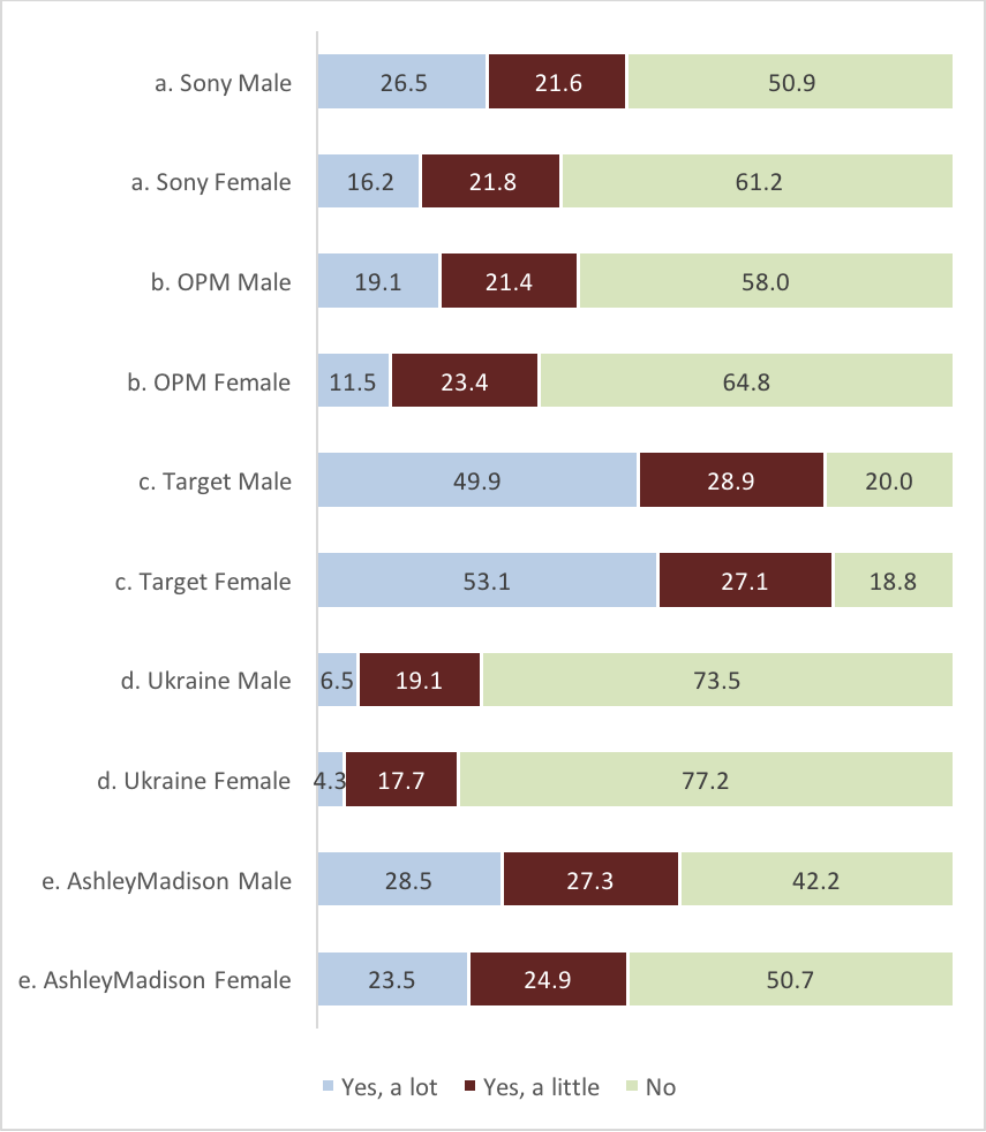
Overall, about 13% of the respondents (N=64 male and N=73 female) had not heard of any of the five major recent cyberattacks. Conversely, only ten respondents (7 men and 3 women) had heard a lot about all of the five data breaches. In Figure 1 below, a mean value close to 1 represents someone who had heard a lot about all incidents, whereas a mean value close to 3 represents someone who had not heard about any of the five incidents.

Figure 1. Awareness of recent cyberattacks (mean value), by gender



Overall, the cyberattack exposing credit card data of customers who shopped at Target registered the highest percentage of consumers who had heard “a lot” or at least “a little” about the cyberattack (79.7% of men and 81% of women). This finding is not surprising at all, given the intense coverage the incident garnered across news media and social media, for an extended period of time (See Figure 2 below). In terms of gender differences, however, this was the only incident where the percentage of women who had heard “a lot” or at least “a little” was substantially higher than for men.

Figure 2. Have you heard of the following cyberattacks?



Overall, respondents who had heard at least a little about these major attacks were less likely to place a lot of trust in the preparedness of US government (men and women) and US businesses

(men only) to prevent cyberattacks (see Appendix Table 1 for the complete list of statistically significant correlations concerning awareness of cyberattacks). Incidentally, though, adult men who heard a little or not at all about cyberattacks were more likely to do online baking or conduct financial transactions while connected to public wifi, to feel their personal information was, in general, more secure than five years ago, and to have reported that someone had attempted to open a credit line or apply for a loan using their name.

A higher level of awareness regarding cyberattacks among women respondents, on the other hand, tended to co-occur with decreased levels of trust in the ability of the cell phone service company and the federal government to protect personal records against hackers and unauthorized users. The same group of women were more likely to use their social media account information when logging into other sites, and to support the idea that encryption technology should be unbreakable, even to law enforcement.

Experience. The next step of this analysis focused on respondents' direct experience with cybertheft (see Table 3 below). It appears that the most frequently reported forms of cybertheft, based on the answer options provided by the Pew survey, were fraudulent charges on debit or credit card (47% of men and 43.5% of women) and compromising of personal information, such as account number (38.5% of men and 38.8% of women). In most cases, both types of cyberattack are solved at little to no cost the consumers must bear directly. The other types of attacks were reported with lower frequency, however a compromised social security number, a fraudulent loan, or a fake tax refund, usually trigger serious damage in terms of direct financial damages, as well as substantial investment of time and money to repair. Hacked social media accounts may be equally annoying to repair, though they often incur lower financial costs. Hacked email accounts may factor into other types of cybertheft, when the perpetrators use such unauthorised access to convince someone within the original owner's network to provide access to other sensitive information or even to transfer funds (DBIR 2016).

Table 3. Direct experience with cybertheft

To the best of your knowledge, did you ever (receive) notice that…	Males N (%)	Females N (%)
a. Social security number had been compromised?	87 (17.1%)	80 (15.1%)
b. Other sensitive personal information, such as account number, had been compromised?	196 (38.5%)	206 (38.8%)
c. Fraudulent charges on debit or credit card?	244 (47.9%)	231 (43.5%)
d. Someone else took over email account without permission?	86 (16.9%)	89 (16.8%)
e. Someone else took over social media account without permission?	52 (10.2%)	71 (13.4%)

f. Someone attempted to open a line of credit or apply for a loan using name?	73 (14.3%)	80 (15.1%)
g. Someone attempted to receive a tax refund using name?	24 (4.7%)	33 (6.2)

Across both genders, consumers who reported higher-incidence of data breach experiences tend to have several types of online accounts, and use the internet and email via mobile devices (smartphones, tablets, etc.), quite frequently ($\rho<0.05$). They have, on average, heard a lot or at least a little about the cyberattacks, and believe it is likely or very likely that in the next five years the US will experience a significant attack on public infrastructure, as well as banking and financial system. Consequently, they are not very confident that companies and government will keep personal records safe from hackers and unauthorized users. They are also more likely to have chosen to NOT use/create an account with an online service because of concerns about how personal data would be handled.

In addition, women who experienced several types of cybertheft are less likely to access their email via public wifi networks. Men, on the other hand, are very likely to use public wifi networks in airports, cafes, hotels, or libraries and even make online purchases. Despite having experienced cybertheft directly, they are more likely to share passwords to online accounts with friends or family (See Appendix Table 2 for complete list of statistically significant correlations for reports of cybertheft experiences).

Trust. The most poignant finding relative to consumer trust regarding cybersafety is the generalized nature of this item, for consumers who reported the smallest number (or complete absence of) cybertheft experiences of any kind. These men and women highly trust the ability and preparedness of organizations handling their personal information. Trust seems to extend across the board, both the US government and various businesses, for current practices and think that major cyberattacks are highly unlikely in the future. Barring negative experiences and in the absence of awareness regarding cybertheft, consumers are quite willing to trust people in general and opening online accounts with all their business and billing organizations.

Within the group of untried internet users who exhibit high levels of trust, women are more likely than men to agree that the government should be able to access encrypted communications when investigating crimes allow government access when investigating crimes. They also tend to have completed higher levels of education, possess and use mobile devices for accessing the internet, and use the internet and email more often. They are also more likely than men to be using social media sites, and to have accounts with their household utility providers.

Among men who expressed high levels of trust, common characteristics include lower awareness of cyberattacks in general, and higher incidence of online accounts that involve bill payments and transactions. They are also more likely than women to believe that in general, their personal information is more secure than it was five years ago (See Appendix Table 3 for full list of

statistically significant correlations regarding consumer trust).

Overall gender-based differences. When it comes to analyzing differences between men and women, the internet is a more integral part of women's lives, and avoidance of cognitive dissonance realities is reflected in an almost deliberate attempt to see its convenience and ignore the risks. Possibly due to their severe underrepresentation in or familiarity with the cybersecurity industry and issues, women were much more likely to trust that the federal government will protect their records, is be very prepared against major cyberattacks, and consequently should have access to encrypted information when investigating crimes.

At the same time, women are more likely than men to say "you can never be too careful" and even that a significant cyberattack on the US public infrastructure, such as air traffic control or power grid, will "definitely happen" within the next five years--while having no such concerns about a major cyberattack on the banking and financial system. So they are also more likely to be "very confident" that federal government, credit card companies, cell phone service company, and retailers will keep their personal records safe from hackers or unauthorized users--even while being less likely to think that the US businesses are very prepared or somewhat prepared to prevent cyberattacks on their own systems.

Regarding online accounts and behaviors, women are more likely to use social media applications such as Facebook, Twitter, or LinkedIn; to have online accounts with their healthcare provider; and to have chosen, at some point, to NOT use or NOT create an account with an online service because they were worried about how personal information would be handled. Regarding reports of identity theft, women were more likely than men to say someone took over their social media account without permission, or that someone attempted to receive a tax refund in their name. Also, the data breach crisis Target suffered in 2015-16 was the only incident where women were significantly more likely than men to have heard a lot about the exposure of consumer credit card data.

DISCUSSION

To summarize the findings of this study, it appears that US consumers operate based on a principle of trust in professionals doing their job, and may be quite naive in their approach to using the internet and safeguarding their personal information. However, this trust is fragile: as with reputation, all it takes to lose it is experiencing cybertheft directly. It is important, and infinitely cheaper, for organizations to promote consumer awareness of cybertheft: what it is, how it happens, where it already happened, what to do next. In the absence of concerted education efforts, consumers are most likely to abruptly flip from blissfully unaware to completely distrustful and likely to make moves that will cost the organization--be it divesting company stock, closing accounts or refusing to do business, or taking their unhappiness to the internet and causing reputational harm.

Consumers who are unaware of cybersecurity pose important risks to both their own and organizations' welfare. There is a substantial number of individuals (30.8% of men and 33.5% of

women), in today's day and age, who refuse to establish online accounts with various organizations, make most of their purchases with cash, and are completely uninterested in, or even actively avoid learning about cybersecurity. In addition to their direct negative impact on organizations' business and communication efforts, be they sales and advertising or public communication campaigns, these individuals are also unlikely to know that their personal information is, in fact, sitting somewhere on a server, and can be accessed with or without their permission. A second group of unaware consumers include those individuals and professionals who have already established a variety of online and electronic accounts with various business and government organizations, or even manage databases containing sensitive information, for their organization. Lack of awareness or interest in cybersafety makes them unwitting agents that could enable the next cybertheft incident to compromise individual or organization-wide cybersystems. Unaware consumers and IT users are most likely to experience or facilitate cybertheft within the category of phishing and scamming incidents.

At some point, however, the majority of the population becomes aware of *some* cybersecurity issues, whether through concerted education efforts at their workplace, or informal sources such as traditional and social media, or perhaps friends and acquaintances spreading the word about good practices and bad consequences. Not everyone understands the complexity of cybertheft, how it may happen, and how to react if they are directly impacted. Insufficient knowledge about how to exercise opt-out and opt-in choices, convenience, or mandated participation may limit consumer interest in changing their cyber behaviors. If inclined to take a fatalistic view on the issue, such individuals or groups may even stop trying to protect or monitor their personal accounts, thus creating opportunities for individual cybertheft.

On a larger scale, the 'unawares' might be serving in organizational positions where they could and should become active due to their ability and obligation to steward others' personal information. Choosing not to engage in problem-solving behaviors is often disastrous for the organization and its clients--as seen in the case of the massive 2017 Equifax data breach, where servers were left vulnerable to cyberattack with admin/admin access, or out-of-date security patches.

It could be argued that not acting on a critical piece of cybersecurity or cybertheft information is a form of engagement. However, the findings of this study emphasized the importance of maintaining an educated trust in government and business organizations. To a point, consumers may decide to trust simply because their needs and behaviors rely on taking the risk of conducting social and business transactions online on a daily basis. Promoting an educated consumer confidence however requires promoting overall consumer knowledge and behavioral changes that would encourage healthy management of information at individual and organizational levels. More and more professionals are blurring the lines between working in the office and from alternate locations (while traveling, from home, etc.). Cybersafety routines and policies are necessary to ensure end-to-end data safety.

Research limitations. This study is based on information collected by the Pew Research Center. While the sample attempted national representation for the US population, it still includes

overrepresentation among various demographic segments. Furthermore, the original study had a different agenda and focused on a limited number of cyberattacks which may or may not have been the best examples to explore with the general population. From a practitioner point of view, it would have been extremely useful to ask respondents where they had heard about the cyberattacks, and where they get the information they consider most relevant about cybersafety.

FUTURE RESEARCH

The findings of this study are critical for managers on crisis communication, consumer education, and overall corporate communication teams. The next step should be to collect information about influencers inside and outside organizations, who can direct and impact consumer behaviors toward increasing cybersafety. Marketing and communication efforts must both acknowledge and incorporate the enterprise character of cybersafety, which means targeting communication efforts both toward individual agency and organization-wide culture.

REFERENCES

Verizon Enterprise. 2017 Data Breach Digest. http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf Last accessed 11/29/2017

Armstrong, DJ (2007). Advancement voluntary turnover and women in IT: A cognitive study of work-family conflict. *Information & Management 44*(2): 142-153

Bagchi-Sen, S, Rao, HR, Upadhyaya, SJ, & Chai, S (2010). Women in cybersecurity: A study of career advancement. *IT Professional 12*(1). DOI 10.1109/MITP.2010.39

Broos, A. (2005). Gender and information and communication technologies (ICT) anxiety: Male self-assurance and female hesitation. *CyberPsychology & Behavior*, *8*(1), 21-31

Center for Cyber Safety and Education (ISC) (2017). Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response. A Frost & Sullivan Executive Briefing. https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf. Last accessed 11/27/2017

Constante E, den Hartog J, and Petkovic M (2015). Understanding perceived trust to reduce regret. *Computational Intelligence 31*(2): 327-347.

Dutton, W, Guerra, GA, Zizzo, DJ, & Peltu, M (2005) The cyber trust tension in E-government: Balancing identity, privacy, security. *Information Polity 10*(1, 2):13-23.

Grunig JE (2005). *Situational Theory of Publics: Encyclopedia of Public Relations*. Thousand Oaks, CA: Sage, 778-780.

Jenkins A, Anandarajan M, and D'Ovidio R (2014) 'All that glitters is not gold': The role of impression management in data breach notification. *Western Journal of Communication 78*(3): 337-357.

Kaspersky Lab. Beyond 11%. A study into why women are not entering cybersecurity. https://d1srlirzdlmpew.cloudfront.net/wp-content/uploads/sites/86/2017/11/03114046/Beyond-11-percent-Futureproofing-Report-EN-FINAL.pdf. Last accessed 11/27/2017

MacIntyre, CR, Engells, TE, Scotch, M, Heslop, DJ, Gumel, AB, Poste, G, & Broom, A. (2017). Converging and emerging threats to health security. *Environment Systems and Decisions*, 1-10.

Mercer, J. (2017, September 29). Why are women leaving technology jobs? Retrieved from https://www.cio.com/article/3229355/it-industry/why-are-women-leaving-technology-jobs.html

Morris, RG (2010). Identity thieves and levels of sophistication: Findings from a national probability sample of American newspaper articles 1995-2005. *Deviant Behavior 31*: 184-207.

O'Neill, P (2016, November 1). How to make sense of the wide open cybersecurity job market. Retrieved from https://www.cyberscoop.com/cyberseek-comptia-nice-cybersecurity-job-market/

Olmstead, K & Smith, A. (2017). Americans and Cybersecurity. Pew Research Center

Rainie, L, & Duggan, M (2016). Privacy and information sharing. *Pew Research Center*

Seeger, MW (2006). Best practices in crisis communication: An expert panel process. *Journal of Applied Communication Research 34*(3): 232-244.

Shields, K. (2015). Cybersecurity: Recognizing the Risk and Protecting against Attacks. *North Carolina Banking Institute* 19: 345-372.

Söderberg, J (2010). Misuser inventions and the invention of the misuser: Hackers, crackers and filesharers. *Science as culture 19*(2): 151-179.

Stuber, J, Meyer, I, & Link, B (2008). Stigma, prejudice, discrimination and health. *Social science & medicine (1982), 67*(3): 351.

Thiede, M (2005). Information and access to healthcare: is there a role for trust? *Social science & medicine, 61*(7): 1452-1462.

Trauth, EM, Quesenberry, JL, & Morgan, AJ (2004, April). Understanding the under representation of women in IT: Toward a theory of individual differences. In *Proceedings of the 2004 SIGMIS conference on Computer personnel research: Careers, culture, and ethics in a networked environment* (pp. 114-119). ACM.

ABOUT THE AUTHORS

Dr. Olga Vilceanu, Associate Professor
B.A. University of Bucharest, M.A. University of Bucharest, Ph.D. Temple University
Dr. Vilceanu's teaching is informed by her international background and experience in communication and management in industry, political organizations, and higher education. Her research interests include semantic network analysis of advertising and media coverage of major issues in science and technology, and communication campaigns using fragmented media, as well as framing, international, and interpersonal communication.

Dr. Kristine C. Johnson, Assistant Professor
B.S. University of Texas, M.S. Texas Christian University, Ph.D. Florida State University
Dr. Johnson teaches courses in marketing communication and advertising. She has industry experience in advertising and a background in radio broadcasting. Dr. Johnson's research focuses on consumer behavior, especially in relation to online media. She has presented her research at multiple conferences, and her work has been published in *The Journal of Radio and Audio Media*, *Cogent Business and Management*, *First Monday*, and *The Journal of Applied Marketing Theory* among others.