Journal of International Technology and Information Management

Volume 30 | Issue 1 Article 1

2021

General Population Demographics of Responses to a Nationwide Catastrophic Cyber-Attack: Exploratory Research

Garry White
Texas State University-San Marcos, Det. of Computer Information Systems and Quantitative Methods, gw06@txstate.edu

General Population Demographics of Responses to a Nationwide Catastrophic Cyber-Attack: Exploratory Research

Cover Page Footnote

This research was funded by the McCoy College Faculty Development funds (2019). 1. Parts of these sections were taken from White, G. (March 2020). “Awareness Training to Counter Panic/Worry for a Nationwide Catastrophic cyber-attack: Proposed Study.” PROCEEDINGS of 2020 Annual Information Systems Educators Conference (ISECON), Dallas/Plano, TX; March 26-28, 2020.

General Population Demographics of Responses to a Nationwide Catastrophic Cyber-Attack: Exploratory Research

Garry White
(Texas State University-San Marcos, Det. of Computer Information Systems and Quantitative Methods)

ABSTRACT

A national catastrophic cyber-attack is coming, just like the unpredictability of an earthquake. This exploratory research looks at the related demographics to the respond to such an attack. The responses used were Technology Optimism and Cyber Self-efficacy. The demographics studied were age, education level, surprise of the severity of an attack, gender, prior countermeasures awareness and devastation surprise. Technology Optimism and Cyber Self-efficacy showed a significant drop with the attack reading. This study's outcomes failed to support the influence of age, gender, and prior countermeasures awareness to significant drops in Technology Optimism and Cyber Self-efficacy. Devastation surprise was significant only with decreased Cyber Self-efficacy. Education level was significant with both technological optimism and Cyber Self-efficacy. However, what is interesting is that the higher the education level, the less Technology Optimism and Cyber Self-efficacy decreased. The results of this study will help policy makers develop effective strategies to help individuals deal with such an attack psychologically.

Keywords: cyber-attack, awareness training, countermeasures, cyber self-efficacy, technology optimism, demographics

ISSN: 1941-6679-On-line Copy

INTRODUCTION

Cyberwarfare is a weapon of mass "disruption" and can bring down a country such as Estonia in 2007 (Tamkin, 2017; McGuinness, 2007). Cyber-attack is more than just phishing and ID theft.
As streetlights, traffic lights, power grids, dams, sewer systems, transit lines, and other services are added to the Internet for management control, they become targets for hostile states, terrorists, and hackers. (Rundle, 2019). "The more connected a city is, the more vulnerable it is to cyberattacks. Hackers have, in recent years, effectively held cites hostage through ransomware, sometimes crippling critical systems for months at a time" (Rundle, 2019). Higher dependence on technology results in more vulnerability. As more information on residents is collected, nation-states or terrorists could incorporate the information into the cyberwarfare campaign.

Offensive information operations in cyberwarfare include 1) deny access to systems and data, 2) exploit information for own advantage, 3) corrupt information, and 4) destroy information and information systems (Chapple & Seidl, 2015). Corrupting information could also include replacing data with bogus/error data. (Rundle, 2019). Cyberwarfare can target civilians and civilian systems (Chapple & Seidl, 2015). Currently, there is no international law limiting cyberwar scope. (Chapple & Seidl, 2015).

Such a massive attack is coming to the U.S.A. A national cyberattack of devastating proportions is not a matter of if but when (Turak, 2018). Such an attack will disable government (Federal, state, county, city), banking (financial transactions, credit card), and communication (news media, Internet), with the power grid as an added target. In March 2019, there was a cyber-attack on the power grid (Sussman, 2019). The attack was a result of a failure to patch a firewall. Is the United States prepared for a massive cyberattack?

Goal of this study

When a devastating cyberattack occurs, how will the public respond? Some cyber-attacks are "panic attacks." Panic attacks are when an attacker creates chaos in communities by attacking emergency systems (Lee, 2018). Most panic studies deal with physical disasters resulting in death and destruction. The literature lacks self-efficacy or optimism related to a cyber-attack. Tthere is no death or destruction; only an inability to function and communicate. What demographic characteristics impact how people will respond when they no longer have technology?
The results of this study will help policymakers develop effective strategies to help

ISSN: 1941-6679-On-line Copy

.

individuals deal with such an attack psychologically.

This paper's two goals are to see first what impact a national catastrophic cyber-attack scenario has on two human dimensions; 1) technology optimism, and 2) cyber self-efficacy for a general population. These two human dimensions were selected because they show psychological well-being. Second, what demographic variables, such as awareness of infrastructure countermeasures, devastation surprise, age, gender, and education level, impact these two human dimensions? Age, gender, and education level variables were selected because they are generally a standard found in other research. Awareness of infrastructure countermeasures and devastation surprise are characteristics unique to this study.

LITERATURE REVIEW

What has happened -- History.[1]

Estonia (2007): In 2007, a cyber-attack disabled computer networks in the tiny Baltic country of Estonia (McGuinness, 2007). This was the first cyber-attack in history that affected an entire country (Tamkin, 2017).

Georgia (2019): The country of Georgia had a massive cyber-attack in October 2019. The cyber-attack took over 15,000 websites offline. The sites were government agencies, banks, courts, local newspapers, and TV stations. The country experienced general panic. (Cimpanu, 2019).

Eastern Europe (2017): In 2017, eastern Europe experienced a massive ransomware attack. The ransomware targeted government ministries, banks, utilities, and other important infrastructure and companies nationwide (Roth & Nakashima, 2017).

People Responses[1]

When people feel threatened with an economic or psychological existence, their anxiety, fear, unrest, crisis mood will lead to panic (Brickenstein, 1980). When a disaster occurs, people may panic with selfish or irrational flight behaviors due to losing control/functionality and a lack of knowing/communication. Quarantelli (2001) and Tierney et al. (2006) find that people's initial response to an emergency is prosocial instead of selfish or irrational flight behaviors.
Singer (1982) discusses people's reactions and responses to disasters and the need for disaster planning and training. There are long term reactions, the reactions of

ISSN: 1941-6679-On-line Copy

.

rescue and relief workers, and psychological first aid. However, this discussion deals with physical destruction (i.e., earthquakes and building collapses), including deaths and injuries. A cyber-attack does not generally create physical destruction, just the inability for a program to function. Hence, the panic that a cyber-attack generates will be different. To overcome panic, c*lear communication from authorities is extremely critical* (Loong, 2018).

Response types[1]

Two response types that impact panic and psychological well-being are:

1. **Optimism:**
   Trumbo et al. (2014) define optimism as a "person's belief of being at less risk from the dangers of the environment." Over the years, students were more optimistic about the impact of computers on their performance. Males are more optimistic than females (Walstrom et al., 2010).
2. **Self-efficacy:**
   Self-efficacy is the perceived ability to perform the needed response to cope with the risk. Self-efficacy is the confidence to successfully perform an action (Bandura, 1977) or deal with a threat (Liang & Xue, 2010). For example, Ng e. al. (2009) showed that self-efficacy is a determinant of employees' email-related security behaviors. Yoon et al. (2012) proposed a model based on PMT. They identified self-efficacy as a variable that significantly affects home wireless network users' decision to implement security features on their networks. They found that high self-efficacy has a significant impact on students' intentions to practice more information security. In this study, we define self-efficacy as the confidence in using current knowledge and software.

These two response types were selected because there is nothing in the literature showing how a cyber-attack impacts these response types.

Demographic variables

Two categories, physiological and cognitive, of five demographic variables were selected to study the impact (change) on the four human dimension responses. Age, gender, and education level variables were selected because they are generally a standard found in other research. Awareness of infrastructure countermeasures and devastation surprise are characteristics unique to this study.

ISSN: 1941-6679-On-line Copy

.

Physiological variables

Gender: Literature indicated males are more optimistic than females (Walstrom et al., 2010). Other research has shown gender differences in youth and adolescents (Alberts et al., 2007; Duggan et al., 2000; Lapsley & Hill, 2010). Panic disorder is twice as common in women as men (Medline Plus, 2020). Optimism bias showed no gender differences (Lapsley & Hill, 2010). However, females tend to be more pessimistic toward the impact of computers (Walstrom et al., 2010). Considering these differences, gender was selected to see if it has an impact on this study.

Age: The literature was minimal for age with cyber-attacks and human dimensions. However, personality traits change with age (Hennecke et al., 2020), and panic symptoms often begin before age 25 but may occur in the mid-30s (Medline Plus, 2020).

Cognitive variables

Education level: The literature lacks any research on the educational level and these two human dimensions dealing with cyber-attacks. Education level was used because it indicates general knowledge and critical thinking skills.

Devastation surprise: This is a new variable not found in the literature. What is being investigated is the emotional shock of an attack outcome.

Awareness: Organizations realize the importance of user security education and awareness training (Dodge et al., 2007; Schultz, 2004). Education makes users more security conscious (Ng et al., 2009) and changes users' Internet behavior (Albrechtsen & Hovden, 2010; D'Arcy, Hovav, & Galletta, 2009; Kruger et al., 2010). However, continued awareness training loses its effectiveness over time (Wolf et al., 2011). Refresher courses will be needed to lower unrealistic thinking, such as Optimistic Bias. Users must constantly be reminded to be aware of security issues (Peltier, 2005). An educational program must continually keep users aware and proactive and build proper security habits (Yoon et al., 2012).

ISSN: 1941-6679-On-line Copy

.

Hypotheses

This study explored how subjects' demographics and reading of a massive national cyber-attack can impact a general population's technology optimism and cyber self-efficacy. The literature lacks studies showing how a cyber-attack impacts human dimensions in relation to the individual's demographics.

Hypothesis 1: Cyber-attack Responses

Reading a scenario of a national catastrophic cyber-attack will result in responses of:
H1-1, lower Technology Optimism.
H1-2, lower Cyber Self-Efficacy

Hypothesis 2: demographic characteristics correlations

H2-1 Age correlates with changes in responses.
H2-2 Education level correlates with changes in responses.

Hypothesis 3: nominal demographic characteristics differences in responses

H3-1 Gender impacts changes in responses
H3-2 Prior countermeasures awareness impact changes in responses.
H3-3 Attack devastation surprise impacts changes in responses.

METHODOLOGY

Subjects

"Internet participants in online studies are a purely self-selected sample of participants and thus may be more homogeneous than desired" (Weiser, 2000). This was avoided by using a random sample of 579 adults from the general population of the U.S.A. (via Qualtrics). Subjects from Qualtrics were invited to participate in this research. All 579 subjects, provided from Qualtrics, fully completed the survey. The Qualtrics survey they accessed contained four instruments and a reading of a national cyber-attack. A pre-survey before the reading was performed as a control base reference for each subject.

ISSN: 1941-6679-On-line Copy

.

The reading was written by a Certified Information System Security Professional of (ISC)2 and a Certified Cyber Security Professional of ICCP. Some of the demographics are: mean age 45 $\pm$ 17; 49% male, 51% female, 46% full-time employment, 48.2% had a 4-yr degree or more, 50% had prior countermeasure awareness, and 48.5% yes to devastation surprise. Age, gender, education level, prior countermeasures awareness, and devastation surprise were the demographic variables studied.

Two instruments used[1] (see Appendix C)

The two instruments used a 7-point Likert scale to indicate the level of agreement. For example, strongly agree to strongly disagree. This provided discrete tiered numbers with a restricted range.

Technology Optimism

Items for Technology Optimism were taken from the Technology Readiness Index (TRI) (Parasuraman, 2000).

Cyber Self-efficacy

Cyber Self-Efficacy items came from Claar & Johnson (2012) and White & Ekin & Visinescu (2017).

Three Phases of this study

1. **Determine current state (Data Set 1)**: The first phase was obtaining demographic information and the administration of the four instruments to determine the current state of Technical Optimism and Cyber Self-efficacy. This is to establish a baseline as the control prior to treatments for comparisons.

2**. Treatment:** All subjects read a scenario of a national catastrophic cyber-attack. See Appendix A. Half of the subjects read a scenario of countermeasures prior to reading the cyber-attack. See Appendix B.

3. **Determine state after reading the Scenario (Data Set 2)**: After reading the attack scenario, the two instruments were administered again to determine the current state of Technology Optimism and Cyber Self-efficacy.

.

Analysis

By using seven-point Likert items with a t-Test (parametric test) and Mann-Whitney-Wilcoxon (MWW) (non-parametric test) will have similar power (Winter & Dodou, 2012). However, found MWW had a power advantage with non-normal distributions. The conclusions for five-point Likert data were that both tests would not find a significant difference in a population when there is none (Winter & Dodou, 2012). This was consistent with another study. This second study showed parametric and nonparametric tests were similar regarding false positives (Type I error rate) for Likert items (Rasmussen, 1989).

Therefore, for analysis, paired-wise t-Tests of the four technology optimism measures, and self-efficacy were performed to determine if differences existed. If the significant data had significant peaked distributions or skewed, the non-parametric related-samples Wilcoxon Signed Rank Test was performed to confirm the t-Test.

RESULTS

Descriptive Statistics

Tables 1 shows the descriptive statistics of the three sets of data (before, after change) for Technology Optimism and Cyber Self-Efficacy. The changes were negative, indicating a drop in score after the attack reading. The data were non-normal. The statistics were more than two standard errors. To confirm any significant findings with the t-Test, the non-parametric related-samples Wilcoxon Signed Rank Test will be used.

Table 1. Descriptive Statistics

	N	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
TechOpt_1*	579	21.1520	5.49939	-.930	.102	.672	.203
Self-Eff_1*	579	19.3092	6.20465	-.654	.102	-.218	.203
TechOpt_2*	579	20.5458	5.74299	-.741	.102	.045	.203
Self-Eff_2*	579	18.4594	6.77924	-.490	.102	-.607	.203
TechOptChange*	579	-.6062	3.44312	.456	.102	14.441	.203
SelfEffChange*	579	-.8497	3.48847	-1.045	.102	4.875	.203
Valid N (listwise)	579						

.

* data were non-normal due to skewness and/or kurtosis significant differences from zero. The related-samples Wilcoxon Signed (WS) rank test was warranted for significant t-Tests.

Face Validity of the readings (scenarios)

Face validity is the extent a measure reflects what is intended to measure (Nunnally & Bernstein, 1994). Another face validity definition is the degree that respondents judge the appropriateness of instrument items (Anastasi, 1988); Nevo, 1985). Three post-survey questions were given to check the readings' quality and validity through the subjects' impression of meaningful and appropriateness of the readings. See Table 2.

Table 2. Three reading (scenarios) survey questions.

1. How much did you learn and gain insight from the readings?		2. How would you describe the readings?		3. Did the attack reading surprise you as to the extent of disruption?	
None	4.2%	Poor	5.3%	Yes	48.5%
A little	32.7%	Reasonable	28.2%	No	40.2%
Good Amount	44.9%	Insightful	48.2%	No opinion	11.3%
Large Amount	18.2%	Very well done	18.4%		

As shown in Table 2, 63.1% of the subjects believed they learned a good/large amount and gained good/large insight from the readings. And 66.6% judged the readings as insightful or very well done. Finally, almost half of the subjects were surprised by the extent of the disruption and countermeasures/response. These perceptions by the subjects suggest good face-validity.

Validity and Reliability Data Analysis

Validity and reliability of the data were checked using Cronbach's Alpha, Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy, and Bartlett's Test of Sphericity before the data was analyzed. The Cronbach's Alphas were over .928, which indicates high internal consistency. The Alpha values were considered "excellent." See Table 3.

.

Table 3. Reliability -- Cronbach's Alpha

Instrument	Data Set 1 (before)	Data Set 2 (After first reading)
Technology Optimism	.928	.940
Cyber Self-Efficacy	.936	.955

For this analysis, each data set's factors were tested for validity by performing the Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy and Bartlett's Test of Sphericity. Since KMO was greater than .88, and Bartlett's Tests were significant ($p < .001$), variables had a strong relationship supporting the use of factor analysis. Although these items are self-reporting/perception, they have significantly high validity and reliability. See Table 4.

Table 4. KMO and Bartlett's Tests before attack reading.

		Data Set 1 (before)	Data Set 1 (after)
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.880	.889
Bartlett's Test of Sphericity Approx. Chi-Square		4058.230	4779.318
	df	28	28
	Sig.	$p < .001$	$p < .001$

A factor analysis using principal component analysis (Varimax rotation with Kaiser Normalization) was performed on each data set to ensure all items of the survey loaded correctly on the factors intended. See Appendix D.

Cumulative total variance explained through rotation sums of squared loadings for Data Sets 1, 2 were 83.25%, 86.51, respectively. All Rotated Component Coefficients were >.831. Refer to Appendix D factor analysis.

ISSN: 1941-6679-On-line Copy

.

Paired-wise t-Test.

Since an ANOVA treats each data set as coming from different subjects rather than from the same subject, Pair-Wise t-Tests were performed to see any significant changes with these four response types. If significant, the non-parametric related-samples Wilcoxon Signed Rank Test was used to confirm the t-Test. See Table 5.

Table 5. Paired-wise t-Test for the two response types

	Mean Difference	Std. Deviation	Std. Error Mean	t	df	Sig. (2-tailed)	Cohen's d
Pair 1 TechOpt_1 - TechOpt_2	**.60622**	**3.44312**	**.14309**	**4.237**	**578**	**.000**	**.1078**
Pair 3 Self-Eff_1 - Self-Eff_2	**.84974**	**3.48847**	**.14498**	**5.861**	**578**	**.000**	**.1308**

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between TechOpt_1 and TechOpt_2 equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between Self-Eff_1 and Self-Eff_2 equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Table 5 shows technological optimism (Pair 1: $t = 4.237$, $df = 578$, $p < .001$, Cohen's $d = .1078$) and cyber self-efficacy (Pair 3: $t = 5.861$, $df = 578$, $p < .001$, Cohen's $d = .1308$) significantly decreased.

Since the data were non-normal, the related-samples Wilcoxon Signed (WS) rank test was performed on technological optimism and cyber self-efficacy. The two WS were consistent with the t-Test ($p < .001$). The null hypotheses of the differences between technological optimism before and after and cyber self-efficacy before and after equals 0 was rejected. However, the Effect Sizes based on Cohen's d were found to be small, < .2. The effect was trivial. The differences were unimportant.

Hypothesis #1 Results for Cyber-attack Four Responses from Paired-wise t-Test

Reading a scenario of a national catastrophic cyber-attack will result in responses of:

H1-1, lower Technology Optimism.
Supportive
(Score dropped by -.6062. Pair 1: $t = 4.237$, $df = 578$, $p < .001$, Cohen's $d = .1078$)

H1-2, lower Cyber Self-Efficacy.
Supportive
(Score dropped by -.8497. Pair 3: $t = 5.861$, $df = 578$, $p < .001$, Cohen's $d = .1308$)

Hypothesis #2 Results for characteristics correlations with Age and Education Level

H2-1a Age correlates with changes in Technology Optimism
Not Supportive

	Pearson		
N	Coor. Coeff.	Sig (2-tail)	Age Data type
579	-.074	.075	Serial

H2-1b Age correlates with changes in Cyber Self-Efficacy
Not Supportive

	Pearson		
N	Coor. Coeff.	Sig (2-tail)	Age Data type
579	-.027	.514	Serial

.

H2-2a Education level correlates with fewer changes in Tech. Optimism
S**upportive**

	Spearman's rho		
N	Coor. Coeff.	Sig (2-tail)	Education Level Data type
550	**.125**	**.003**	**Ordinal**

H2-2b Education level correlates with fewer changes in Cyber Self-Efficacy
Supportive

	Spearman's rho		
N	Coor. Coeff.	Sig (2-tail)	Education Level Data type
550	**.098**	**.021**	**Ordinal**

The higher the Technology Optimism and Cyber Self-Efficacy scores, the less drop in response. Because the rho correlations are positive, the higher the education level, the lesser drop in Technology Optimism, and Cyber Self-Efficacy scores.

Hypothesis #3: nominal characteristics of gender, prior awareness, and devastation surprise differences in responses

H3-1 Gender impacts changes in responses (See table 6). **Not Supportive**

Table 6. ANOVA: Gender (Nominal data: Male, Female)

		Sum of Squares	df	Mean Square	F	Sig.
TechOptChange	Between Groups	.000	1	.000	.000	.997
	Within Groups	6852.217	577	11.876		
	Total	6852.218	578			
SelfEffChange	Between Groups	21.926	1	21.926	1.804	.180
	Within Groups	7012.001	577	12.153		
	Total	7033.927	578			

H3-2 Prior countermeasures awareness impact changes in responses
Not Supportive

(See table 7).

.

Table 7. ANOVA: Awareness of countermeasures before reading cyber-attack.(Nominal data: Yes, No).

		Sum of Squares	df	Mean Square	F	Sig.
TechOptChange	Between Groups	10.614	1	10.614	.895	.344
	Within Groups	6841.603	577	11.857		
	Total	6852.218	578			
SelfEffChange	Between Groups	35.392	1	35.392	2.918	.088
	Within Groups	6998.535	577	12.129		
	Total	7033.927	578			

H3-3 Attack devastation surprise impacts changes in responses

Not Supportive

(See Table 8). Tech. Optimism

Supportive

Cyber Self-Efficacy

Table 8. ANOVA: Attack Surprise (Nominal data: Yes, No)

		Sum of Squares	df	Mean Square	F	Sig.
TechOptChange	Between Groups	43.159	1	43.159	3.359	.067
	Within Groups	6243.938	486	12.848		
	Total	6287.096	487			
SelfEffChange	Between Groups	59.220	1	59.220	5.011	**.026**
	Within Groups	5743.630	486	11.818		
	Total	5802.850	487			

The “no” group had a mean score of -0.5249 for Cyber Self-efficacy.
The “yes” group had a mean score of -1.2247 for Cyber Self-efficacy, indicating a greater drop in Cyber Self-Efficacy.

.

DISCUSSION

Technology Optimism and Cyber Self-Efficacy did significantly drop after reading about a national catastrophic cyber-attack that paralyzes a country. For **Technology Optimism**, subjects consciously lose faith in technology. Gender, age, awareness of countermeasures before the reading, and surprise of devastation had no impact on the decrease of Technology Optimism. What is interesting is that knowledge of countermeasures failed to maintain optimism with technology. This may be explained by the emotions of lacking control overriding any rational content. They may have realized that most cyber operations are out of their control since infrastructure computers were attacked. Also, the surprise of devastation did not contribute to a drop in Technology Optimism. Subjects possibly believe technology will, in time, overcome the devastation. What is interesting is that the higher the education level results with fewer drops in Technology Optimism.

For **Cyber Self-efficacy,** a massive cyber-attack will result in subjects losing their confidence to control the attack's effect on the internet and their computer. Gender, age, and awareness of countermeasures before the reading had no impact. However, the surprise of devastation did; the more surprise, the lower cyber self-efficacy. This is a human characteristic that needs to be considered. The issue here is confidence based on the ignorance of consequences. What is interesting is that the higher the education level results in fewer drops in Cyber Self-efficacy.

Gender, age (for those over 18), and awareness of infrastructure countermeasures appear not to be issues in people's responses to a catastrophic cyber-attack. From this study, the big find is that general education level and devastation surprise of an attack are important factors in how people will respond.

Can general education level over-ride the effect of a catastrophic cyber-attack? Based on these results, the answer is yes. It appears that better well-rounded, educated people can deal with a massive cyber-attack better. Education may provide higher general self-efficacy and better critical thinking skills to deal with the attack. Future research needs to investigate this. This study did fail to support the value and need for awareness of countermeasures (a form of specific education) before a catastrophic cyber-attack. An explanation may be that the countermeasures were for the infrastructure, which is out of the subject's control. Instead of reassuring people, the infrastructure can deal with the massive national cyber-attack, awareness of action the subject can take may be in order.

ISSN: 1941-6679-On-line Copy

.

Age did not correlate with Technology Optimism and Cyber Self-Efficacy changes, while educational level did correlate with these changes. An explanation is that age measures a physical characteristic, and educational level impacts cognition and attitudes. Technology Optimism and Cyber Self-Efficacy are cognitive and attitude characteristics.

Gender did not differentiate between changes in Technology Optimism and Cyber Self-Efficacy. An explanation is that gender is a physical characteristic while Technology Optimism and Cyber Self-Efficacy are cognitive and attitude characteristics.

Prior countermeasures awareness did not differentiate between changes in Technology Optimism and Cyber Self-Efficacy. An explanation is that this prior awareness failed to address the personal countermeasures needs, or the anxiety from the attack had a greater impact.

The attack devastation surprise did not impact Technological Optimism changesbut did impact Cyber Self-efficacy. The surprise may have led to self-doubt, which would lower self-efficacy (confidence). However, the surprise did not change the infrastructure's optimism since the infrastructure is outside the self.

CONCLUSION

As Rhee et al. (2012) indicated, since technology alone cannot completely protect information systems from potential threats, there needs to be more effort into addressing the human dimensions when dealing with information security events. This study showed that reading about a national catastrophic cyber-attack that paralyzes a country lowers the two responses of Technological Optimism and Cyber Self-Efficacy. Interestingly, those who were surprised by the devastation of such an attack had a greater significant drop in Cyber Self-Efficacy, less confidence in dealing with the cyber-attack. But those with a higher education level had a lesser drop in Technology Optimism and Cyber Self-Efficacy.

The significant drops in these two responses were trivial as defined by Cohen's d. What needs to be noted is that two unexpected factors were found: devastation surprise and education level. These two factors, affecting responses to an attack, are lacking in the literature.

ISSN: 1941-6679-On-line Copy

.

Implications

This study indicates two demographic characteristics to consider, education level and knowledge of attack consequences. People's responses are more positive to a cyber-attack when they have higher general education and awareness of possible devastation (not surprised). Reassurance comes from understanding the devastation and higher education (more general knowledge and critical thinking skills). This suggests a better ability to deal with a national catastrophic cyber-attack emotionally. Preparing for a disaster, be it a massive national cyber-attack, a hurricane, or an earthquake, requires having a general education at the highest level and awareness of the disaster's consequences to ensure panic avoidance. The findings of this study can lead to better proactive strategies to prepare individuals for an attack by understanding attacks and then being able to better deal with the attack psychologically.

Limitations

This study does have limitations. The survey relies on self-reported measures, which could have self-report bias, where respondents tend to answer inaccurately or more positively as opposed to documented data. In addition, users are likely to vary in their perceptions. However, the data's validity and reliability were excellent based on Cronbach's Alpha, KMO, Bartlett's Tests, and factor analysis.

Another limitation is the Effect Size. This poses the question: does understanding and knowing these differences have practical usage? As measured by Cohen's d, the Effect Sizes were small for the drop in technology optimism scores (d = .1078) and small for the drop in cyber self-efficacy scores (d = .1308). This is trivial, and the practicality is questionable. To confirm the practicality of findings, a larger sample size is needed for a larger Effect Size.

Future research

Future research needs to address the differences between youth (under age 18) and adults(over age 18)? This study only used subjects over the age of 18. While youth play/entertain on the computer for up to 9 hours each day (Fox & Edwards, 2015), adults use the computer for other reasons unrelated to entertainment (i.e., bank transactions, bill payments). The motivations for computer usage become different. The youth are still in the learning phase of life, while adults are in the productive phase of life. Also, youth know life only with technology, while older adults have lived without such technology.

ISSN: 1941-6679-On-line Copy

.

Will their responses be different when experiencing an attack that shuts down technology? The results of a similar study with youth (under age 18) vs. adults (over age 18) may be very different.

REFERENCES

Alberts, A., Elkind, D., & Ginsberg, S. (2007). The personal fable and risk-taking in early adolescence. *Journal of youth and adolescence, 36*(1), 71-76.

Albrechtsen, E. & Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation, and collective reflection; an intervention study. *Computers & Security*, 29(4), 432.

Anastasi A. (1988) Psychological testing. Macmillan, New York.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavior change. *Psychological Review*, 84, 191-215.

Brickenstein, R. (1980). Individual reactions, summation phenomena and collective reactions. MMW, *Munchener Medizinische Wochenschrift*, 122(42), 1459-1462. Retrieved from http://libproxy.txstate.edu/login?url=https://search.proquest.com/docview/75441251 ?accountid=5683.

Britt P. (2008). You've got mail….and security breaches. *Inf Today* 25(7), 1–1, 44.

Chapple, M. & Seidl, D. (2015). *Cyberwarfare: Information Operations in a Connected World*. Jones & Bartlett Learning: Information systems security & assurance series, Burlington, MA 01803 .

Cimpanu, C. (28 October 2019). Largest cyber-attack in Georgia's history link to hacked web hosting provider. ZDNet, Trend Micro. Accessed (11/9/19) from https://www.zdnet.com/article/largest-cyber-attack-in-georgias-history-linked-to-hacked-web-hosting-provider/

Claar C.L. & Johnson J. (2012). Analyzing home PC security adoption behavior. *J Comput Inf Syst*. 52(4), 20–29.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security

.

countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20(1), 79-98.

Dodge, R. C. & Carver, C. & Ferguson, A. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73.

Duggan, P. M., Lapsley, D. K., & Norman, K. (2001). Adolescent invulnerability and personal uniqueness: Scale development and initial construct validation. Ball State University, Ph.D. Thesis. LD2489.Z68 2001 .D84, http://liblink.bsu.edu/catkey/1203838.

Fazzini, K. (2018). Warnings about a massive cyberattack aren't new- intelligence officials have raised the red flags for years. *CNBC* July 24, 2018. https://www.cnbc.com/2018/07/24/cyberattack-warnings-from-us-intelligence-officials-are-not-new.html (accessed on 11/3/2018).

Fox, M. & Edwards, E. (2015). Teens Spend 'Astounding' Nine Hours a Day in Front of Screens: Researchers. NBC News Health web access on November 24 at https://urldefense.proofpoint.com/v2/url?u=http-3A__www.nbcnews.com_health_kids-2Dhealth_kids-2Dspend-2Dastounding-2Dnine-2Dhours-2Dday-2Dfront-2Dscreens-2Dresearchers-2Dn456446&d=BQIFaQ&c=OrYO-caJHQE1g_AJU3az1awi55It-bjDIQrtRiZ6WBk&r=gA9KwoVNR4Hf1oF0vRRojA&m=BngVrRSXmwtdwx2dXiDi9zsz0vtmfY5xNZh5nlLnTnY&s=ovGijM5KtBxs3DP-KuCTWYRQ5LQdcrSmNxK-fsRYz_4&e

Hennecke, M., Schumann, P., & Specht, J. (Sept 2020). Age-related differences in actual-ideal personality trait level discrepancies. Psychology and Aging, Advance online publication. https://doi.org/10.1037/pag0000573

Kirkpatrick, D. D. & Nixon, R. (2018). U.S.-U.K. Warning on Cyberattacks Includes Private Homes. New York Times, April 16, 2018. https://www.nytimes.com/2018/04/16/world/europe/us-uk-russia-cybersecurity-threat.html (accessed on 11/3/2018).

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, 18(5), 316-327.

.

Ku, C.Y. & Chang, Y.W. & Yen, D. D, (2009). National Information Security Policy and its Implementation: A case study in Taiwan. *Telecommunications Policy*, 33(7), 371.

Lapsley, D. K., & Hill, P. L. (2010). Subjective invulnerability, optimism bias and adjustment in emerging adulthood. Journal of youth and adolescence, 39(8), 847-857.

Lawler, D. & Swan, J. (2018). **Special report: America's greatest threat is a hurricane-force cyberattack.** *Axios,* Aug 4, 2018. https://www.axios.com/americas-greatest-threat-hurricane-force-cyberattack-67ff9c98-1cb8-4358-9d9e-e8c26836dec3.html. (Accessed 10/31/ 2018).

Lee, D. (9 August 2018). Warning over 'panic' hacks on cities. BBC News. Accessed (11/9/19) from https://www.bbc.com/ news/technology-45128053

Liang, H. & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11(7), 394-413.*

Loong, L. H. (2018). Sing Health cyber-attack: Now what? (2018). *SMB World Asia* (Online), Retrieved (11/9/19) from http://libproxy.txstate.edu/login?url=https://search.Proquest .com/docview/2074824570?accountid=5683

McDuling, J. (2014). America is the prime target of international cyberattacks. *Quartz,* February 27, 2014. https://qz.com/180700/america-is-the-prime-target-of-international-cyberattacks/ (accessed 11/5/2018)

McGuinness, D. (2007). How a cyber-attack transformed Estonia. *BBC News, Tallinn, Estonia,* April 27, 2017. https://www.bbc.com/news/39655415 (accessed on 10/31/2018).

McLaughlin K. (2006). COMPTIA: end-user training is critical to security. *CRN* 1194, 35.

.

Medline Plus (2020). Panic disorder. NIH: U.S. National Library of Medicine, Bethesda, MD. https://medlineplus.gov/ency/article/000924.htm#:~:text=Symptoms%20often%20begin%20before%20age,diagnosed%20until%20they%20are%20older (accessed October 7, 2020).

Mensch, S. & Wilkie, L. (2011). Information security activities of college students: an exploratory study. *Acad Inf Manage Sci J*. 14(2), 91–116.

Nevo B. (1985). Face validity revisited. *J Educ Meas*, 22, 287 – 93.

Nunnally, J.C. & Bernstein, I.H. (1994). Psychometric theory. McGrawHill, New York.

Palmer, D. (2018). Cloud computing: Why a major cyber-attack could be as costly as a hurricane: The economic costs of a large cyber-attack could be as large as the impact of a major natural disaster. *ZDNet*, January 17, 2018. https://www.zdnet.com/ article/cloud-computing-why-a-major-cyber-attack-could-be-as-costly-as-a-hurricane/ (access 11/10/18).

Panetta, L. E. (2012). Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, October 11, 2012 U.S. Department of Defense News Transcripts. http://archive.defense.gov/transcripts/transcript.aspx? transcriptid=5136 (accessed on 10/31/2018).

Parasuraman, A. (2000). Technology Readiness Index (TRI). *Journal of Service Research*, 2(4), 307-320.

Peltier, T. (2005). Implementing an information security awareness program. *EDPACS*, 33(1), 1-18.

Pollitt D. (2005). Energis trains employees and customers in IT security. *Hum Res Manage Digest.* 13(2), 25–28.

Puhakainen P, & Siponen M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quart*. 34(4), 757

.

Quarantelli, E. L. (2001). The sociology of panic. In N. J. Smelser & P. B. Baltes (Eds.), *International encyclopedia of the social and behavioral sciences* (pp. 11020–11023). Oxford, UK: Elsevier Science Ltd. http://dx.doi.org/10.1016/B0-08-043076-7/ 01867-2

Rasmussen, J. L. (1989). Analysis of Libert-scale data: A reinterpretation of Gregoire and Driver. *Psychological Bulletin*, 105, 167-170.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221-232.

Rogers, J. (2011). U.S. Power Grid Still Prime Cyber Target. *The Street*, Oct. 26, 2011. https://www.thestreet.com/story/ 11290254/1/us-power-grid-still-prime-cyber-target.html

Roth, A. & Nakashima, E. (2017). Massive cyberattack hits Europe with widespread ransom demands. *Washington Post*, June 27, 2017. https://www.washingtonpost. com/world/europe/ukraines-government-key-infrastructure-hit-in-massive-cyberattack/2017/06/27/7d22c7dc-5b40-11e7-9fc6-c7ef4bc58d13_story.html? noredirect=on&utm_term=.258c0d474ca7 (accessed 11/6/2018)

Rotvoid, G. & Landry, R. (2007). Status of security awareness in business organizations and colleges of business: an analysis of training and education, policies, and social engineering testing. Dissertation, University of North Dakota.

Rundle, J. (2019). How Hackers Could Break Into the Smart City. *Journal Report Cyber Security, Wall Street Journal*, September 18, 2019, p. R1, R8-R9.

Schultz, E. (2004). Security training and awareness – fitting a square peg in a round hole. *Computers & Security*, 23, 1-2.

Singer, T. J. (1982). An introduction to disaster: Some considerations of a psychological nature. *Aviation, Space, and Environmental Medicine*, 53(3), 245-250. Retrieved from http://libproxy.txstate.edu /login?url=https://search.proquest.com/docview/80381394?accountid=5683.

Sussman, B. (2019). Revealed: Details of 'First of Its Kind' Disruptive Power Grid Attack. Secure World, Seguro Group Inc., Oct 8, 2019. https://www.secureworldexpo. com/industry-news/first-u.s.-power-grid-attack-details (Accessed on 12/15/2019)

.

Tamkin, E. (2017). 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats? *Foreign Policy (FP),* April 27, 2017. https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/ (accessed on 10/31/2018)

Tierney, K., Bevc, C., & Kuligowski, E. (2006). Metaphors matter: Disaster myths, media frames, and their consequences in Hurricane Katrina. *Annals of the American Academy of Political and Social Science*, 604, 57–81. http://dx.doi.org/10 .1177/0002716205285589

Trumbo, C. & Meyer, M.A. & Marlatt, H. & Peek, L. & Morrissey B. (2014). An assessment of change in risk perception and Optimistic Bias for hurricanes among Gulf Coast residents. *Risk Analysis,* 34(6):1013-24.

Turak, N. (2018). The next 9/11 will be a cyberattack, security expert warns. *CNBC*, 1 June 2018. https://www.cnbc.com/2018/06/01/the-next-911-will-be-a-cyberattack-security-expert-warns.html (accessed 11/3/2018).

Wagley J. (2010). Breaches lead to employee training. *Secur Manage*; 54(4), 44.

Walstrom, K.A. & Thomas, C.E. & Weber A. (2010). Changes in Student Computer Technology Attitudes over 20 Years: 1988 to 2009. *Journal of Computer Information Systems*, 51(2), 81-6.

Weiser, E. B. (2000). Gender Differences in Internet Use and Internet Application Preferences: A Two-Sample Comparison. *Cyber Psychology & Behavior,* 3(2), 167-178.

White, G. & Ekin, T. & Visinescu, L. (2017). "Analysis of Protective Behavior and Security Incidents for Home Computers." *Journal of Computer Information Systems*: 57(4): 353-363. Online: (2016) http://www.tandfonline.com/doi/full/10.1080/08874417.2016.1232991

Winter, J. C. F. & Dodou, D. (2012). Five-Point Likert Items: t test versus Mann-Whitney-Wilcoxon. *Practical Assessment, Research & Evaluation,* 15(11), 1-16. ISSN 1531-7714.

Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring an information security awareness program. *The Review of Business Information Systems*, 15(3), 9.

.

World Economic Forum (2018). The Global Risks Report 2018, 13th Edition. W*orld Economic Forum publisher*. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf (accessed 11/11/18)

Worrall, S. (2015). Is the United States Prepared For A Massive Cyberattack. *National Geographic* November 8, 2015. https://news.nationalgeographic.com/2015/11/151108-cybercrime-cyberattack-ted-koppel-computers-hacking-internet-ngbooktalk/ (accessed 10/31/2018).

Yoon, C., Hwang, J.W., Kim, R. (2012). Exploring Factors that Influence Students' Behaviors in Information Security. *Journal of Information Systems Education*, 23(4), 407-415.

ISSN: 1941-6679-On-line Copy

.

APPENDIX A

Scenario Reading A: the results of a national catastrophic cyber-attack.

The targets of a catastrophic national cyber-attack are the government, the military, businesses, the power-grid, and homes. Such an attack makes no distinction between targets. All are targets.

The attackers can be hostile governments, terrorists, and criminals (organized crime). Their attack objective is to make a nation unable to function/communicate by corrupting data and shutting down information systems, resulting in people panicking.

Warnings about a massive cyberattack are not new – intelligence officials have raised red flags for years (CNBC July 2018). USA and UK warn of cyber-attacks on homes as well (NY Times, April 2018). A cyberattack of devastating proportions is not a matter of if but when (Turak, 2018).

Hints of attacks have already occurred. For example, the Atlanta government was shut down due to the ramson attack (NY Times, March 2018). In the State of Texas, 23 city governments were hit with ransomware. In 2002, a cyber-attack aimed squarely at all 13-domain name systems' root servers almost brought the Internet to its knees. The attack lasted for one hour. If the attack lasted more than an hour, it would have brought the Internet to a standstill. In 2007, the government and banks of Estonia were hit with a denial-of-service attack.

When a massive cyber-attack occurs across the nation, the infrastructure computers will crash due to installed malware. Water, sewage, phone systems, electrical power, and the Internet will be disabled across the nation. People will be unable to use credit cards, do banking transactions, and access government websites. It will be like the aftermath of a hurricane or earthquake, except it extends from the east coast to the west coast. There will be a lack of communication between the government, people, utilities, businesses. The result is a society unable to function.

Is the United States prepared for such a massive cyberattack? No, says a new book by journalist Ted Koppel. The book explains why the Internet is potentially a weapon of mass destruction (Worrall, 2015).

ISSN: 1941-6679-On-line Copy

.

APPENDIX B

Scenario Reading B: the countermeasures/ recovery to a national catastrophic cyber-attack.

The results between a Cat 5 hurricane and a catastrophic cyber-attack are the same: no electricity, no sewage, no water, no communication, no Internet, no banking, no credit card usage.

However, there are differences. With a hurricane or earthquake, there is massive physical destruction and deaths with a long time to recover. A catastrophic cyber-attack has minimal, if any, physical destruction, few if any deaths, and the time to recover is short. The roads/bridges, buildings, equipment will be intact, but data and computer systems will be corrupted. Here are five things people need to know:

1. The duration may last between 4 hours to two weeks. The Denial-of-Service attack on Estonia in 2007 lasted only a few days. For such attacks, there are countermeasures, such as firewalls and adjusting computer configurations.

3. Communications may be the same as a hurricane or earthquake, via ham-radio operators (armatures), cell phones, i-phones, and car or battery radios. Key infrastructure facilities have backup generators for electrical power.

4. Computers will need to be re-configured or restored from backup files. This may take a few days to a few weeks. FEMA advises people to plan to be on their own for two weeks, just like a hurricane or earthquake.

5. If data are corrupted, backup files will need to be restored. Backup files generally are detached from the computers during an attack.

6. Backup gas generators or hand pumps can be placed at gas stations so cars will be able to obtain gas.

7. Stores can still do business with consumers via cash.

ISSN: 1941-6679-On-line Copy

.

APPENDIX C

Survey
Demographic Information

Q1. Age

Q2. Gender: Male Female

Q3. Employment Status

Employed full-time
Employed part-time
Unemployed looking for work
Unemployed not looking for work
Retired
Student
Disabled

Q4. Job Type

Computer Professional/Technician
Computer Security Professional
Computer user on the job/school
Do not use computer on the job/school
Unemployed

Two instruments

Technology Optimism
Indicate your optimism on the following topics by indicating:

Strongly disagree; Disagree; Somewhat disagree; Neither agree nor disagree; Somewhat agree; Agree; Strongly agree.

- New technologies contribute to a better quality of life.
- Technology gives me more freedom of mobility
- Technology makes me more productive in my personal life
- Technology gives people more control over their daily lives

Cyber Self-Efficacy
Compared to others in the U.S. that are similar age as you, answer the following questions. (NOT at all confident; NOT confident; Somewhat NOT confident;

.

Neutral; Somewhat confident; Confidant; Totally confident).

- I can select the appropriate security software for my home computer.
- I can correctly install security software on my home computer.
- I can correctly configure security software on my home computer.
- I can find the information needed if I have problems using security software on my home computer.

Readings Survey

1. How much did you learn, and gain insight form the readings?
   None
   A little
   Good Amount
   Large Amount

2. How would you describe the readings?
   Poor
   Reasonable
   Insightful
   Very well done

3. Did the attack read surprise you as to the extent of disruption?
   Yes
   No
   No opinion

4. Did the countermeasures/response read surprise you as to what can be done to a national attack?
   Yes
   No
   No opinion

.

APPENDIX D

Factor Analysis of 2 data sets
Rotated Component Matrix a

	Data Set 1 (before reading) Total Variance Explained 83.25%		**Data Set 2 (after reading)** Total Variance Explained 86.51%	
	Component		Component	
Item	1	2	1	2
Q5_1	.199	.885	.207	.896
Q5_2	.183	.896	.224	.903
Q5_3	.230	.877	.243	.888
Q5_4	.221	.873	.225	.886
Q31_1	.831	.293	.890	.250
Q31_2	.917	.213	.925	.231
Q31_3	.921	.169	.926	.204
Q31_4	.891	.183	.900	.231

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 3 iterations.

Matrix Items:	Q5	Technology Optimism,	Component 2
	Q31	Cyber Self-efficacy	Component 1

.