Infrastructure Cyber-Attack Awareness Training: Effective or Not?

Garry L. White, Texas State University, San Marcos, USA*

ABSTRACT

The purpose of this study is to provide insight as to how infrastructure countermeasures awareness training will impact individuals dealing with a nationwide catastrophic cyber-attack. Can this awareness training lessen the psychological effect of an attack? This study showed no value for this type of training. Reading about such an attack, the subjects had lower technical optimism and cyber self-efficacy. Reading about infrastructure countermeasures, before or after reading about a cyber-attack, did not improve or maintain the subjects’ optimism and self-efficacy. A possible explanation is that emotional arousal may override or block rational thinking. Another explanation may be that a nationwide attack is towards the infrastructure and not the personal computer. Here the individual lacks any control. Future research needs to look at personal preparation and response training to see if it will help the psychological effects of a catastrophic cyber-attack.

KEYWORDS
Catastrophic Cyber Attack, Countermeasures, Cyber Self-Efficacy, Cyber-Warfare, Technology Optimism, Worry

INTRODUCTION

Cyberwarfare is a weapon of mass “disruption” and can bring down an entire country like the situation that occurred in Estonia, 2007 (Tamkin, 2017; McGuinness, 2007). A 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). According to Rundle, “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). Being more dependent on technology results in more vulnerability. As more information on residents is collected, nation-states or terrorists could incorporate the information into cyberwarfare campaigns.

Cyberwarfare methods include: 1) denial of access to systems and data, 2) exploitation of information for advantage, 3) corrupting information, and 4) destroying information and information systems (Chapple & Seidl, 2015). Corrupting information can also include replacing data with bogus or error filled data. (Rundle, 2019). And cyberwarfare can target civilians and civilian systems (Chapple & Seidl, 2015) as well as military and government systems.
Such a massive attack is coming to the U.S.A. (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, in the western United States, there was a cyber-attack on the power grid (Sussman, 2019). The attack was successful because of a failure to patch a firewall. Is the United States prepared for a massive cyberattack?

There have been warnings. In 2018, Fazzini wrote, “Warnings about a massive cyberattack aren’t new – intelligence officials have raised red flags for years” (Fazzini, 2018). The director of National Intelligence, Dan Coats, warns of an impending “cyber 9/11” (Fazzini, 2018). Corporations and governments will not be the only ones impacted. The USA & UK have been warning of cyber-attacks to homes as well (Kirkpatrick & Nixon, 2018) due to smart technology and the Internet of Things.

Research has indicated that cyberattacks can have a psychological impact (Gandhi et al., 2011, Modic and Anderson, 2015). The public is more likely to respond psychologically to the effects of a cyberattack rather than the cyberattack inconvenience (Gandhi et al., 2011, Minei and Matusitz, 2011). Psychological impact can be anxiety, worry, anger, outrage, and depression (Bada & Nurse, 2020).

**Goal of This Study**

When a devastating cyber-attack occurs, how will the public respond? The goal of this study is to see how to best prepare people psychologically for a cyber-attack. The purpose of some cyber-attacks is to cause panic. The attacker creates chaos in communities by attacking emergency systems (Lee, 2018). Most panic studies deal with physical disasters resulting in death and destruction, not cyberattacks. There is nothing in the literature about worry or panic or optimism resulting from a cyber-attack when it only impacts the ability to function and communicate. Will they worry more, have less technological optimism, and less self-confidence dealing with technology? Understanding the psychological impacts of cyber-attacks are crucial factors in how to best respond to an attack (Bada & Nurse, 2020).

Technology alone cannot completely shield information systems from potential threats. (Rhee, et al. 2012). More effort needs to be focused on “addressing the human dimensions” of information security (Rhee et al., 2012). Gross states: “Further research is required to understand how ... educational and intervention programs might impart the fear/stress reducing skills to cope with cyberterrorism and to improve resiliency, i.e., withstand adverse psychological effects of cyberterrorism, overcome feelings of vulnerability and regain a sense of control” (Gross, et al., 2017).

First, this paper will show the impact of a national catastrophic cyber-attack scenario on four human dimensions: 1) technology optimism, 2) optimistic bias, 3) cyber self-efficacy, and 4) worry. Second, this paper will show whether awareness of infrastructure countermeasures and responses, before and after an attack, restore or maintain these four human dimensions.

**LITERATURE REVIEW**

What Has Happened -- History.

**Estonia:** In 2007, computer networks in the tiny Baltic country of Estonia were disabled in a cyberattack. This was the first cyber-attack in history that affected an entire country (Tamkin, 2017). Online services of banks, media outlets, and government bodies were disabled while massive waves of spam were sent by botnets, and huge amounts of automated online requests overloaded the servers. Cash machines and online banking services were blocked; government employees were unable to communicate with each other via email. Newspapers and broadcasters were unable to deliver the news (McGuinness, 2007).
Georgia: The country of Georgia had a massive cyber-attack in October 2019. Over 15,000 websites were taken offline. The sites affected were banks, courts, local newspapers, and TV stations. General panic was reported to have occurred in the country (Cimpanu, 2019).

Eastern Europe: 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).

USA Prime Target
America is the prime target of international cyberattacks (McDuling, 2014). Most of these attacks appear to originate in the US, but this may be misleading. Attackers often route or proxy their traffic through multiple servers, to make it harder to trace attack origin (McDuling, 2014). As Rep. Jim Langevin, co-chair of the congressional cyber-security caucus states: “the threat of a cyber war against critical U.S. infrastructure looms larger than ever” (Rogers, 2011). Secretary of Defense Panetta states a destructive cyber-terrorist attack could virtually paralyze the nation (Panetta, 2012).

People's Responses
When people feel threatened, their anxiety, fear, unrest, crisis mood, will lead to panic (Brickenstein, 1980). When a disaster occurs, panic could lead to selfish or irrational flight behaviors due to a loss of control, functionality, lack of knowledge and lack of communication. “Lack of control over a situation that is perceived as threatening or dangerous can give rise to feelings of emotional distress, fear and insecurity. Such strong emotions can on occasion lead to irrational behaviour” (Sutherland, 2007). “These are all aspects that can influence how members of the public (psychological) . . . are impacted by an attack” (Bada & Nurse, 2020).

Quarantelli (2001) and Tierney et al. (2006) find that people’s initial response to an emergency is prosocial rather than selfish or irrational flight. Singer (1982) discusses people’s reactions and responses to disasters and the need for disaster planning and training. 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, it disrupts computer systems. Hence, the panic that a cyber-attack generates will be of a different nature, a disruption of the ability to function while infrastructure is still intact. To overcome panic, clear communication from authorities is extremely critical (Loong, 2018). The problem here is with a cyber-attack, clear communication can be blocked. Prior communication, such as awareness training before the cyber-attack may be needed to reassure people.

Response Types
Four responses to a cyber-attack include:

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 a specific risk (Ajzen, 2002). “Self-efficacy is considered not as skills themselves, but as the evaluation of what one can do with skills. It considers a person’s belief in themselves and their abilities” (Bandura, 1991). 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 determines employees’ email-related security behaviors. Yoon et al. (2012) proposed a model that identified self-efficacy as a variable which significantly affects the decision of home wireless network users to implement security features on their networks. They
found that self-efficacy has a significant impact on students’ intentions to practice information security. “This concerns issues such as cyberattacks because it is important that individuals believe that they stand a chance of protecting themselves and responding successfully to an attack’s occurrence” (Bada & Nurse, 2020). In this study, we define self-efficacy as the confidence in using current cyber knowledge and software.

3. **Worry**: Panic disorder is a form of worry (Davey & Wells, 2006). Worrying is perceived as feelings of inability to control the situation, which is a feature of generalized anxiety disorder (GAD) (Davey & Wells, 2006). Worry can become a source of extreme emotional discomfort (Davey & Wells, 2006). It is an attempt to engage in mental problem-solving whose outcome is uncertain but contains the possibility of one or more negative outcomes. Worry relates closely to the fear process (Borkovec, et al., 1983).

**Education/Awareness Training**

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). 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 must build proper security habits (Yoon et al., 2012). The belief is that as more people are informed, the better off society will be when a massive attack does occur. They will be trained, educated and psychologically prepared to deal with an attack. However, repeated awareness training can lose its effectiveness over time (Wolf et al., 2011).

Most business organizations conduct security awareness training to deal with policy, procedures, and tools (Ku et al., 2009; Peltier, 2005; Rotvoid & Landry, 2007). Research about security awareness and education has focused on protective behavior (Britt, 2008; Claar & Johnson, 2012; McLaughlin, 2006; Mensch & Wilkie, 2011; Pollitt, 2005; Puhakainen & Siponen, 2010; Wagley, 2010). The training focuses on the organization’s system instead of a national catastrophic cyber-attack. However, the literature lacks any evidence showing training and education impacting psychological reaction to a national catastrophic cyber-attack.

**Hypotheses**

This study explored subjects reading about a massive national cyber-attack and reading about infrastructure countermeasures (awareness training) and how it impacts a general population’s technology optimism, cyber optimism bias, cyber self-efficacy, and general worry. The readings did not focus on personal computer and personal actions and preparedness. For the reading, physical infrastructures, such as roads and bridges, were not affected.

**Hypothesis 1**: Reading about a Cyber-attack before Awareness Training of Infrastructure Countermeasures-- Group A

Reading a scenario of a national catastrophic cyber-attack will:

- **H1-1a**, lower Technical Optimism.
- **H1-2a**, lower Cyber Self-Efficacy.
- **H1-3a**, increase Worry.

Reading a scenario of countermeasures after reading a scenario of an attack will:

- **H1-1b**, increase Technical Optimism.
H1-2b, increase Cyber Self-Efficacy.
H1-3b, decrease General Worry.
Hypothesis 2: Awareness Training of Countermeasures before reading about a Cyber-attack – Group B

Awareness training of infrastructure countermeasures will:

H2-1a, increase Technical Optimism.
H2-2a, increase Cyber Self-Efficacy.
H2-3a, decrease Worry.

Reading a scenario of national catastrophic cyber-attack after reading awareness training of infrastructure countermeasures will:

H2-1b, not change Technology Optimism.
H2-2b, not change Cyber Self-Efficacy
H2-3b, not change General Worry.

METHODOLOGY

Subjects:
“Internet participants in online studies are a purely self-selected sample of participants and thus maybe 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). They were invited to participate in this research. They were divided into two groups: Group A, countermeasures awareness after attack, and Group B, countermeasures awareness before an attack. They accessed a Qualtrics survey that contained four instruments and two readings. The two readings were 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 ± 17; 49% male, 51% female, and 46% full time employment. Age, gender, employment status, and job type were not considered in this study. Those variables will be used in a future study dealing with demographic impacts.

Four Instruments Used (see Appendix C):
The three instruments were designed with either a 5-point or 7-point Likert scale to indicate level of agreement. For example, strongly agree to strongly disagree. This provided discrete tiered numbers with a restricted range (1 to 5 or 1 to 7).

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

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

General Worry Instrument
The Penn State Worry Questionnaire (PSWQ) represents excessive and/or uncontrollable general worry (Startup & Erickson, 2006). The content was not cyber. It was taken from a published paper by Meyer et al. (1990). The 16-item PSWQ has high internal consistency for both clinical and non-
clinical groups (Molina & Borkovec, 1994). Cronbach’s alpha coefficients have been between 0.88 and 0.95 for clinical samples.

Of the 16 items, seven were selected. The items were selected based on three research paper factor analysis loadings (Brown, 2003; Meyer et al. 1990; Fresco e. al. 2002). For an item to be selected, two of the loading factors had to be greater than .7, and the third had to be greater than .6.

Five phases of this study:

1. **Determine current state (Data Set 0):** The first phase was the administration of the four instruments to determine the current state of worry, optimism, optimistic bias, and cyber self-efficacy. This was to establish a baseline as the control prior to treatments for comparisons. The subjects were then placed in one of two groups, group A or group B.

2. **First Treatment:**
   - Group A read a scenario of a national catastrophic cyber-attack. See Appendix A.
   - Group B read a scenario of countermeasures. See Appendix B.

3. **Determination of state after reading the Scenario A & B (Data Set 1):** After reading the first Scenario, the four instruments were administered again to determine the current state of worry, optimism, optimistic bias, and cyber self-efficacy.

4. **Second Treatment:**
   - Group A read a scenario of countermeasures. See Appendix B.
   - Group B read a scenario of a national catastrophic cyber-attack. See Appendix A.

5. **Determination of state after reading scenario A & B (Data Set 2):** After reading the second Scenario, the four instruments were administered again to determine the current state of worry, optimism, optimistic bias, and cyber self-efficacy.

**Analysis**

Winter & Dodou (2012) wrote a paper on using five-point Likert items with a t-Test (parametric test) and Mann-Whitney-Wilcoxon (MWW) (non-parametric test). They found both tests have similar power. However, Winter & Dodou (2012) found MWW had a power advantage with non-normal distributions. Their conclusion for five-point Likert data were that both tests will not find a significant difference in a population when there is none. This was consistent with Rasmussen (1989). That 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 measures of technology optimism, optimistic bias, self-efficacy, and worry were done to determine if there were differences. If the significant data had skewed or peaked distributions, the non-parametric related-samples Wilcoxon Signed Rank Test was used to confirm the t-Test.

**RESULTS**

**Descriptive Statistics**

Tables 1A & 1B shows the descriptive statistics of the three sets of data for Technical Optimism, Cyber Optimistic Bias, Cyber Self-Efficacy, and General Worry for Groups A and B. 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 was used.
Face Validity of the Readings (Scenarios)

Nunnally & Bernstein (1994) defined face validity as the extent a measure reflects what it is intended to measure. Anastasi (1988), and Nevo (1985) defined face validity as the degree that respondents judge the appropriateness of instrument items. To determine if the two readings were meaningful and appropriate to the subjects, four post-survey questions were given to check the quality and validity of the readings (scenarios). See Table 2.

As shown in Table 2, 63% of the subjects believed they learned a good or large amount and gained good or large insight from the readings. Table 2 also shows 66% judged the readings as insightful.
or very well done. Finally, 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 were analyzed. Except for one value (.78), the Cronbach’s Alphas were over .82, which indicates high internal consistency. The Alpha values were considered “excellent.” See Tables 3A & 3B.

**Table 2. Four reading (scenarios) survey questions**

| Question                                                                 | None 4% | A little 33% | Good Amount 45% | Large Amount 18% | Poor 5% | Reasonable 28% | Insightful 48% | Very well done 18% | Yes 49% | No 40% | No opinion 11% | Yes 51% | No 35% | No opinion 14% |
|--------------------------------------------------------------------------|---------|--------------|-----------------|-----------------|---------|----------------|----------------|-------------------|---------|--------|--------------|---------|--------|--------------|
| 1. How much did you learn and gain insight from the readings?            | None 4% | A little 33% | Good Amount 45% | Large Amount 18% | Poor 5% | Reasonable 28% | Insightful 48% | Very well done 18% | Yes 49% | No 40% | No opinion 11% | Yes 51% | No 35% | No opinion 14% |
| 2. How would you describe the readings?                                  |         |              |                 |                 |         |                |                |                    |         |        |              |         |        |              |
| 3. Did the attack reading surprise you as to the extent of disruption?    |         |              |                 |                 |         |                |                |                    |         |        |              |         |        |              |
| 4. Did the countermeasures response reading surprise you as to what can be done to a national attack? |         |              |                 |                 |         |                |                |                    |         |        |              |         |        |              |

**Table 3a. Reliability -- Cronbach's Alpha for Group A**

| Instrument             | Data Set 0 (before) | Data Set 1 (After first reading) | Data Set 2 (After second reading) |
|------------------------|---------------------|----------------------------------|----------------------------------|
| Technology Optimism    | .929                | .935                             | .945                             |
| Cyber Self-Efficacy    | .928                | .954                             | .957                             |
| General Worry          | .946                | .955                             | .957                             |

**Table 3b. Reliability -- Cronbach's Alpha for Group B**

| Instrument             | Data Set 0 (before) | Data Set 1 (After first reading) | Data Set 2 (After second reading) |
|------------------------|---------------------|----------------------------------|----------------------------------|
| Technology Optimism    | .922                | .957                             | .965                             |
| Cyber Self-Efficacy    | .901                | .944                             | .955                             |
| General Worry          | .946                | .960                             | .967                             |

For this analysis, the factors for each data set 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 .87, 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 Tables 4A & 4B.

Normalization) was performed on each data set to ensure all items of the survey loaded correctly on the factors intended.
Group A cumulative total variance explained through rotation sums of squared loadings for Data Sets 0, 1, 2 were 80.31%, 83.76%, 84.96%, respectively. All Rotated Component Coefficients were >.79, with most >.85. Refer to Appendix D-A for Group A factor analysis.

Group B cumulative total variance explained through rotation sums of squared loadings for Data Sets 0, 1, 2 were 78.78%, 83.95%, 86.82%, respectively. All Rotated Component Coefficients were >.76, with most >.85. Refer to Appendix D-B for Group B factor analysis.

To ensure there were no initial differences between groups A and B, an Independent Samples t-Test was performed between the two groups variables before treatment. There were no significant differences initially between the two groups for Technology Optimism, Cyber Self-Efficacy, and General Worry.

**Paired-Wise t-Test and Mean Plots**

Since an ANOVA treats each data set as coming from different subjects rather from the same subject, Pair-Wise t-Tests were performed. Pair-Wise is used when the difference between the two variables came from the same subject. The subject becomes their own control. If significant, a Plot Means graph was generated and the non-parametric related-samples Wilcoxon Signed Rank Test was used to confirm the t-Test.
Group A: Reading about a Cyber-Attack Before Awareness of Countermeasures

Technology Optimism (H1-1)

Table 5 show the results of a massive cyber-attack lowers technology optimism (Pair 1: $t = 3.395$, $df = 289$, $p < .001$; Cohen’s $d = .134$). However, awareness of countermeasures, after the fact, does not restore technology optimism. Instead, Technology Optimism continued to decrease (Pair 2: $t = 2.292$, $df = 289$, $p < .023$; Cohen’s $d = .085$). See Graph 1.

Table 5. Paired t-Tests for Technology Optimism

|       | Mean differ | Std. Dev | Std. Error Mean | t    | df  | Sig (2-tailed) | Cohen’s d |
|-------|-------------|----------|-----------------|------|-----|----------------|-----------|
| Pair 1| TechOpt_0   | .741     | 3.718           | .218 | 289 | .001           | .134      |
|       | TechOpt_1   |          |                 |      |     |                |           |
| Pair 2| TechOpt_1   | .503     | 3.740           | .220 | 289 | .023           | .085      |
|       | TechOpt_2   |          |                 |      |     |                |           |

Since the data were non-normal, the related-samples Wilcoxon Signed (WS) rank test was performed on both pairs. The first pair had $p < .001$ and the second pair had $p < .003$. WS was consistent with the t-test. The null hypotheses of the differences between OptTech0/1 and OptTech1/2 equals 0 was rejected.

However, the Effect Sizes based on Cohen’s $d$ (.134 & .085) were found to be small, < .2. The Effect was trivial.

Cyber Self-Efficacy (H1-2)

Table 6 and Graph 2 show that reading about the results of a massive cyber-attack lowered cyber self-efficacy (Pair 1: $t = 5.408$, $df = 289$, $p < .001$; Cohen’s $d = .324$). However, awareness of countermeasures, after the fact, does not restore cyber self-efficacy (Pair 2: $t = 1.044$, $df = 289$, $p$...
As Graph 2 indicates, Cyber Self-Efficacy decreased after the reading the scenario of the attack and the awareness scenario failed to restore Cyber Self-Efficacy. The confidence with installing and configuring security software on their computer to deal with the attack decreased.

General Worry (H1-3)

Table 7 shows that General Worry is not impacted by reading about an attack or awareness of countermeasures.

Group B: Awareness of Countermeasures before reading about a Cyber-attack

Technology Optimism (H2-1)

Table 9 shows that awareness training did not change technology optimism (Pair 1: \( t = 1.002, \text{df} = 288, p < .317 \)). However, reading about an attack after awareness training, did lower technology optimism (Pair 2: \( t = 2.545, \text{df} = 289, p < .011; \) Cohen’s d = .084). See Graph 3.

Since the data were non-normal, the related-samples Wilcoxon Signed (WS) rank test was performed on the significant second pair. The second pair had \( p < .029 \). WS was consistent with the t-test. The null hypotheses of the differences between OptTech0/1 and OptTech1/2 equals 0 was rejected. However, the Effect Sizes based on Cohen’s d (.084) was found to be small, < .2. The Effect was trivial.
Table 7. Paired t-Tests for General Worry

|                | Mean Difference | Std. Deviation | Std. Error Mean | t    | df | Sig. (2-tailed) |
|----------------|-----------------|----------------|-----------------|------|----|----------------|
| Pair 1         | Worry_0 - Worry_1 | 0.214          | 3.519           | 0.207| 1.035| 0.317          |
|                | Worry_1 - Worry_2 | 0.224          | 2.639           | 0.155| 1.446| 0.011          |

Table 8. Paired t-Tests for Technology Optimism

|                | Mean Difference | Std. Dev | Std. Error Mean | t    | df | Sig. (2-tailed) |
|----------------|-----------------|----------|-----------------|------|----|----------------|
| Pair 1         | TechOpt_0 - TechOpt_1 | .187    | 3.169           | .186 | 1.002| .317           |
|                | TechOpt_1 - TechOpt_2 | .471    | 3.144           | .185 | 2.545| .011           |

Figure 3. Mean Plots for Technology Optimism

Cyber Self-Efficacy (H2-2)

Table 9 and Graph 4 show that awareness training does not change cyber self-efficacy (Pair 1: t = 0.080, df = 288, p < .936). However, reading about an attack, after awareness training, does lower cyber self-efficacy (Pair 2: t = 2.91, df = 288, p < .004). Effect Size based on Cohen’s d (.094) was found to be small, < .2. The Effect was trivial.

Since the data were non-normal, the related-samples Wilcoxon Signed (WS) rank test was performed on the significant second pair. The second pair had p < .007. WS was consistent with the t-test. The null hypothesis of the differences between Self-Eff_1 and Self-Eff_2 equals 0 was rejected.
As Graph 4 indicates, Cyber Self-Efficacy decreased after reading the scenario of the attack. The awareness training before the attack reading failed to change Cyber Self-Efficacy. The confidence with installing and configuring security software on their computer to deal with the attack decreased.

**General Worry (H2-3)**

Table 10 and Graph 5 show that General Worry decreases with the awareness of countermeasures. However, reading about an attack after awareness training, leaves General Worry the same.

Since the data were non-normal, the related-samples Wilcoxon Signed (WS) rank test was performed on the significant first pair. The first pair had $p < .012$. WS was consistent with the t-test. The null hypotheses of the differences between Worry_0 and Worry_1 equals 0 was rejected. However, the Effect Sizes based on Cohen’s $d$ (.059) was found to be small, $< .2$. The Effect was trivial, and the difference is unimportant.

**Hypothesis Results**

Based on these results, the findings for the hypotheses are as follows:

Hypothesis 1: Reading about a Cyber-attack before Awareness Training of Infrastructure Countermeasures-- Group A
Reading a scenario of a national catastrophic cyber-attack will:

**H1-1a**, lower Technical Optimism. **Significant but Trivial**
**H1-2a**, lower Cyber Self-Efficacy. **Significant but Trivial**
**H1-3a**, increase Worry. Not Significant

Reading a scenario of countermeasures after reading a scenario of an attack will:

**H1-1b**, increase Technical Optimism. **Significant Decrease but Trivial**
**H1-2b**, increase Cyber Self-Efficacy. Not Significant
**H1-3b**, decrease General Worry. Not Significant

Hypothesis 2: Awareness Training of Countermeasures before reading about a Cyber-attack – Group B

Awareness training of infrastructure countermeasures will:

**H2-1a**, increase Technical Optimism. Not Significant
**H2-2a**, increase Cyber Self-Efficacy. Not Significant
**H2-3a**, decrease Worry. **Significant Decrease but Trivial**
Reading a scenario of national catastrophic cyber-attack after reading awareness training of infrastructure countermeasures will:

H2-1b, change Technology Optimism. **Significant Decrease but Trivial**
H2-2b, change Cyber Self-Efficacy **Significant Decrease but Trivial**
H2-3b, change General Worry. Not Significant

**DISCUSSION**

As Rhee et al. (2012) indicated, since technology alone cannot completely protect information systems from potential threats, there needs to be more effort in addressing the human dimensions when dealing with information security events.

**Technical Optimism** decreased before and after reading about a catastrophic cyber-attack on the infrastructure, resulting in the increase in the belief of dangers. After awareness training of countermeasures, Technical Optimism continued to decrease. A possible explanation is that the awareness training stressed the lack of personal control since the control was with the infrastructure. Awareness training did not increase Technical Optimism before or after the attack reading. Findings indicate that awareness of infrastructure countermeasures has no positive impact on Technical Optimism.

**Cyber self-efficacy** decreased after reading about an attack whether awareness training of countermeasures was done before or after. This is consistent with Technical Optimism. It appears a massive cyber-attack will increase the belief of being at greater risk from the dangers of the technical environment. The subjects consciously lost faith in technology and lost their confidence to control the attack’s effect on the internet. This may be explained by the lack of control over the situation.

Their personal computer is not the major target of massive national cyber-attack. It is the infrastructure computers that are the major targets (i.e., ISP, computers controlling the power grid and water systems). They may have realized that much of cyber operations are out of their control because it was infrastructure computers were attacked.

**General Worry** (non-cyber) appears to not be affected by a cyber-attack. This may be due to the PSWQ’s focus on self-feelings in general (non-cyber). This suggests that subjects can differentiate their worry consciously and/or sub-consciously between cyber and non-cyber situations. However, General Worry does decrease after awareness training of countermeasures before reading an attack scenario.

**CONCLUSION**

Will awareness training of countermeasures before or after reading about a cyber-attack provide an immunization effect? Can education override the psychological effect of a catastrophic cyber-attack? Based on these results, the answer is no.

This study shows that awareness training of infrastructure countermeasures has little or no impact on the psychological consequences of a cyber-attack. Considering Sutherland (2007) research, it appears the emotional distress inhibits psychological recovery. Since an attack on cyber infrastructure deals with the subject’s inability to control infrastructure, self-efficacy, the ability and confidence to control, drops (Ajzen, 2002). This can lead to emotional distress and irrational behavior (Sutherland, 2007). This may explain why awareness training has no effect as found in this study.

The outcomes of this study failed to support the value and need for infrastructure awareness training and education before and after reading about a catastrophic cyber-attack. Overall, most findings were non-significant. The few significant findings were trivial as defined by Cohen’s d. Awareness training of infrastructure countermeasures before or after reading about a massive national cyber-attack for a general population appears to be of little value when it comes to internal responses.
for technical optimism, cyber self-efficacy, cyber optimistic bias, and general worry. However, an actual experience, rather than just a reading, may have a greater impact on psychological dimensions.

Reading about a catastrophic cyber-attack did lower technical optimism and cyber self-efficacy. Half of the subjects were surprised about the extent of disruption. It appears the emotional response when reading about a cyber-attack may cause awareness training to be ineffective. A reason for this may be that the countermeasures were for the infrastructure, which is out of the control of the subject. The point here is that awareness training needs to be proactive and focus on local or personal computers. Instead of reassuring people the infrastructure can deal with the massive national cyber-attack, awareness of action and preparation the subject can take may be to show better results with an actual attack.

Another consideration for future research would be intervening variables such as demographics. Age and computer knowledge may have an impact on the effectiveness of awareness training and internal responses.

**Implications**

Singer (1982) discussed people’s reactions and responses to disasters and the need for disaster planning and training. There is a need for more training and education on how to prepare and respond to security incidents before an attack happens. This study used a reading scenario stressing infrastructure countermeasure instead of stressing what the individual can do.

Awareness training and education have traditionally tended to focus on infrastructure systems and protocols, aiming to be reassuring of the security of the infrastructure. Learning how to prevent and respond to security incidents on the individual/local level before incidents happen may improve technical optimism, cyber optimistic bias, cyber self-efficacy, and general worry. These are actions to take to build confidence of what you can control.
ACKNOWLEDGMENT

Funding: this work was supported by the McCoy Faculty Development Fund, Texas State University (2019)

REFERENCES

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. Journal of Applied Social Psychology, 32(4), 665–683. doi:10.1111/j.1559-1816.2002.tb00236.x

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation, and collective reflection; an intervention study. Computers & Security, 29(4), 432–445. doi:10.1016/j.cose.2009.12.005

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

Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cyberattacks. In Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press. doi:10.1016/B978-0-12-816203-3.00004-6

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavior change. Psychological Review, 84(2), 191–215. doi:10.1037/0033-295X.84.2.191 PMID:847061

Bandura, A. (1991). Social cognitive theory of self-regulation. Organizational Behavior and Human Decision Processes, 50(2), 248–287. doi:10.1016/0749-5978(91)90022-L

Borkovec, T., Robinson, E., Pruzinsky, T., & DePree, J. (1983). Preliminary exploration of worry: Some characteristics and processes. Behaviour Research and Therapy, 21(1), 9–16. doi:10.1016/0005-7967(83)90121-3 PMID:6830571

Brickenstein, R. (1980). Individual reactions, summation phenomena and collective reactions. MMW. Munchener Medizinische Wochenschrift, 122(42), 1459–1462. http://libproxy.txstate.edu/login?url=https://search.proquest.com/docview/75441251 ?accountid=5683 PMID:6780834

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

Brown, T. A. (2003, December). Confirmatory factor analysis of the Penn State Worry Questionnaire: Multiple factors or method effects? Behaviour Research and Therapy, 41(12), 1411–1426. doi:10.1016/S0005-7967(03)00059-7 PMID:14583411

Chapple, M., & Seidl, D. (2015). Cyberwarfare: Information Operations in a Connected World. Jones & Bartlett Learning.

Cimpanu, C. (2019). Largest cyber-attack in Georgia’s history link to hacked web hosting provider. ZDNet, Trend Micro. Accessed 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. Journal of Computer Information Systems, 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. doi:10.1287/isre.1070.0160

Davey, G. C. L., & Wells, A. (2006). Worry and Its Psychological Disorders: Theory, Assessment and Treatment. John Wiley & Sons Ltd. doi:10.1002/9780470713143

Dodge, R. C. Jr., Carver, C., & Ferguson, A. (2007). Phishing for user security awareness. Computers & Security, 26(1), 73–80. doi:10.1016/j.cose.2006.10.009

Fazzini, K. (2018). Warnings about a massive cyberattack aren’t new- intelligence officials have raised the red flags for years. CNBC. https://www.cnbc.com/2018/07/24/cyberattack-warnings-from-us-intelligence-officials-are-not-new.html
Fresco, D. M., Heimberg, R. G., Mennin, D. S., & Turk, C. L. (2002, March). Confirmatory factor analysis of the Penn State Worry Questionnaire. *Behaviour Research and Therapy, 40*(3), 313–323. doi:10.1016/S0005-7967(00)00113-3 PMID:11863241

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Social, political, economic, and cultural. *IEEE Technology and Society Magazine, 30*(1), 28–38. doi:10.1109/MTS.2011.940293

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017, March). Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity, 3*(1), 49–58. doi:10.1093/cybsec/tyw018

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

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security, 18*(5), 316–327. doi:10.1108/09685221011095236

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), 371–384. doi:10.1016/j.telpol.2009.03.002

Lee, D. (2018). Warning over ‘panic’ hacks on cities. *BBC News*. Accessed 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. doi:10.17705/1jais.00232

Loong, L. H. (2018). Sing Health cyber-attack: Now what? *SMB World Asia*. Retrieved 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*. https://qz.com/180700/america-is-the-prime-target-of-international-cyberattacks/

McGuinness, D. (2007). *How a cyber-attack transformed Estonia*. *BBC News*. https://www.bbc.com/news/news/39655415

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

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

Meyer, T. J., Miller, M. L., Metzger, R. L., & Borkovec, T. D. (1990). Development and validation of the Penn State Worry Questionnaire. *Behaviour Research and Therapy, 28*(6), 487–495. doi:10.1016/0005-7967(90)90135-6 PMID:2076086

Minei, E., & Matusitz, J. (2011). Cyberterrorist messages and their effects on targets: A qualitative analysis. *Journal of Human Behavior in the Social Environment, 21*(8), 995–1019. doi:10.1080/10911359.2011.588569

Modic, D., & Anderson, R. (2015). It’s all over but the crying: The emotional and financial impact of internet fraud. *IEEE Security and Privacy, 13*(5), 99–103. doi:10.1109/MSP.2015.107

Molina, S., & Borkovec, T. D. (1994). The Penn State Worry Questionnaire: Psychometric properties and associated characteristics. In G. C. L. Davey & F. Tallis (Eds.), *Worrying: Perspectives on theory, assessment, and treatment* (pp. 265–283). John Wiley & Sons, Ltd.

Nevo, B. (1985). Face validity revisited. *Journal of Educational Measurement, 22*(4), 287–293. doi:10.1111/j.1745-3984.1985.tb01065.x

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

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?

Parasuraman, A. (2000). Technology Readiness Index (TRI). *Journal of Service Research, 2*(4), 307–320. doi:10.1177/109467050024001
Peltier, T. (2005). Implementing an information security awareness program. *EDPACS*, 33(1), 1–18. doi:10.1201/1079.07366981/45423.33.1.20050701/89329.1

Pollitt, D. (2005). Energis trains employees and customers in IT security. *Hum Res Manage Digest.*, 13(2), 25–28. doi:10.1108/09670730510586986

Puhakainen, P., & Siponen, M. (2010). Improving employees’ compliance through information systems security training: An action research study. *Management Information Systems Quarterly*, 34(4), 757. doi:10.2307/25750704

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). Elsevier Science Ltd., doi: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(1), 167–170. doi:10.1037/0033-2909.105.1.167

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221–232. doi:10.1016/j.cose.2011.12.001

Rogers, J. (2011). U.S. Power Grid Still Prime Cyber Target. *The Street*. 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*. https://www.washingtonpost.com/world/europe/ukraines-government-key-infrastructure-hit-in-massive-cyberattack/2017/06/27/7d22c7dc-5b40-11e7-9fc6-c7ef4bc58d13_story.html?

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, Sept. 18). How Hackers Could Break Into the Smart City. *Wall Street Journal*, pp. R1, R8-R9.

Schultz, E. (2004). Security training and awareness – fitting a square peg in a round hole. *Computers & Security*, 23(1), 1–2. doi:10.1016/j.cose.2004.01.002

Singer, T. J. (1982). An introduction to disaster: Some considerations of a psychological nature. *Aviation, Space, and Environmental Medicine*, 53(3), 245–250. http://libproxy.txstate.edu/login?url=https://search.proquest.com/docview/80381394?accountid=5683 PMID:6764870

Startup, H. M., & Erickson, T. M. (2006). The Penn State Worry Questionnaire (PSWQ). In *Worry and Its Psychological Disorders: Theory, Assessment and Treatment*. John Wiley & Sons Ltd. doi:10.1002/9780470713143.ch7

Sussman, B. (2019). *Revealed: Details of ‘First of Its Kind’ Disruptive Power Grid Attack*. Secure World, Seguro Group Inc. https://www.secureworldexpo.com/industry-news/first-u.s.-power-grid-attack-details

Sutherland, S. (2007). *Irrationality: The enemy within*. Pinter & Martin.

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

Tierney, K., Beve, C., & Kuligowski, E. (2006). Metaphors matter: Disaster myths, media frames, and their consequences in Hurricane Katrina. *The Annals of the American Academy of Political and Social Science*, 604(1), 57–81. doi: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), 1013–1024. doi:10.1111/risa.12149 PMID:24286290

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

Wagley, J. (2010). Breaches lead to employee training. *Security Management*, 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), 81–86.

Weiser, E. B. (2000). Gender Differences in Internet Use and Internet Application Preferences: A Two-Sample Comparison. *Cyberpsychology & Behavior, 3*(2), 167–178. doi:10.1089/109493100316012

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. https://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.

Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring an information security awareness program. *The Review of Business Information Systems, 15*(3), 9–22. doi:10.19030/rbis.v15i3.5398

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

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.

**ENDNOTE**

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.
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 to 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 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 web sites. 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 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).
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.
2. 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.
3. 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.
4. If data are corrupted, backup files will need to be restored. Backup files generally are detached from the computers during an attack.
5. Backup gas generators or hand pumps can be placed at gas stations so cars will be able to obtain gas.
6. Stores can still do business with consumers via cash.
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

Three 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.

Penn State Worry Questionnaire

Rate each of the following statements on a scale of 1 (“not at all typical of me”) to 5 (“very typical of me”). Please do not leave any items blank.
• My worries overwhelm me
• Many situations make me worry
• I know I should not worry about things, but I just cannot help it.
• I am always worrying about something.
• I notice that I have been worrying about things.
• Once I start worrying, I cannot stop
• I worry all the time.

Readings Survey

1. How much did you learn, and gain insight from 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-A

Group A Factor Analysis of 3 data sets

| Gr A Control data | Gr A Cyber-attack | Gr A Awareness |
|-------------------|-------------------|----------------|
| Data Set 0 (before) | Data Set 1 (first reading) | Data Set 2 (second reading) |

| Q5_1 | Q5_2 | Q5_3 | Q5_4 | Q19_1 | Q19_2 | Q19_3 | Q19_4 | Q19_9 | Q19_10 | Q19_11 | Q19_12 | Q19_13 | Q19_14 | Q19_15 |
|------|------|------|------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| -0.54 | 0.113 | 0.894 | 0.148 | -0.034 | 0.133 | 0.144 | 0.906 | -0.006 | 0.186 | 0.136 | 0.097 | -0.041 | 0.188 | 0.131 | 0.879 |
| -0.012 | -0.167 | 0.887 | 0.131 | -0.012 | 0.167 | 0.887 | 0.210 | -0.066 | -0.120 | 0.888 | 0.168 | -0.064 | -0.113 | 0.888 | 0.168 |
| -0.064 | 0.113 | 0.888 | 0.168 | -0.064 | 0.113 | 0.888 | 0.168 | -0.066 | -0.120 | 0.887 | 0.210 | -0.066 | -0.120 | 0.887 | 0.210 |
| 0.087 | 0.181 | 0.114 | 0.167 | 0.078 | 0.191 | 0.141 | 0.096 | 0.106 | 0.096 | 0.129 | 0.120 | 0.098 | 0.119 | 0.123 | 0.083 |
| 0.078 | 0.191 | 0.141 | 0.096 | 0.098 | 0.119 | 0.123 | 0.083 | 0.106 | 0.096 | 0.129 | 0.120 | 0.098 | 0.119 | 0.123 | 0.083 |
| 0.089 | 0.123 | 0.236 | 0.190 | 0.089 | 0.123 | 0.236 | 0.190 | 0.089 | 0.123 | 0.236 | 0.190 | 0.089 | 0.123 | 0.236 | 0.190 |
| 0.070 | 0.118 | 0.174 | 0.161 | 0.070 | 0.118 | 0.174 | 0.161 | 0.070 | 0.118 | 0.174 | 0.161 | 0.070 | 0.118 | 0.174 | 0.161 |
| 0.089 | 0.123 | 0.117 | 0.919 | -0.046 | 0.873 | 0.190 | 0.203 | -0.033 | 0.919 | 0.149 | 0.202 | -0.007 | 0.926 | 0.119 | 0.144 |
| 0.048 | 0.102 | 0.132 | 0.901 | 0.883 | 0.065 | 0.022 | 0.006 | 0.894 | 0.040 | 0.017 | 0.003 | 0.825 | 0.031 | 0.003 | 0.020 |
| 0.112 | 0.077 | 0.068 | 0.049 | 0.045 | 0.895 | 0.009 | 0.050 | 0.024 | 0.049 | 0.036 | 0.019 | 0.089 | 0.006 | 0.088 | 0.011 |
| 0.114 | 0.070 | 0.089 | 0.039 | 0.024 | 0.870 | 0.027 | 0.055 | 0.028 | 0.078 | 0.027 | 0.055 | 0.024 | 0.090 | 0.039 | 0.024 |
| 0.116 | 0.080 | 0.092 | 0.044 | 0.042 | 0.853 | 0.092 | 0.044 | 0.042 | 0.087 | 0.049 | 0.041 | 0.058 | 0.087 | 0.049 | 0.041 |

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. a Rotation converged in 5 iterations.

Total Variance Explained 80.31% Total Variance Explained 83.76%
Total Variance Explained 84.96%
Matrix Items: Q5 | Technical Optimism,
Q29 | Cyber Self-efficacy
Q11 | Worry
APPENDIX D-B

Group A Factor Analysis of 3 data sets

| Gr A Control data | Gr A Cyber-attack | Gr A Awareness |
|-------------------|-------------------|----------------|
| Data Set 0 (before) | Data Set 1 (first reading) | Data Set 2 (second reading) |

**Total Variance Explained 80.31%**  
**Total Variance Explained 84.96%**  
**Total Variance Explained 83.76%**

Matrix Items:  
Q5  
Q29  
Q11  
Technical Optimism,  
Cyber Self-efficacy,  
Worry

Garry L. White is an Associate Professor in the Computer Information Systems department at Texas State University in San Marcos, Texas. He holds a MS in Computer Sciences from Texas A & M University – Corpus Christi and a PhD in Information Systems Education from The University of Texas at Austin. Professional Certifications from the Institute of Certified Computer Professionals (ICCP) include C.D.P, C.C.P., C.S.P. and Expert Certified in Security Systems. He also holds the Certified Information Systems Security Professional (CISSP). Research interests and work are in the areas of human factors with computer technology, infrastructure security, Internet security, privacy, and global assurance. He has published papers in journals such as the Journal of Computer Information Systems and Journal of Information Systems Education. He was a guest editor for a special issue of the Journal of Information Systems Education; Global Information Security and Assurance in IS Education.