


5-2023

**Predicting the PEBCAK: A quantitative analysis of how cybersecurity education, literacy, and awareness affect individual preparedness.**

Annie Goodman

Follow this and additional works at: [https://digitalcommons.unomaha.edu/university\\_honors\\_program](https://digitalcommons.unomaha.edu/university_honors_program)

 Part of the [Emergency and Disaster Management Commons](#), [Information Literacy Commons](#), [Other Computer Sciences Commons](#), and the [Science and Technology Studies Commons](#)

Please take our feedback survey at: [https://unomaha.az1.qualtrics.com/jfe/form/SV\\_8cchtFmpDyGfBLE](https://unomaha.az1.qualtrics.com/jfe/form/SV_8cchtFmpDyGfBLE)

**Predicting the PEBCAK: A quantitative analysis of how cybersecurity education, literacy, and awareness affect individual preparedness.**

**Introduction**

Cybersecurity seems like a faraway concept to many people, often evoking images from *The Matrix*, someone frantically coding on a green-text screen trying to gain access to a network. This, however, is not how most hackers gain access. A startling majority of cases of data breaches and cyber-attacks are caused by an individual negligently accessing malware through an email or other means. Phishing emails work this way and evoke an image just like their name; the hacker drops some bait in the form of a fake email asking for login information, credit card numbers, or something else entirely, and then they wait for someone to click on a link or fill out a form.

For some, their knowledge of cybersecurity requirements or best practices is limited to an onboarding training or password requirements when they sign up for a new website. There is no standardization of education, nor is there standard training for all people interacting with computers and technology. Coupled with the rapid expansion of diversity in technology, this leads to an interesting question of an individual's cybersecurity preparedness or posture. If individuals are to be the first line of defense and the weakest link in the proverbial cybersecurity chain, then their education, literacy, awareness, and preparedness in that area is of critical importance to researchers. Additionally, because most people utilize technology at work, their own adherence to best practices at home may inform how they utilize them at work. A person's laxity could even have direct effects on their work's cybersecurity by introducing hazards if they use their personal devices for work, plug them in to their work computer, or connect them to a corporate network.

Therefore, the goal of this work is to survey a varied sample population across various criteria to determine their relevant cybersecurity education/training, literacy, awareness, and preparedness and then to perform regression analysis to determine their relationships. At an individual level, understanding the influence of education/training, literacy, and awareness on their overall adherence to best preparedness factors will help others understand where people may be lacking, or where increased knowledge doesn't seem beneficial. This will help future researchers to augment existing measures to strengthen individuals' defensive abilities and to determine where gaps may exist due to a lack of one of the preceding factors.

### **Literature Review**

Cybersecurity is a growing field and there are many dedicated research efforts to determine how to train people to improve their cybersecurity and to comply with best practices. These efforts hinge on a general sense of consensus (rightly so) that people do not generally like the inconvenience of securing their information, of taking extra steps to access or audit it regularly, and of learning and remembering standard practices. It is widely understood that the weakest link in every system is the user who can fall for any number of traps and introduce malware or other hazards to the network or system they are using. Many people also do not understand the dangers they are in despite knowing that they are failing to uphold the best available cybersecurity practices. For the purposes of this work, relevant adjacent research includes the effects of some demographic data and personality traits on individual cybersecurity behaviors and the efficacy of training in enterprise settings to encourage compliance with cybersecurity policies.

Personality is an interesting and applicable focus to my research but much of the existing scholarship doesn't quite meet the criteria I am looking to establish. One area of consensus and depth is in whether certain behaviors or personality trait may affect the compliance of people to a given training program or policy.<sup>1</sup> Generally, it seems, that people's impulsivity and risk-tolerance may inform their willingness to accept cybersecurity risks even when they are aware of their risky behavior.<sup>2</sup> However, much of this data is flawed because it is drawn from primarily young college students who have a different relationship with technology, risk, and security than older members of the workforce.<sup>3</sup> Existing research notes these predictive factors such as lack of awareness and risky behavior and urges greater awareness and training. The issue with this is that they do not address the efficacy of training outside of enforced policies in the workplace or school setting.

In short, while many students or employees may exhibit potentially risky behaviors, most of their cybersecurity requirements on enterprise equipment will be monitored and enforced.<sup>4</sup> This is relevant because psychological or demographic factors may be necessary to control against to narrow down the actual effects of awareness and literacy on individual cybersecurity posture. My goal is to determine whether awareness, training, and associated literacy change people's unenforced behavior at home. Further, I will provide discussion later that there may be a causal mechanism or, at least, a correlation between increased security policies in the workplace and laxity at home due to a form of burn-out that leads people to unintentionally

---

<sup>1</sup> Hadlington, "Human Factors in Cybersecurity; Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours."

<sup>2</sup> Kennison and Chan-Tin, "Taking Risks With Cybersecurity."

<sup>3</sup> Hadlington, "Human Factors in Cybersecurity; Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours"; Kennison and Chan-Tin, "Taking Risks With Cybersecurity."

<sup>4</sup> Stiller and LeBlanc, "From Computer Literacy to Cyber-Literacy."

devalue the importance of their data in their own minds. This project is not intended to necessarily explain the persuasive aspects of corporate education/training efforts, nor is it meant to provide recommendations for changing these to improve individual compliance in enterprise settings or at home. This paper is focused wholly on measuring the influence of factors on individual preparedness and then some discussion on how changing those could affect outcomes generally.

It makes sense that enterprise operations are the focus of cybersecurity because, typically, they are the ones who are most at risk for major-scale cyber-attacks. The goal of the research, generally falls into one of two areas, introduced hazards and the effectiveness of training on compliance.<sup>5</sup> Introduced hazards includes things like medical devices, personal electronics, and other devices that employees may connect to enterprise devices or networks that could introduce a danger.<sup>6</sup> Medical devices are often overlooked but, necessarily, have little encryption and can transmit significant data, depending on the type of device. Newer models of hearing aids can store, transmit, and process data which is intended to improve the settings of the device to better support the needs of the hard-of-hearing person but, should sensitive data, like from a secret or proprietary meeting, be transmitted, it could pose a major security threat.<sup>7</sup> Further, the connection of medical devices to cell phones introduces further dangers such as employees bringing phones into spaces where they really should be prohibited, plugging them into company devices to charge, or even wearing GPS tracking smartwatches and revealing the location of a

---

<sup>5</sup> Reddy and Reddy, "A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies."

<sup>6</sup> Mohan, "Cyber Security for Personal Medical Devices Internet of Things."

<sup>7</sup> Reddy and Reddy, "A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies."

secret military base.<sup>8</sup> These are all generally able to be remedied with policy which requires training and compliance from employees.

The other focus of enterprise cybersecurity operations research is on training efficacy in ensuring compliance with policy. Most companies have some level of cybersecurity policy that is inherently enforced by their systems.<sup>9</sup> This could include private networks, two-factor authentication, and minimum password standards. However, many policies, such as not bringing personal devices into the office, not utilizing external storage media, or not using webcams in certain areas are left up to the training and compliance of the employees using the devices. There is much research, and little consensus, on what make a training program effective at getting compliance. Some methods do include, however, making the program applicable to the student's interests, teaching broad concepts of cyber and computer literacy before explaining specific policies, providing justifications and examples for why policies are necessary, and repetition of lessons.<sup>10</sup> One significant pedagogical shift made to improve training and compliance was a shift from computer literacy to cyber literacy.<sup>11</sup> Essentially, a shift in the training program from simply using a computer, to interacting with the online community, being critical of media you are consuming, and other technological ethical lessons. While computer literacy, especially for non-standard/specialized systems, is still critical, a transition to cyber literacy concepts helps students learn practical uses for their technology.<sup>12</sup> One study posited a way to bring this type of cyber literacy into the home to fill the gaps for people who are not heavy computer users at

---

<sup>8</sup> Alex Hern, "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases | GPS | The Guardian"; Mohan, "Cyber Security for Personal Medical Devices Internet of Things."

<sup>9</sup> Reddy and Reddy, "A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies."

<sup>10</sup> AlDaajeh et al., "The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education"; Caldwell, "Making Security Awareness Training Work."

<sup>11</sup> Stiller and LeBlanc, "From Computer Literacy to Cyber-Literacy."

<sup>12</sup> Stiller and LeBlanc.

work.<sup>13</sup> However, there are fundamental flaws to requiring training at the Internet Service Provider (ISP) level.<sup>14</sup> To name just a few, requiring standardized training isn't equitable to people who may have less education or capability to understand, people are unlikely to be receptive to mandates in their home, especially for something so critical to their connection to the world, and there are plenty of people in the world who do not utilize home internet but rather rely on mobile phones, public libraries, and other resources who would still be missed.

Improving training has been proven to increase understanding and compliance with company policies but, because these are relatively easily monitored, the connection to individual's personal cybersecurity remains unknown. This leads into the focus of my research project which aims to determine if people's cyber literacy and awareness affects their at-home utilization of technology which, as evidenced by some of the research in introduced hazards, could be critical to maintaining the safety of enterprise systems. Further, based on my survey data collection, I will attempt to explain some of the implications of lax home cybersecurity and provide reasonable, implementable, solutions to commonly faced issues. My goal is to consider both computer and cyber literacy and cybersecurity awareness to get a clear picture of people's existing interaction level with computers and use that to determine how prepared they may be overall. This will address critical gaps in existing literature to determine if training in the workplace translates to the home, to determine if increasing awareness is really a worthy goal, and to shift the narrative from corporate mandate to a people-focused approach.

---

<sup>13</sup> Kritzinger and von Solms, "Cyber Security for Home Users."

<sup>14</sup> Kritzinger and von Solms.

## **Research Design**

The variables of interest for this project are all related to individual cybersecurity. They are grouped into Training, Literacy, Awareness, and Preparedness. The goal with these variables is to discuss whether any specific relationship exists between the first three and Preparedness.

Cybersecurity preparedness is a critical variable that is not often measured at the individual level, despite the consensus of existing scholarship that individuals are the weakest link in the security chain. As more and more systems are computerized, integrated, and automated, ensuring that the individuals who use and interact with them are effectively trained, aware, and prepared to handle the potential for cyber threats is of the utmost importance.

### **Variables:**

#### *Education, Employment, & Training*

The goal of the section on education, employment, and training is to determine, generally, the potential correlation or effects of those factors on an individual's literacy, awareness, and preparedness. This can also be controlled for to determine if other factors are related to each other or if the causal relationship can be explained away by someone's education, training, or employment. The questions in this section are adapted from general demographics surveys as well as Farooq et. al. 2019. While the Farooq paper focused on human compliance and adoption of corporate socialized responsibility, their ideals help to develop several of the questions listed in Table 1. Additionally, due to my work in a security conscious field, I also wanted to inquire about people's interactions with higher levels of security than the average job. In this, my goal was to determine if higher security jobs had an influence on people's behavior at home.



### *Literacy*

For the purposes of this paper, I have combined the concepts of computer literacy and cyber literacy into one measurement to determine how much an individual knows about the device and its general functions and how confident they are in executing those functions. Traditionally, computer literacy has been measured in a laboratory setting by asking individuals to execute different tasks on the computer such as renaming files, operations in the settings menus, and more. Cyber literacy is generally more focused on the applicable uses of technology. To measure both, in this section, I asked a variety of questions adapted from scholarship which can be found in Table 2.<sup>15</sup> However, to reduce any potential confounds, I removed questions relating to computer/cyber ethics such as those pertaining to finding reputable sources, appropriate social media use, and the like.

### *Awareness*

Awareness, in cybersecurity, can be difficult to measure due to the vast and varied areas in which cybersecurity is applicable. For the purposes of this paper, I chose to assess people's general awareness of recent cybersecurity news, best practices, and concepts. These were selected from a variety of sources including cybersecurity quizzes and lists of the most prolific data breaches.<sup>16</sup> To ensure the emphasis remained on individual cybersecurity, the data breaches I selected all affected common consumer companies that were breached over the last few years. Additionally, because many people are unaware of the role of individuals in corporate data

---

<sup>15</sup> Julian Fraillon et al., "IEA International Computer and Information Literacy Study 2018 - Assessment Framework"; Olney and Bakhtiari, "Assessing Computer Literacy of Adults with Low Literacy Skills"; Johnson, Bartholomew, and Miller, "Improving Computer Literacy of Business Management Majors."

<sup>16</sup> Kritzinger and von Solms, "Cyber Security for Home Users"; Hadlington, "Human Factors in Cybersecurity; Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours"; Caldwell, "Making Security Awareness Training Work"; Reddy and Reddy, "A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies."

breaches, I included questions that address individual awareness of that role. All awareness questions can be found in Table 3.

### *Preparedness*

The focus of the cybersecurity preparedness section is to determine how many standard cybersecurity recommendations individuals are implementing on their personal devices. To that end, I adapted questions from several sources and attempted to standardize them so they would be applicable for many devices as there is significant variation in what devices people use daily.<sup>17</sup> Preparedness factors are important measures of the ways people interact with their devices, data, and storage, they can greatly impact the resilience of the individual and their family when recovering from a data breach, loss, or other disruption. The goal of this overall project is to compare which of the previous factors impact/improve an individual level of preparedness and then analyze ways to intentionally improve preparedness.

### **Methods of Analysis**

Training/education data will be used qualitatively or scored on a binary yes/no to be compared according to the hypotheses below. All other data will receive a score based on the scoring information in Tables 1-4. The applied scores were selected based either on a binary, a range of scores coded for confidence intervals, or along a gradient from least prepared to most prepared efforts. Each section will be totaled for overall analysis of the variables and individual questions that show additional trends may also be utilized. Each hypothesis will be evaluated as a single-variable regression, then with controls based on other relevant factors.

### *Assumptions:*

---

<sup>17</sup> Kritzinger and von Solms, “Cyber Security for Home Users”; “Search Data Security Breaches”; “Top Scams to Watch out for in 2023, According to the Better Business Bureau”; “Cybersecurity Quizzes”; Farooq et al., “Assessing Human Factor in the Adoption of Computer-Based Information Systems as the Internal Corporate Social Responsibility.”

1. As individuals' education increases, they will be more likely to meet one of the other education/training criteria and therefore have more exposure to cybersecurity topics.

*An aside on the interactions of the following variables*

The purposes of this study are to establish some baseline interactions between the variables listed below. Some variables will be considered as both independent and dependent variables to support the hypotheses listed below and to best explain the interactions of the different human factors relating to cybersecurity.

*Hypotheses:*

In general, higher education requires more interaction with computers and specialized software as well as more emphasis on problem solving and independence. Most employment today also requires some interaction with computer and often comes with additional training on cybersecurity topics. Therefore, I am expecting a positive relationship between education/training and literacy because people who have more education/training are not only more likely to have used computers more frequently but are also more likely to have received instruction on how to use them or been required to complete specific tasks with them.

**H1: As individuals' education and training increases, they will be more likely to be more literate on cybersecurity topics.**

Higher education and employer training generally includes some reference to current or relevant threats. Given recent increases in cyber threats, training could generally be expected to include

information related to different types of threats and cybersecurity information<sup>18</sup>. Therefore, I am expecting a positive relationship between education/training and awareness because people who have more education/training are more likely to have received instruction on general current events or relevant computer topics related to their job or schooling which would likely increase their overall awareness.

**H2: As individuals' education and training increases, they will be more likely to be more aware of cybersecurity issues.**

Literacy and awareness do not always translate, however, to actions. Knowing how to utilize a computer and how to implement some cybersecurity practices as well as being aware of recent trends in cybersecurity, I suspect, may increase individuals' feelings of security despite not actually putting them into effect. Also, as the complexity of the recommendations and difficulty with implementing them increases, people become increasingly frustrated with them<sup>19</sup>. So, I argue, that people with increased literacy and awareness are less likely to be prepared against cybersecurity threats due to both a false sense of security that their data is unlikely to be targeted and a type of burnout due to increasing complexity of requirements and security recommendations. I plan to discuss these explanations with information from existing research along with my data analysis.

---

<sup>18</sup> Reddy and Reddy, "A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies"; Hadlington, "Human Factors in Cybersecurity; Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours."

<sup>19</sup> Oh et al., "Measurement of Digital Literacy Among Older Adults"; Kritzinger and von Solms, "Cyber Security for Home Users."

**H3: As individuals' literacy and awareness increases, they will be less likely to be prepared.**

There is little consensus in existing research about the effectiveness of training and education on actual individual preparedness because much of the education and training is job specific or is too cumbersome to apply to individual measures<sup>20</sup>. There are some measures, like real-world examples, application exercises, and repetition, that are agreed to increase adoption and understanding in the workplace, but no further research has been done into how those changes may affect the individual's preparedness. As such, I believe that there will be no correlation between education/training and preparedness levels because of causal relationships discussed in existing scholarship.

**H4: As individuals' education level changes, there will be no effect on preparedness.**

## **Results & Analysis**

**H1: As individuals' education and training increases, they will be more likely to be more literate on cybersecurity topics.**

Hypothesis 1 was evaluated using a simple linear regression, selected results can be found in the tables below.

---

<sup>20</sup> Caldwell, "Making Security Awareness Training Work."

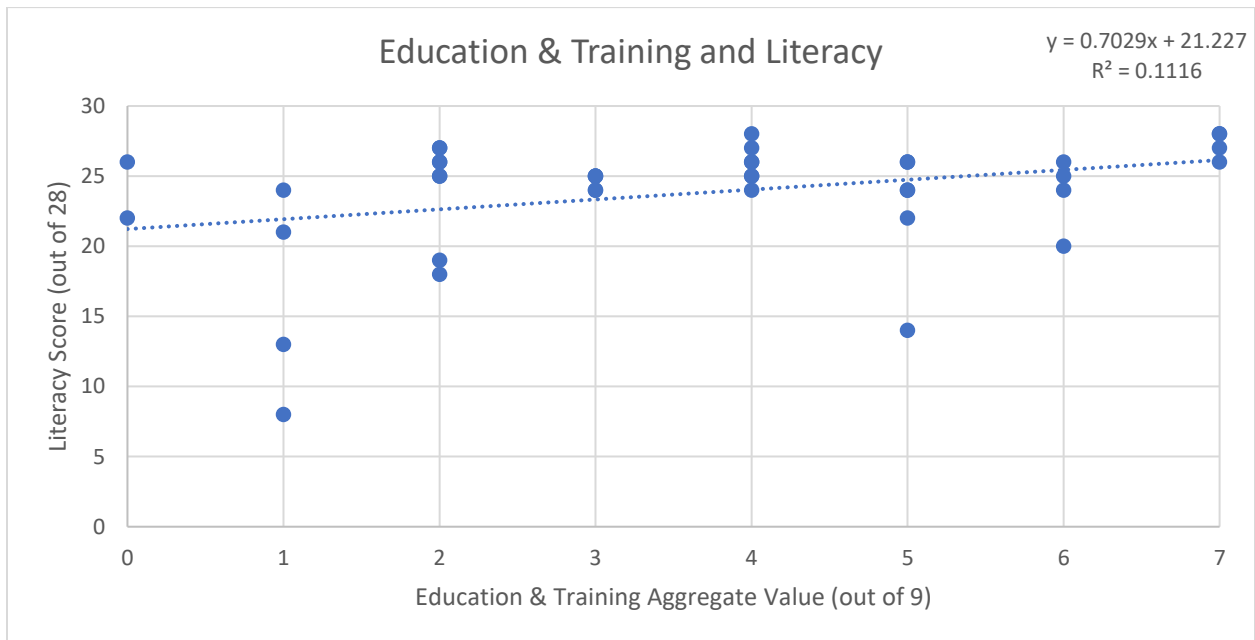
**Table 1: Descriptive Statistics for the Aggregate Education/Training Value and Literacy**

| <i>Score</i>                              |              |                                   |               |
|---|--------------|-----------------------------------|---------------|
| <i>Aggregate Education/Training Value</i> |              | <i>Literacy Score (out of 28)</i> |               |
| <i>(out of 9)</i>                         |              |                                   |               |
| <b>Mean</b>                               | <b>3.625</b> | <b>Mean</b>                       | <b>23.775</b> |
| <b>Mode</b>                               | <b>2</b>     | <b>Mode</b>                       | <b>26</b>     |
| <b>Standard Error</b>                     | <b>0.318</b> | <b>Standard Error</b>             | <b>0.668</b>  |
| <b>Minimum</b>                            | <b>0</b>     | <b>Minimum</b>                    | <b>8</b>      |
| <b>Maximum</b>                            | <b>7</b>     | <b>Maximum</b>                    | <b>28</b>     |
| <b><i>N</i></b>                           | <b>40</b>    | <b><i>N</i></b>                   | <b>40</b>     |

**Table 2: Aggregate Values of Education & Training for Literacy Scores**

|                               |                           |                              |                       |
|-------------------------------|---------------------------|------------------------------|-----------------------|
| <b>R Square</b>               | <b>0.11157159</b>         |                              |                       |
| <b>Standard Error</b>         | <b>4.03671437</b>         |                              |                       |
| <b><i>N</i></b>               | <b>40</b>                 |                              |                       |
|                               | <b><i>Coefficient</i></b> | <b><i>Standard Error</i></b> | <b><i>P-value</i></b> |
| <b><i>Literacy Scores</i></b> | <b>0.703</b>              | <b>0.322</b>                 | <b>0.035</b>          |

Hypothesis 1 stated above expected a direct relationship between education/training values and literacy scores. The descriptive statistics are presented in Table 1 on the previous page. The primary descriptive statistic of interest is the Mode of Education/Training which was 2. When reviewing the data set, it became clear that the mode of '2' generally indicates an education score/code of '1' (in college or some college completed) with one of the other factors (employment in IT, college major/focus in computers, or cybersecurity training). Then, looking at the simple linear regression results in Table 1, the data found was statistically significant because the P-value was less than 0.05 ( $p=0.035$ ). The coefficient of Literacy Scores was 0.703, suggesting that for each point increase in education/training, Literacy Scores would increase by 0.703. This is consistent with the hypothesis which expected a positive coefficient value indicating an increase in literacy as education and training increased.



**H2: As individuals' education and training increases, they will be more likely to be more aware of cybersecurity issues.**

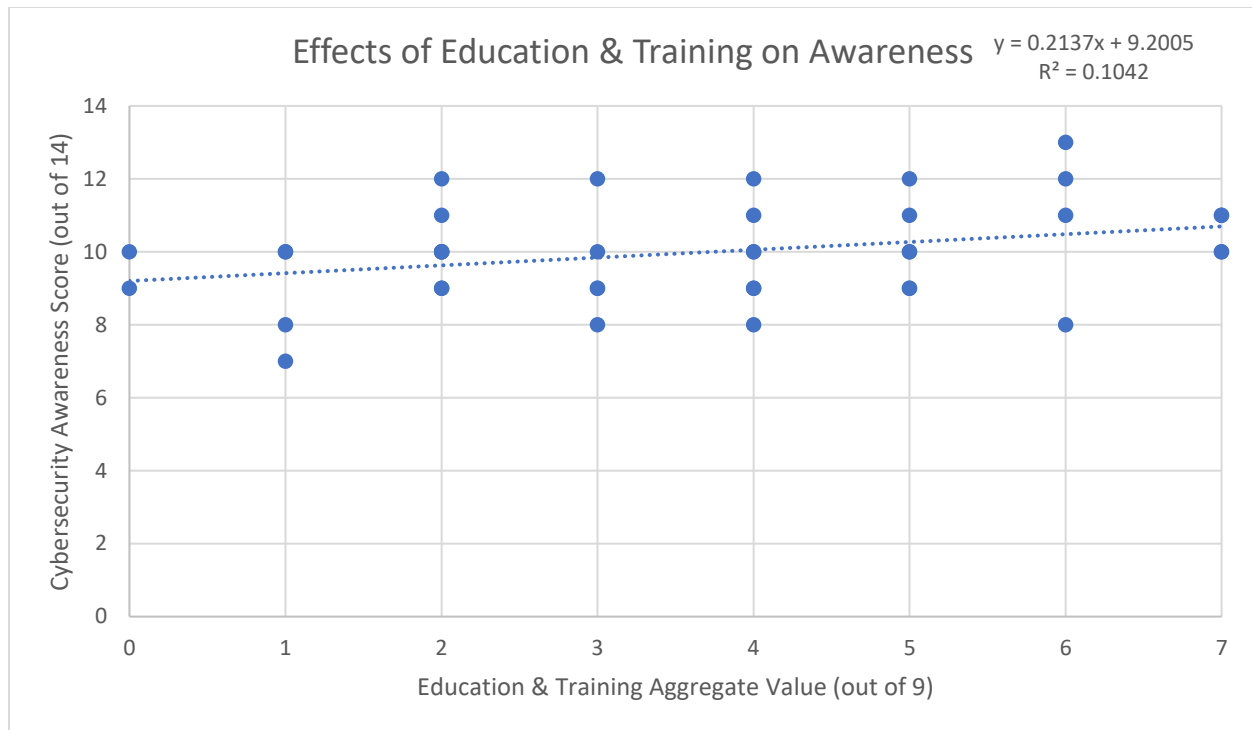
*Table 3: Descriptive Statistics for the Aggregate Education/Training Value and Awareness*

| <i>Scores</i>                             |              |                                    |                   |
|---|--------------|------------------------------------|-------------------|
| <i>Aggregate Education/Training Value</i> |              | <i>Awareness Score (out of 14)</i> |                   |
| <i>(out of 9)</i>                         |              |                                    |                   |
| <b>Mean</b>                               | <b>3.625</b> | <b>Mean</b>                        | <b>9.975</b>      |
| <b>Mode</b>                               | <b>2</b>     | <b>Mode</b>                        | <b>10</b>         |
| <b>Standard Error</b>                     | <b>0.318</b> | <b>Standard Error</b>              | <b>0.21027302</b> |
| <b>Minimum</b>                            | <b>0</b>     | <b>Minimum</b>                     | <b>7</b>          |
| <b>Maximum</b>                            | <b>7</b>     | <b>Maximum</b>                     | <b>13</b>         |
| <i>N</i>                                  | <b>40</b>    | <i>N</i>                           | <b>40</b>         |

*Table 4: Aggregate Values of Education & Training for Awareness Scores*

|                         |                    |                       |                |
|-------------------------|--------------------|-----------------------|----------------|
| <b>R Square</b>         | <b>0.10415908</b>  |                       |                |
| <b>Standard Error</b>   | <b>1.275174162</b> |                       |                |
| <i>N</i>                | <b>40</b>          |                       |                |
|                         | <i>Coefficient</i> | <i>Standard Error</i> | <i>P-value</i> |
| <i>Awareness Scores</i> | <b>0.214</b>       | <b>0.102</b>          | <b>0.042</b>   |





Hypothesis 2 stated above expected a direct relationship between education/training values and cybersecurity awareness scores. The descriptive statistics are presented in Table 3 on the previous page. Then, looking at the simple linear regression results in Table 4, the data found was statistically significant because the P-value was less than 0.05 ( $p=0.042$ ). The coefficient of Awareness Scores was 0.214, suggesting that for each point increase in education/training, Awareness Scores would increase by 0.214 points. This is consistent with the hypothesis which expected a positive coefficient value indicating an increase in literacy as education and training increased. However, given the small coefficient and closer-to-.05 P-value, this is not a strong correlation and does not provide strong evidence for this relationship.

**H4: As individuals' education level changes, there will be no effect on preparedness.**

**Table 7: Descriptive Statistics for the Aggregate Education/Training Value and Preparedness**

| <i>Scores</i>                             |              |  |               |
|---|--------------|--|---------------|
| <i>Aggregate Education/Training Value</i> |              | <i>Preparedness Scores (out of 20)</i> |               |
| <i>(out of 9)</i>                         |              |  |               |
| <b>Mean</b>                               | <b>3.625</b> | <b>Mean</b>                            | <b>12.625</b> |
| <b>Mode</b>                               | <b>2</b>     | <b>Mode</b>                            | <b>14</b>     |
| <b>Standard Error</b>                     | <b>0.318</b> | <b>Standard Error</b>                  | <b>0.420</b>  |
| <b>Minimum</b>                            | <b>0</b>     | <b>Minimum</b>                         | <b>7</b>      |
| <b>Maximum</b>                            | <b>7</b>     | <b>Maximum</b>                         | <b>19</b>     |
| <i>N</i>                                  | <b>40</b>    | <i>N</i>                               | <b>40</b>     |

**Table 8: Aggregate Values of Education & Training for Preparedness Scores**

|                            |                    |                       |                |
|----------------------------|--------------------|-----------------------|----------------|
| <b>R Square</b>            | <b>0.024</b>       |                       |                |
| <b>Standard Error</b>      | <b>2.659</b>       |                       |                |
| <i>N</i>                   | <b>40</b>          |                       |                |
|                            | <i>Coefficient</i> | <i>Standard Error</i> | <i>P-value</i> |
| <i>Preparedness Scores</i> | <b>0.206</b>       | <b>0.212</b>          | <b>0.338</b>   |

Hypothesis 4 stated above expected no relationship between education/training values and preparedness scores. Then, looking at the simple linear regression results in Table 8, the data found was not statistically significant because the P-value was greater than 0.05 ( $p=0.338$ ). The coefficient of Preparedness Scores was 0.206, suggesting that for each point increase in education/training, Preparedness Scores would have increased by 0.206 points. This data is consistent with the hypothesis which expected no statistically significant relationship between education/training and overall preparedness.

### **Implications of Hypothesis Data**

H1, 2, and 4 were found to be correct hypotheses. H1 & 2 were both positively correlated indicating that increased education/training was associated with increases in individuals' literacy and awareness. In terms of causality, this would make sense as education and training are often associated with increased computer usage which would reasonably increase literacy as well as with increased interaction with current events which often include cybersecurity-related events. Hypothesis 4, which predicted no relationship between education and training and preparedness was also found to be correct due to a lack of statistically significant correlation between the variables. This also makes sense due to the ways that education and training are coded. Increased education does not always mean more functional implementation of cybersecurity preparedness measures.

In terms of implications for this body of research, it could be extrapolated that increasing education and training for individuals can help improve their overall computer and cyber literacy and awareness of cybersecurity topics and events. However, more must be done to improve the actual implementation that individuals do on their personal devices. The larger implications for the field of emergency management further reaffirm the knowledge that people are the weakest

link in the cybersecurity chain and must be further studied to ensure implementation of reasonable security measures. Further, companies with concern for their cybersecurity (which should be all of them) should consider the risks introduced by personal devices used for work and/or connected to corporate machines.

Hypothesis 3, which expected a decrease in preparedness with increases in literacy and awareness was not found to have statistical significance within this body of data. The expected causal mechanism was that as people became more literate and aware, they would have a false sense of security due to their awareness and neglect to take actual preparedness measures on their home devices. The relationship discovered in the data could indicate that people do not rely on literacy or their own awareness to make decisions about their preparedness measures or could indicate an entirely different relationship not discussed by this body of research.

### **Potential Sources of Error**

There are several potential sources of error with the survey as it was conducted. First and foremost, the sample size was limited and non-representative of the larger population. My general access to survey-takers was limited to primarily college students and people with higher education which means that the sample was skewed to higher education/training values and therefore more exposure to these topics. Second, I hand-selected questions based mostly on my experiences with people and in order to limit the length of the survey. Therefore, the survey questions may not be entirely reliable gauges of their variables. Additionally, because this was a measured survey which included confidence intervals, the results may not be perfectly reproduceable. In an ideal experiment or measurement, each variable would be measured in a controlled laboratory setting and then compared against the personally identified information. The final potential source of error was that the questions provided in the survey were not skewed

to higher-educated people as they were intended to be measured against a wider range of skill sets which means that, within this sample, the questions may have been too easy.

**Data Points/Statistics of Note**

Table 9 below lists some interesting statistics gathered from aggregate survey data that, while not directly related to the hypotheses, may assist with future research endeavors.

*Table 9*

| <b>Statistics of Note</b>  |               |
|--|---------------|
| <i>Average Preparedness Score</i>  | 12.625 (~63%) |
| <i>Average Literacy Score</i>  | 23.775 (~85%) |
| <i>Average Awareness Score</i>   | 9.975 (~71%)  |
| 18% of all participants kept physical copies of their passwords  |               |
| 25% of all participants reuse the same password on >10 websites  |               |
| The most commonly identified data breach was Equifax (2017)  |               |
| Several participants considered alternative methods to securing private data over public networks to answer the ‘using public WIFI for online banking’ question. |               |
| Nearly all participants correctly identified all hallmarks of phishing emails.   |               |

**Conclusions**

Despite the small sample size and imperfections in data collection, there was statistically significant evidence for relationships between education/training and literacy and awareness. Therefore, if one’s goal is to improve computer literacy and awareness of ongoing cybersecurity topics, investing in higher education and specialized training may be a worthy endeavor. However, there is a distinct lack of evidence for any relationship between improvements in

literacy and awareness and actual implementation of personal cybersecurity measures. Therefore, if one's goal was to actually make a change in the way people implement cybersecurity at home, there is certainly more research to be done on effective ways to do that. Overall, this survey is just one steppingstone into the body of research that is personal cybersecurity. By and large, there is much emphasis on enterprise/corporate level implementation and compliance but not as much to identifying hazards at home and how to mitigate them not only to protect the company, but also to protect individuals and their data.

Areas for future research could include correlative studies on people who have experience or know somebody who experienced a cyber-attack/crime and whether that changed their personal cybersecurity measures. They could also consider measuring the amount of interaction between personal and corporate/work devices to measure the overall risk or the risk to a specific company to determine if changes need to be made to enterprise-level policies to reduce the risk of compromised personal devices introducing hazards to the corporate environment. One final idea would be to build a lab-based controlled study to measure true awareness and literacy by putting subjects through several tests to determine if, and within what parameters, they are able to complete computer tasks and identify potential hazards.

## Works Cited

- AlDaajeh, Saleh, Heba Saleous, Saed Alrabaee, Ezedin Barka, Frank Breitingner, and Kim-Kwang Raymond Choo. "The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education." *Computers & Security* 119 (August 1, 2022): 102754. <https://doi.org/10.1016/j.cose.2022.102754>.
- Alex Hern. "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases | GPS | The Guardian," January 28, 2018. <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>.
- Caldwell, Tracey. "Making Security Awareness Training Work." *Computer Fraud & Security* 2016, no. 6 (June 1, 2016): 8–14. [https://doi.org/10.1016/S1361-3723\(15\)30046-4](https://doi.org/10.1016/S1361-3723(15)30046-4).
- Farooq, Qamar, Peihua Fu, Shahzad Ahmad, Yanni Zhang, and Yunhong Hao. "Assessing Human Factor in the Adoption of Computer-Based Information Systems as the Internal Corporate Social Responsibility." *SAGE Open* 9, no. 3 (July 1, 2019): 2158244019868858. <https://doi.org/10.1177/2158244019868858>.
- Federal Trade Commission. "Cybersecurity Quizzes," October 14, 2018. <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz>.
- Hadlington, Lee. "Human Factors in Cybersecurity; Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours." *Heliyon* 3, no. 7 (July 1, 2017): e00346. <https://doi.org/10.1016/j.heliyon.2017.e00346>.
- Johnson, David W., Kimberly W. Bartholomew, and Duane Miller. "Improving Computer Literacy of Business Management Majors: A Case Study." *Journal of Information Technology Education: Research* 5, no. 1 (January 1, 2006): 77–94.
- Julian Fraillon, John Ainley, Wolfram Schulz, Daniel Duckworth, and Tim Friedman. "IEA International Computer and Information Literacy Study 2018 - Assessment Framework," 2018. <https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/22874/1007287.pdf?sequence=1&isAllowed=y>.
- Kennison, Shelia M., and Eric Chan-Tin. "Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors." *Frontiers in Psychology* 11 (2020). <https://www.frontiersin.org/articles/10.3389/fpsyg.2020.546546>.
- Kritzinger, E., and S. H. von Solms. "Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement." *Computers & Security* 29, no. 8 (November 1, 2010): 840–47. <https://doi.org/10.1016/j.cose.2010.08.001>.
- Mohan, Apurva. "Cyber Security for Personal Medical Devices Internet of Things." In *2014 IEEE International Conference on Distributed Computing in Sensor Systems*, 372–74, 2014. <https://doi.org/10.1109/DCOSS.2014.49>.
- Oh, Sarah Soyeon, Kyoung-A. Kim, Minsu Kim, Jaeuk Oh, Sang Hui Chu, and JiYeon Choi. "Measurement of Digital Literacy Among Older Adults: Systematic Review." *Journal of Medical Internet Research* 23, no. 2 (February 3, 2021): e26145. <https://doi.org/10.2196/26145>.
- Olney, Andrew M, and Dariush Bakhtiari. "Assessing Computer Literacy of Adults with Low Literacy Skills," n.d.

Reddy, G. Nikhita, and G. J. Ugander Reddy. "A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies." arXiv.org, February 8, 2014. <https://arxiv.org/abs/1402.1842v1>.

State of California - Department of Justice - Office of the Attorney General. "Search Data Security Breaches." Accessed March 30, 2023. <https://oag.ca.gov/privacy/databreach/list>.

Stiller, Evelyn, and Cathie LeBlanc. "From Computer Literacy to Cyber-Literacy." *Journal of Computing Sciences in Colleges* 21, no. 6 (June 1, 2006): 4–13.

"Top Scams to Watch out for in 2023, According to the Better Business Bureau." Accessed March 30, 2023. <https://www.denver7.com/money/consumer/dont-waste-your-money/top-scams-to-watch-out-for-in-2023-according-to-the-better-business-bureau>.



**Appendix A – Survey Questions, Coding, & Scoring**

*Table 1 – Education and Training*

| Question  | Answer Choices                       | Coding/Scoring  |
|---|--------------------------------------|---|
| <p>What is the highest level of education you have completed?</p>   | Less than high school                | <p>This information to be used qualitatively to compare to and control for education level as a factor for overall cyber literacy, awareness, and preparedness.</p> |
|   | High school graduate                 |   |
|   | Some college or currently in college |   |
|   | 2-year degree                        |   |
|   | 4-year degree                        |   |
|   | Professional degree                  |   |
|   | Doctorate                            |   |
| <p>Are you studying, or did you study, information technology, computer science, or another related field as a focus of your education (major, minor, concentration, etc.)?</p> | Yes                                  | <p>Qualitative or Binary Yes=1/No=0<br/>Unsure answers coded manually based on explanation</p>  |
|   | Maybe (please explain)               |   |
|   | No                                   |   |
|   | Not applicable                       |   |
| <p>Do you work in Information Technology (IT), Cybersecurity, or in a related field?</p>  | Yes                                  | <p>Qualitative or Binary Yes=1/No=0<br/>Unsure answers coded manually based on explanation</p>  |
|   | Maybe (please explain)               |   |
|   | No                                   |   |
|   | Yes                                  | Qualitative or  |

|   |   |   |
|---|---|---|
| Do you consider yourself to work in a security conscious field? Security conscious jobs may work with classified, proprietary, patent, HIPPA, or other protected information. | Unsure (please explain)                                 | Binary Yes=1/No=0<br><br>Unsure answers coded manually based on explanation                       |
|   | No  |   |
| Have you completed computer or cybersecurity training or education? This could include classes in school, training by your employer, online courses, etc.                     | Yes   | Qualitative or<br><br>Binary Yes=1/No=0<br><br>Unsure answers coded manually based on explanation |
|   | I think so, but I'm not sure it counts (please explain) |   |
|   | No  |   |

Table 2 – Computer/Cyber Literacy

| Question   | Answer Choices | Coding/Scoring                          |
|--|----------------|---|
| On a scale from 0-5: how confident are you that you could do each of the following computer tasks independently? |                |   |
| Check your computer or other device for operating system updates.  | Scale from 0-5 | Count by total score<br><br>Total of 25 |
| Search online and find the answer to a simple question   |                |   |

|  |  |   |
|--|--|---|
| <p>such as ‘what is the largest rodent in the world?’</p>  |  |   |
| <p>Find and follow instructions to resolve an error or a bug in a piece of software.</p>             |  |   |
| <p>Download and install drivers for a new piece of hardware.</p>                                     |  |   |
| <p>Create a document in a word processor.</p>  |  |   |
| <p>Which of the following helps to indicate that a website is legitimate? Select all that apply.</p> | <p>A padlock icon next to the URL</p>                                    | <p>1 point for each correct answer, 0 points for incorrect answers.</p> <p>Total of 3</p> |
|  | <p>URL begins with https://</p>  |   |
|  | <p>A misspelling in the URL</p>  |   |
|  | <p>Customer reviews on the website are all 5-stars</p>                   |   |
|  | <p>The website has a mailing address and contact phone number listed</p> |   |
|  | <p>URL begins with http://</p>   |   |
| <p>Total points out of 28</p>  |  |   |

Table 3 – Cybersecurity Awareness

| Question  | Answer Choices   | Coding/Scoring  |
|---|--|---|
| <p>Select any/all the data breaches you were aware of before this survey. (i.e., you heard about them on the news, etc.).</p> | <p>Equifax (Sept. 2017, 163 million users)</p>                                 | <p>Scored as 1 awareness point each. Total of 0-6.</p>  |
|   | <p>Los Angeles Unified School District (Sep. 2022, 600,000 students)</p>       |   |
|   | <p>Twitter (Nov 2022, 5.4 million users)</p>                                   |   |
|   | <p>PayPal (Jan 2023, 35,000 customers)</p>                                     |   |
|   | <p>No Fly List (Jan. 2023, US Federal No Fly List Exposed on the Internet)</p> |   |
|   | <p>AT&amp;T (March 2023, 9 million customers)</p>                              |   |
| <p>Is it generally considered safe to use public Wi-Fi for online banking?</p>  | <p>No</p>  | <p>Binary 0 or 1 point for Yes/No. Answers of Maybe will be manually scored based on explanation.</p> |
|   | <p>Maybe (please explain)</p>  |   |
|   | <p>Yes</p>   |   |

|  |   |  |
|--|---|--|
| <p>Which of the following are hallmarks of potential phishing emails? Select all that apply.</p> | <p>An email address not matching the company sending the email</p>                          | <p>1 point for each correct answer, 0 points for unselected answers<br/>Total of 4 points.</p> |
|  | <p>Claims of a problem with your account</p>  |  |
|  | <p>Links that do not direct to the company sending the email</p>                            |  |
|  | <p>Requests to provide contact information or passwords</p>                                 |  |
| <p>What is the most common way for ransomware to enter an organization/company?</p>              | <p>Server vulnerability</p>   | <p>1 point for correct answer of 'Phishing email', 0 points for incorrect answers.</p>         |
|  | <p>Phishing email</p>   |  |
|  | <p>Browser extensions</p>   |  |
|  | <p>Open-Source Software</p>   |  |
| <p>Which of the following best describes ransomware?</p>   | <p>A type of malware that causes pop-up ads on your device</p>                              | <p>1 point for correct answer of 'encrypts', 0 points for incorrect answers</p>                |
|  | <p>A type of firewall that protects financial data</p>                                      |  |
|  | <p>A type of malware that encrypts/locks you out of data</p>                                |  |
|  | <p>A type of software that performs automated tasks to assist you with daily activities</p> |  |
|  | <p>&lt;25%</p>  |  |

|  |                |  |
|--|----------------|--|
| What percentage of corporate cyber-attacks are caused by employee error? (Clicking on a malicious link in an email, downloading malware from the internet, etc.) | Between 25-50% | 1 point for correct answer of “>75%”, 0 points for incorrect answers |
|  | Between 50-75% |  |
|  | > 75%          |  |
| Awareness Total: 0 - 14  |                |  |

Table 4 – Cybersecurity Preparedness

| Question  | Answer Choices   | Coding/Scoring  |
|---|--|---|
| Do you use any of your passwords for multiple websites? Please select the most applicable answer. | Yes, I reuse the same password for > 10 websites                   | Scored as 0- 2. 0 points for 10+, 1 point for 2-10 uses, and 2 points for totally unique passwords.<br><br>Total of 0 - 2 |
|   | Yes, but I only reuse the same password for 2-10 websites          |   |
|   | No, I have totally unique passwords for every website that I visit |   |
| Which of these password standards do your password(s) generally meet? Select all that apply.      | 8 or more characters in length                                     | Each password standard will equate to 1 point for a total possible score of 0-4.  |
|   | Includes upper- and lower-case letters and at least one number     |   |

|  |   |   |
|--|---|---|
|  | Includes special characters (symbols)   |   |
|  | Doesn't include information such as birthdays, phone #s, or addresses.                        |   |
| Do you generally use optional two-factor authentication where possible for personal accounts?    | Yes, I usually turn on optional two-factor authentication                                     | Scored from 0-2, from 'No' to 'Yes, whenever'.  |
|  | I turn on two-factor authentication only on some accounts that I feel are important to secure |   |
|  | No, I don't use two-factor authentication on my personal accounts. Please explain why.        |   |
| How do you back up important information and photos? You may select more than one if applicable. | Cloud-based storage (like iCloud, Google Drive, OneDrive, Dropbox, etc.)                      | Scored as 0-2. No backup equates to 0 preparedness points, any physical backup is worth 1 point, cloud backups are worth 2.<br><br>Total of 0 – 4 |
|  | Personal storage media (like an external hard drive, home server, or flash drive)             |   |
|  | With physical copies (i.e., a filing cabinet or folder)                                       |   |

|   |  |  |
|---|--|--|
|   | I do not keep backups of my important data and photos  |  |
| How do you store/access your passwords?                                 | With a password manager (like Google Chrome, iCloud Keychain, LastPass, 1Password, etc.)           | 2 points for digital password manager, 1 point for digital storage, 0 points for memory, -1 point for physical. Answers of 'Other' will be scored based on information provided in the text box.<br><br>Total of 0-2 |
|   | A personal digital storage method (like in a Notes app, spreadsheet, or Word document)             |  |
|   | By memory (remembering which password goes with which website)                                     |  |
|   | In a physical form (like on a piece of paper in your wallet or planner)                            |  |
|   | Other (please explain)   |  |
| How often do you check your devices for updates? Select all that apply. | My devices are all set to update automatically   | 2 points for automatic and routine, 1 point for problems and pop-ups, 0 points for never.<br><br>Total of 0 – 6  |
|   | I routinely manually check to make sure my computer is up to date (at least a few times per year). |  |



|                                   |  |  |
|-----------------------------------|--|--|
|                                   | <p>I check for updates if I am<br/>having a problem</p>                        |  |
|                                   | <p>I check for updates when I<br/>get a pop-up/notification<br/>about them</p> |  |
|                                   | <p>I do not ever check my<br/>devices for updates</p>                          |  |
| <p>Preparedness Total: 0 - 20</p> |  |  |