7-11-2018

Survey Results on Adults and Cybersecurity Education

Frank Breitinger
University of New Haven, fbreitinger@newhaven.edu

Joseph Ricci
University of New Haven

Ibrahim Baggili
University of New Haven, ibaggili@newhaven.edu

Publisher Citation

Breitinger, Frank, Ricci, Joseph, Baggili, Ibrahim (2018). Survey results on adults and cybersecurity education. Education and Information Technologies. doi: 10.1007/s10639-018-9765-8

This work was funded by the University of New Haven's Summer Research Grant.

Dr. Baggili was appointed to the University of New Haven's Elder Family Endowed Chair in 2015.

Survey Results on Adults and Cybersecurity Education

Joseph Ricci, Frank Breitinger*, Ibrahim Baggili

Cyber Forensics Research and Education Group (UNHcFREG)
Tagliatela College of Engineering, ECECS
University of New Haven, 300 Boston Post Rd., West Haven, CT, 06516

Abstract

Cyberattacks and identity theft are common problems nowadays where researchers often say that humans are the weakest link the security chain. Therefore, this survey focused on analyzing the interest for adults for 'cyber threat eduction seminars', e.g., how to project themselves and their loved ones. Specifically, we asked questions to understand a possible audience, willingness for paying / time commitment, or fields of interest as well as background and previous training experience. The survey was conducted in late 2016 and taken by 233 participants. The results show that many are worried about cyber threats and about their children exploring the online domain. However, seminars do not seem to be a priority as many individuals were only willing to spend 1-1.5h on seminars.

Keywords: Adult Education, Cybersecurity, Survey, Training, Security Awareness, Children.

1. Introduction

More and more people utilize the Internet daily, but many are not aware of the threats in the online domain. According to Kaspersky Lab (2016), "people over 55 are overall not well educated when it comes to cyber-security. Only one-third of respondents have ever heard that someone can spy on them via a webcam." The study also shows that they are "heavy users of gadgets: One-quarter of respondents use tablets and one-third smartphones, with Apple devices being a big hit among them." The article concludes that the "representatives of the older generation are less aware of cyber-threats, and they are in general more trusting and thus more vulnerable." These findings coincide with results from Olmstead & Smith (2017) that show that "higher levels of education and younger Internet users are more likely to answer cybersecurity questions correctly". Spafford (2009) indicated that the lack of attention to cybersecurity threats is making matters worse and that action needs to be taken to prevent stolen properties that happen in the cyber domain.

Not knowing about the risks and dangers from utilizing the Internet can be even a bigger problem if the individuals are parents. For instance, Symantec (2015)[1] states that "surprisingly, overly confident, digital-native Millennials are the most vulnerable to online crime". While online crime is one challenge, another major problem is cyber bullying Hinduja & Patchin (2011).In order to help and support teenagers with cyber bullying, parents need to be educated and aware of latest trends and technologies; parents need to know which apps are used by their children and teach them. This can also prevent another problem. According to National Cyber Security Alliance (2017), "the majority of online teens continue to engage in some online activities that their parents don't know about; 57% say they have created an account that their parents were unaware of, such as on a social media site or for an app they wanted to use."

We argue that education is essential to all Internet users so that parents are aware of how their children are using the Internet and video games (which allow them to socialize with strangers). For example, a father of two witnessed another player on an online video game sexually exploit the children's video game character Kidspot.com.au (2016). The father assumed that the children were playing online with friends from school but upon discovering what was happening immediately removed the game from the children's iPad.

In this paper we present the result of our online survey named 'Cyber Threat Education Seminars' to better understand interests and concerns of adults. The goal was to identify a cornerstone for cybersecurity seminars. In detail, the research questions for this study were:

1. Is there a general interest in understanding the domain of cybersecurity?
2. What kind of audience should be targeted with such an effort (the demographics)?
3. What are the fields of interests? (e.g., only cyber threats in general vs. the latest developments in online trends, new smartphone applications, and so on.)

*Corresponding author.
Email addresses: jricc3@unh.newhaven.edu (Joseph Ricci), FBreitinger@newhaven.edu (Frank Breitinger), IBaggili@newhaven.edu (Ibrahim Baggili)
URL: http://www.UNHcFREG.com/ (Joseph Ricci), http://www.FBreitinger.de/ (Frank Breitinger), http://www.Baggili.com/ (Ibrahim Baggili)

[1] The authors do not have any association with the cybersecurity companies Kaspersky and Norton, their work was referenced in this article on the basis that their work helped support the points of this article.

4. How much money is the audience willing to spend on seminars / courses?
5. Is there a relationship between the relative understanding of cyber threats and a persons technical knowledge in the domain?

The survey was available at the end of 2016 and we received a total of 233 responses. 80% of the responses came from 40-70 year old individuals who were mostly well educated. Our results show that there is an interest in cybersecurity education but there are several obstacles. For instance, participants are interested in learning about the topic however they are not willing to spend time (seminars should only be 1h or 1.5h) or money ($20 in average).

The structure of this paper is as follows: The methodology and the survey design are presented in Sec. 2 and 3, respectively. The heart of this paper is Sec. 4 which presents our findings. The next three sections highlight the Background and Related work (Sec. 5), provide a discussion in (Sec. 7) and outline the limitations of this work (Sec. 6). The last section concludes the paper.

2. Methodology

The following high-level methodology was used to complete the survey:

1. A literature review was conducted (see Sec. 5) which ensure the relevance of this project / survey.
2. Designed a survey that gathered general demographic information, current knowledge of technology, identify the most concerning topics related to cyber threats, if there is a desire to learn about cybersecurity and questions regarding a possible course itself.
3. Obtained a category two exemption from the Institutional Review Board (IRB) at the University of New Haven restricting the survey from recording participant identification information or behavior, and disclaiming that it posed risk or harm to subjects not encountered in everyday life.
4. Distributed the survey to local schools, within our institution and social media.
5. Obtained data by exporting the coded responses to XLSX and CSV files from the Baseline survey system.
6. Analyzed the data using statistical probability, power tests, and crossing non-demographic questions with demographics and other.

The aim of this survey was to better understand the desire of the local population to learn about the different types of threats related to cybersecurity. First, it was important to see if any similar work had been conducted where we could not find any closely related work. However, the literature review helped in developing and structuring survey questions.

The design of the survey ensured that the scope of the population was limited to a certain area. The reasoning behind is that the authors plan to develop workshops and thus were particularity interested in local interests / concerns. It was also of interest to see if different demographic groups were impacted differently by cybersecurity related threats. The medium used to deliver the survey was an online surveying platform that was shared with many individuals by sharing a link. The authors shared this link by sending emails, contacting local schools, posting it on social media and by asking friends and family to participate in the survey. While some of the basic analysis was conducted using the built-in, survey platform functions, cross-correlations were mostly done using python scripts.

3. Survey design

We developed our survey based on the lack of literature that identifies the specific challenges that this survey aims to explore, what the authors decided were necessary to identify the amount of knowledge adults had in cybersecurity, their concerns for their children (if applicable) and the desire to learn about cybersecurity and the latest technologies (e.g., Apps their children might use). The survey went through several drafts and was reviewed by experts in the field to refine wording, content, and formatting of the survey. The survey itself consisted of 26 questions:

- 17 multiple choice
- 4 multiple selection (check box)
- 1 ranking
- 4 free response

According to IRB regulations at our institution, participants cannot be forced to answer any single question. The target audience were adults over 18 years old who mostly lived in and around the city of New Haven (CT) with diverse backgrounds and who do not necessarily have to have a cybersecurity background or training.

4. Results

The online survey was disseminated for over two months starting mid September 2016. In total, we received 233 responses. The calculated required sample size was 188 indicating that the number was large enough to make inferences from and that statistical tests were unlikely to exhibit type II errors (two-sided t-test, alpha = 0.06, using a medium effect size of 0.5 and power of 0.99).

The targeted participants for this study are the local community in New Haven County as we intend to provide seminars / workshops designed for this audience. Thus, results for other cities / states or nations may look different and a potential workshop may need adjustments according to the local audience. While we aimed at reaching a variety of different backgrounds, the majority of the our participants are in the education sector. This originated from spreading the survey through local Universities / schools where we targeted parents. However, it looks like primarily faculty and staff answered the survey.

In the following we present the survey results. A discussion about the results can be found in Sec. 7.

4.1. Demographics

The first part of the survey focused on the demographics which are shown in Table 1. The majority of participants were between 40 and 69 years old (78%) which was the age group we were aiming for. There is a minor shift in gender towards females. 84% of the participants have at least a college degree reflected by 57% of the respondents reporting an annual house earning of more than $100k In terms of respondent occupations, 63% of participants are in the education sector. The rest of participants work in a variety of fields such as health care, government, construction, law, public service, information technology, among many other jobs that participants filled in the open text box. Of all the participants, 48% have children under the age of fourteen and the rest of the participants either have children over the age of fourteen (35.2%) or no children at all (17.2%).

4.2. General Questions

This section discusses general questions about the usage of technology, how participants feel about their children using technology and how safe they feel on the Internet.

4.2.1. Familiarity with technology

First, we asked participants to rate their *familiarity with computers and technology* as we assume that highly skilled individuals will deny education / further training. The question was answered on a 1 to 5 scale starting with '(1) I know how to turn on and off a computer', '(3) use it frequently for web browsing and office work' and '(5) I am a professional/studied in a related area'. This question was answered by 231 participants and almost 99.0% rated their familiarity with a 3 or above. Specifically, we obtained 49.4% for option three, 35.9% for option four and 13.4% for option five which matched our expectations; most people use computers for work and perform daily activities.

4.2.2. Usage

To get a better understanding of how much time participants spend on a device connected to the Internet, we asked users to estimate the number of hours per week. The question accepted any full number as an answer and averaged to 38.5 hours per week (from 230 given answers) with a minimum of 4 hours and a maximum of 230 hours (which is obviously a typo). The top answers from 34 individuals was 40h followed 50h and 60h hours (each one counted 22 times). Although this correlates to the typical work week, we did not distinguish between free time and work. Looking at ranges, gave the following results:

- 66% of responses were <= 40h,
- 23% of responses were between 41h and 60,
- 6% of responses were between 61h and 80, and
- 5% of responses were > 81.

Table 1: Demographics results from survey

Gender	
Female	67.7%
Male	31.5%
Transgender	.4%
Other	.4%
Age	
18 to 29	4.3%
30 to 39	14.2%
40 to 49	39.2%
50 to 69	39.2%
69 and older	3.0%
Highest Completed Level of Education	
High school graduate	2.6%
Technical training	1.7%
Some college	11.7%
College graduate	20.4%
Some postgraduate	2.6%
Post graduate degree	61.0%
Annual Household Income	
$20,000 - $34,999	1.4%
$35,000 - $49,999	5.4%
$50,000 - $74,999	18.0%
$75,000 - $99,999	18.0%
$100,000 - $149,999	30.2%
$150,000 or more	27.0%
Job Sector	
Education	62.5%
Health care	8.6%
Information Technology	5.6%
Public Service	3.0%
Government	3.0%
Construction	1.3%
Law	.9%
Children the Age of 14 and Younger	
None	17.2%
Children are older	35.2%
One	24.0%
Two	16.3%
Three	5.6%
More	1.7%

Splitting it by gender did not show any significant difference in usage.

Subsequently, we asked participants *what they use their PC for* to get a better understanding of how technology is being utilized in every day life. This was a checkbox question where multiple answers were possible. The answers of the 232 respondents were as follows:

1. Web browsing (92.2%)
2. Clerical and office work (87.1%)

3. Social media (61.6%)
4. Online learning (59.5%)
5. Entertainment (58.2%)
6. Programming (14.2%)
7. Playing video games (13.8%)
8. Graphic design (9.1%)

The last checkbox of the question was 'other' and allowed participants to add additional options. The 33 responses can be clustered to the following groups: banking/finances, CADD work, communication/email, design, development, directions, shopping, information, education, hobbies, research, information security work, instructor, lesson plans, marketing, movie editing, news, profession, or web enterprise applications.

4.2.3. Cybersecurity awareness

The next three questions targeted the security awareness of participants. Therefore, we first asked whether or not participants use any type of cybersecurity product. In result, the majority of participants indicate that they do use some form of cybersecurity software/hardware (note this was a checkbox question and multiple answers where allowed):

1. Anti-virus 80%
2. Firewall (hardware or software) 68%
3. Anti-spyware 51%
4. Unsure 13%
5. Other 5%
6. None 3%

41% of the participants indicated that they use all three (anti-virus, anti-spyware and firewall) and 29% participants indicated that they use two of the mentioned products. The 12 responses under *other* were wide spread and included qualified answers such as encryption or Intrusion Detection and Prevention System but also less qualified answers such as incognito mode, constant backups or MAC, which do not protect the user from phishing, viruses or other maliciousness. However, this indicated that several participants do not quite understand the products / technologies they are using.

Subsequently, participants were asked if they are *concerned about cyber threats and latest technologies*. Three-fourths of participants were concerned that cyber threats and technology could impact both their personal and professional life; 15% were concerned that it could only affect their personal life; 2% said they were concerned it could affect their professional life and 8% of participants were not concerned at all.

The last question in this category asked if the participant had fallen victim to cyber crime (e.g., identity theft, credit fraud, account hacked, etc), with exactly half of all participants indicating that they have been a victim in the past. The other half was either unsure (10%) or were not victims at all (40%). When correlating the usage of cybersecurity products to falling victim of cybercrime, we realized that about 50% are using products and the other half does not use products. We see this as in indicator that awareness / education is an important aspect and that using security products only is not sufficient. Of the 50% who were victims, 47% also indicated that they were concerned about the latest cybersecurity threats and how it might affect their lives (personal, professional or both).

Between male and female participants, our study shows that 60% of all men who participated were victims. Women were less likely to be a victim, 44% of participating females falling victim. Comparing the victims with the household income, over 60% (65) of those making $100,000+ were victims of some type of cyber crime, which makes up 30% of all participants. On the other hand, for the participants making between $50,000 and $99,999, only 47% (37) were victims. For the participants making $49,999 and less, 4% (6) were victims. Thus, we see a tendency that the more money participants make, the more likely they are to fall victim to some form of cyber crime.

4.2.4. Children and technology

The next set of questions focused on children and technology where participants were first asked if they are concerned about the devices and apps that their children use. About 60% answered with yes, 30% with no and for the remaining participants this question did not apply to them.

Next, we asked participants *at what age do you think it is appropriate for a child to have her/his own smartphone?* and summarized the results in Table 2. The answers range widely between 0 to 25 with an average of 12.93. While we cannot make assumptions and manipulate the data, 0 and 25 may have resulted from typos. 62% of participants answered between 12 and 14 years with the most common answer 12 years by 65 individuals.

Table 2: The age participants believe a child should own a smartphone.

Children's age	Number of participants
0	1
8	6
9	3
10	23
11	3
12	65
13	50
14	24
15	15
16	29
18	4
20	1
25	1

Before coming to training / seminar related questions, we asked participants whether or not they have currently or in the past taken measures to either monitor their children's online activities or speak with them about the dangers on the Internet (e.g., there are multiple tools that are available for parents to monitor their children's behavior on mobile devices). The results are as follows (multiple answers were possible):

1. Yes, I limit the time of their online activity (55%).
2. Yes, I use programs/apps to limit their online activity / possibilities (35%).

3. Yes, I talk with them frequently about online dangers (31%).
4. No (25%).

Having a closer look at the 111 participants who have children under the age of 14, we found that only 63% of the adults talk to their kids, 47% limit the time of the online activity and 44% use programs/apps to limit activities online. Our survey also shows that females are more likely to talk to their children; only 48% of the males checked this option compared to 69% females.

4.3. Training Questions

This section identifies the results with regard to history, experience, and desire for training in cybersecurity and the latest technologies.

4.3.1. Security Training

The first question started by asking participants for prior training in cybersecurity which revealed that over two-thirds (159 or 70%) never had training before. We cross referenced this to *have you been a victim of cyber crime* where the results are shown in Table 3. The table shows that there is not a significant correlation between training and never been a victim. More research is needed to find out (a) how the training was structured and (b) the content of the training. This could then explain why training did not have impact.

Table 3: A matrix of participants who had prior training and were victims.

	Training	**No Training**	Total
Victim	37	78	115
Never a victim	24	65	89
Unsure	6	16	22
Total	67	159	226

The next question asked if participants would be interested in attending a seminar that teaches them how to minimize cyber threats and understand the latest trends. Over 80% of participants were interested in attending some kind of cybersecurity training. Specifically,

- 15% indicated that they were interested in training about minimizing cyber threats,
- 5% were interested in understanding the latest technology trends (e.g., apps or smart devices),
- 63% were interested in both aforementioned topics, and
- 17% were not interested in either topics.

Correlating this question with 'have previous training' showed that the majority of participants would be interested in another training. All details are listed in Table 4.

When further analyzing the 26 participants who are not interested in training and had no prior training, we found that only one considered herself *5 (I am a professional/studied in a related area)*, 11 considered themselves a 4 and 13 considered themselves *3 (Use frequently for web browsing and office work)*. One person did not answer the familiarity question.

Table 4: A matrix of participants who had prior training and were willing to take additional training.

	Training	**No training**	Total
Interested	53	135	188
Not Interested	14	26	40
Total	67	161	228

For the last question of this set, we asked participants to rank six topics in regards to cybersecurity, with 1 being the most interesting and 6 being the least: *protecting children from online dangers*, *preventing identity theft*, *identifying safe websites*, *recognizing safe Apps*, *identifying malicious e-mails*, and *protect data stored in my computer*. The results are depicted in Figure 1 where the very left section of each bar indicates the results for one (most interesting), and the very right parts the results for six (least interesting). Most participants worry about the safety of their children and ranked *protecting children from online dangers* highest (43%) followed by *how to prevent identity theft* with 37%. Note that this topic also had the most votes as second choice (35%). The remaining areas were ranked very similar.

When correlating these results to *what they use their PC for*, it is interesting to see that their areas of interest do not align with what they do on their PC. For example, web browsing was ranked as the main purpose that participants use their PC, however, three-quarters of participants ranked *Identifying safe websites* between three and six.

4.3.2. Training location and length

Next, we tried to identify the preferred location and duration of possible seminars. With respect to environment, the results were almost balanced with a minor favor for 'hybrid solution' (both online and local). Specifically, 39% (88) preferred a hybrid solution, 31% of participants preferred an online seminar and 31% preferred a location at a physical site. In order to get an exact location, participants were asked where they would like the seminar to take place. Results of this checkbox questions are listed as follows:

1. University of New Haven[2] (63%)
2. Home (35%)
3. Online (30%)
4. Work (27%)
5. Local School (21%)

Subsequently, we asked *what a desired seminar length would be* and *how frequently the participant would be willing to attend a training course*. The most common responses were for 1 hour per seminar (43%) and only one weekday evening (74%). Precisely, we received the following responses for the first question:

[2]Given that the survey was distributed at the University, this might be the workplace for many of the participants.

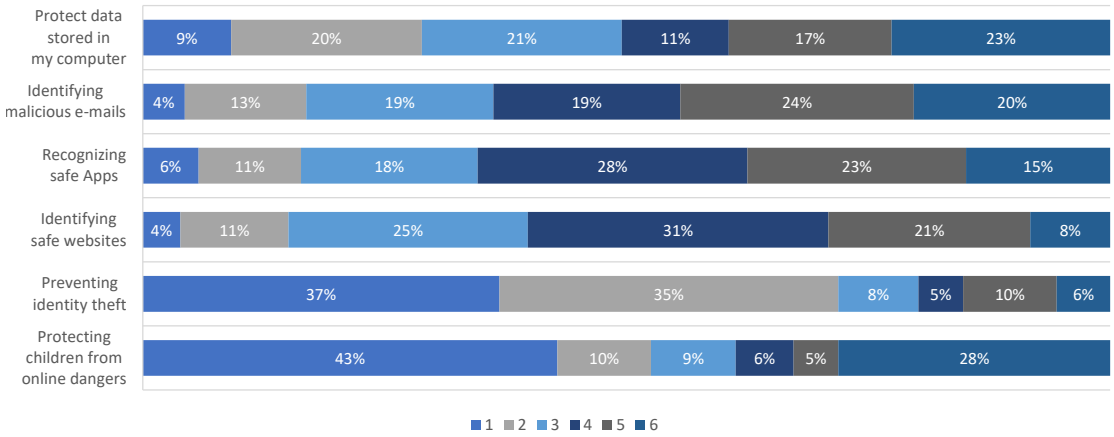

Figure 1: On a scale of 1 to 6 (1 being the most interesting and 6 being the least), participants were asked to rank which topics were interesting.

1. 1 hour (43%)
2. 1.5 hours (34%)
3. 2 hours (18%)
4. 3 hours (3%)
5. 4 hours (1%)
6. One Day (1%)
7. More (.4%)

With regards to the frequency, the vast majority of participants preferred a weekday evening (74%) followed by weekends (15%), multiple weekday evenings (7%) and two weekday evenings (5%).

4.3.3. Instructors

A possible seminar would be designed to educate adults who have little to no experience with cybersecurity. Therefore, the authors were curious to see whether or not participants would tolerate a student instructor (majoring in cybersecurity) to the teach the seminar. 84% participants would be willing to accept a student who is majoring in cybersecurity as a seminar instructor whereas 4% responded with *no*. The remaining 12% commented it would depend on factors like ability to communicate and engage, depth of knowledge (material created jointly with a professor), experience, etc.

4.3.4. Costs

This section discusses the last two multiple choice questions. First, participants were asked *how much money (in dollars) would you be willing to spend on a seminar?*. The text box accepted any whole number.

200 participants entered values ranging from \$0 to \$300, with an average of \$20.44, a standard deviation of 31.64, and a median of \$10. The most common responses are listed below:

1. 40% answered \$0,
2. 14% answered \$25,
3. 12% answered \$20,
4. 11% answered \$50,
5. 9% answered \$10, and
6. 5% answered \$100.

In other words, even though many are concerned about the devices that their children use or are generally concerned about cyber threats, 40% are not willing to pay at all; only 20% were willing to pay \$30 or more. This seems to indicate that while there are concerns around technology and children, it is not a high enough priority for many adults to spend money on training. The downside to this is that adults should spend the time and some money to learn about how to mitigate the risks that may impact their finances. Spending money on training would be small in comparison to the amount of resources spent on trying to recover from identity theft. We correlated the \$0-group with several other questions (e.g., income, previously been a victim, and willingness to train) but we did not see any statistically significant impact / correlation.

Next, participants were asked if they would be willing to attend a seminar if the employer pays for it. The vast majority of participants answered *yes* (96%). The remaining 4% who were not interested, indicated that they were experienced, i.e., one participant rated themselves as a 5 and the other participants rated themselves a 4.

4.4. Comments and Suggestions

The last question was on open text box and allowed participants the possibility to provide comments and/or suggestions which resulted in 37 responses. In the following we summarize the content of the 30 relevant comments (seven of the responses were either *Not Applicable* or *Thank you*; four comments addressed the questions / answers we had).

Eight comments were very supportive and recommend to do a seminar, mentioned most relevant topics and asked to advertise it early. One out of the eight even wrote 'I think a class on security should be mandatory for all [..] employees'. Additionally, one wrote 'should be offered to students as well'.

One participant wrote that in response to 'age of smart phone for a child' that they were forced to write in a number, but they originally wrote that it depends on the circumstance. For instance, there might be situation where you want your child to have a phone such as need to come home alone, or planned long distance travel. We agree with this comment although our questions asked about daily scenarios.

Another set of comments addressed time challenges stating it would be difficult to squeeze training into their schedules. One person raised the idea to have a webinar during the lunch hour or in the afternoon. This was because employers may find the webinar to be beneficial to employees and might allow them to take time to watch during lunch hours.

Several comments addressed the pricing and suggested that the employer should sponsor this; that they had free cybersecurity training with a local police department; and that workshop had been free. In contrast, one comment mentioned that they already had training but wishes to attend a mored tailored seminar towards personal/home computing and ideally to children. Another one asked for more advanced training.

Another comment stated, 'it would be good to have a seminar for both parents and kids to attend together to understand threats and learn how to manage them'. From a parent's perspective, it would be even more beneficial for their children to attend a security course. Allowing for both adult and child to see what to avoid when using the Internet and apps and how to determine what is safe and what is not. Interestingly, one respondent commented 'Information from teenagers who actually use the internet and apps would be helpful.'

5. Background and Related work

Cybersecurity is an important aspect of our lives as we are confronted with it daily. In response, the education sector is changing their curricula to educate students early on about the dangers of the Internet. For instance, the Air Force Association (2009) created CyberPatriot is a National Youth Cyber Education Program aimed at educating American high school and middle school students which has three programs: (1) the National Youth Cyber Defense Competition, (2) AFA Cybercamps, and (3) Elementary School Cyber Education Initiative (ESCEI). Students have to find vulnerabilities within their system and harden them while maintaining critical services. Another cybersecurity education program called *GenCyber* is a summer camp for students and teachers throughout American grade school levels that is supported NSA / NSF (2017). Both programs are offered at no cost to students and are intended to increase interest in cybersecurity careers; they are meant to be a solution to the shortfall of skilled cybersecurity professionals in America but also to teach students how to protect themselves in a networked world. The National Institute of Standards and Technology (2016) (NIST) has launched its own initiative to promote cybersecurity career awareness and support academic preparedness of K-12 students with its National Initiative for Cybersecurity Education (NICE) program. This initiative provides resources to grade schools throughout America in an attempt to educate the coming generations grow up with a background in cybersecurity.

5.1. Need for Education / Training

Analogously, one would imagine that there are possibilities for adults to educate themselves as there is a significant lack of knowledge. According to a survey from Olmstead & Smith (2017), which was then also picked up by Forbes.com (Murnane, 2017), many Americans are unaware of key cybersecurity topics, terms and concepts. The majority of adults were able to identify a strong password when they saw one and recognize the use of public Wi-Fi. However, many did not know what two-factor authentication is or how to determine whether or not a web site uses encryption. The survey covered topics regarding Virtual Private Networks (VPN), Internet Service Providers (ISP) ability to track network traffic, botnet and phishing.

Abela (2017) found that 80% of Americans admitted to risky cybersecurity behaviors. Nearly half of the 2,006 participants used unsecured networks, one third clicked unfamiliar links on social media, one third downloaded third-party sourced files, one third opened unsolicited email attachments and one third had the same password for all logins. Much of which should be common cybersecurity practice among adults. There were several other concerning findings that indicated poor practices by adults that shop online.

American Association of Retired Persons (2016) (AARP) conducted a survey of adults 18 and over to understand their use of social media and the different ways they connect to the Internet. Over 70% of adults use public Wi-Fi to access their Facebook or personal email. Almost 70% of participants reported that they did not recall the public location they accessed Wi-Fi providing any information about how to protect themselves from cyber scams.

This reaffirms the goals of this research, which is to determine and identify adults largest concerns with cybersecurity and the areas they are most interested in. There is a large population of adults who are unaware of some of the basic ways to protect themselves from online dangers. Seeing the lack of cybersecurity awareness throughout adults populations from a variety of surveys, getting adults to become interested and effectively teaching them may present challenges in itself.

5.2. Challenges / Willingness to Learn

There are several challenges that need to be taken into consideration when assessing an adult population's willingness to learn. According to Charness & Boot (2009), "older adults reluctant to adopt new technology, such as the Internet [...] We conclude that normative age-related changes in ability must be taken into account when designing products and training programs for aging adults". On the other hand, Li & Perkins (2007) conclude that education rather than age is a significant factor influencing the willingness to learn about new technology.

While adults are often resistant in the beginning, at some point they will (have to) use newer technologies. Xie et al. (2012) conducted an exploratory study to understand how adults felt about social media and what strategies can be used to facilitate their learning of social media. The results indicated that initially adults were uninterested in learning about social media to progressively having a positive but cautious outlook but eventually contribute personal content to social media. The primary cause for the slow adaptation to social media was concern regarding privacy.

The thesis from Jeffers (2016) aimed to determine if best practices exist in adult learning theories, and how they can be

applied in corporate cybersecurity training programs. Also, part of the study was to identify why corporate training fails and what some of the methods are that can implement best practices. The author proposed a hybrid approach of multiple training methods to get the best training implemented. Understanding where corporations fail at training the layman in cybersecurity can help give the researchers an understanding of what might be the challenges that we may face when trying to determine the biggest concerns for adults.

Work by Furman et al. (2012) tried to understand users' mindset of online security by conducting in-depth interviews to identify correct perceptions, myths, and potential misconceptions. Participants were aware of and concerned with online and computer security but lacked a complete skill set to protect their computer systems, identities, and information online.

On the other hand, there are scenarios were adults are required or willing to learn. According to Brooks (2016), "career success depends on your willingness to learn" which is very similar to Forbes Coaches Council (2014) who released an article titled: 'Changing Careers? Here's whether you should return to school first'.

5.3. Education possibilities for adults

With cybersecurity becoming a major concern for the United States, budgeting to augment the current workforce has been allocated to build and strengthen skill sets of children and adults. With our emphasis focused on educating adults, we explored the education possibilities for adults that are offered by a variety of American agencies, open source material and pay to learn sources.

There are several programs that exist throughout the country meant to educate parents about online dangers. One program Loudoun County (Gibson, 2013) in Loudoun County, Virginia, the local police department holds sessions called 'Internet Safety: What Parents Need to Know', two, one hour sessions. The topics range from statistics about children sexting to different real world scenarios where children were tracked through the GPS coordinates recorded into their pictures that they took with their phones.

A paid online program meant to educate parents about online dangers (Internet Safe Education, 2017) delivers content through online courses. Enough is Enough (2017) provides a series of DVD's that has material to teach both parents and adults about the variety of dangers associated with the Internet which include pornography, social media, cyber bullying, protecting their identity, phishing, virus protection, etc.

Many articles (Concise AC, 2017; Phoenix, 2017; Bradford, 2017; Sheridan, 2016) discuss the possibilities of changing careers to cybersecurity and provide insight as to what might be the best method to start. Topics range from reasons to start a career in cybersecurity, different resources to use to learn and tips to accelerate their career.

There is a variety of resources available for adults, to educate themselves in the cybersecurity discipline which are free. Examples are Cybrary (`cybrary.it`), edX (`edx.org`), Department of Homeland Security (DHS) National Initiative for Cybersecurity Careers and Studies (NICCS) and CyberAces by SysAdmin, Audit, Network and Security (SANS) Institute (`cyberaces.org`). Additionally, there are several paid training courses and degrees.

For cybersecurity professionals looking to enhance their current skill sets in order to better educate others additional programs have been created. The 'Cyber Teacher' (`cyberteachers.org`) certification program aims to help teachers in grades 6 - 12 add cybersecurity lessons to their curriculum. Another cybersecurity program, The National Integrated Cyber Education Research Center (NICERC), aims to develop cyber-based curricula for K-12 teachers in the United States.

6. Limitations

There are several limitations with this survey. First, 62.5% of the participants were in the education sector and thus some answers may be biased. Another limitation was that 61% of participants had a very high level of education, which again may not be an accurate representation of the local population. Over 50% of participants did not have children or had children that were older than 14. There is a limitation there since this survey focused on the concerns of parents and their concerns with their children using apps and the Internet. During the time of the survey, there were several data breaches (Franceschi-Bicchierai, 2016). These data breaches could have influenced how the participants feel about their safety when using the Internet and the apps that their children use.

7. Discussion and Conclusion

While there are several initiatives to increase the shortfall of skilled cybersecurity professionals (see Sec. 5), we argue that it is also essential to educate an everyday Internet user as many of us spend a lot of time in the cyber world by browsing, for work or other online activities. Most participants of this survey have at least a basic understanding about cyber threats and use Anti-virus software and/or Firewalls. However, about 50% had fallen victim to cyber crime which is not a surprise in times of mass-hacks, e.g., OPM, Home Depot, Target, Walmart, Deloitte, Yahoo, etc. (Roberts, 2017; McCoy, 2017; Krebs, 2017; Hill, 2016; Fiegerman, 2017).

Many participants expressed anxiety about their online safety, new technologies as well as the technologies their kids are using. Specifically, three-fourths of participants were concerned that cyber threats and technology could impact both their personal and professional life. Given their on concerns, it feels natural that the majority tries to project their children by limiting their online activities and educating them. However, how can they educate them if they are lacking sophisticated knowledge in the domain themselves, e.g., some participants did not know the security products they use, did not consider themselves as experts (3 out of 5 rating) or have not had a security seminar before.

Correspondingly, the vast majority of participants is interested in education and to learn more about cybersecurity (regardless if they had prior training); especially if would be sponsored by the employer. On the other hand, some individuals

asked for more advanced seminars and / or recommend that every employee should have some cybersecurity education.

The results also show that participants are less willing to spend money nor time on possible seminars. In regards to time, 77% favored seminars that are 1 or 1.5h. Participants stressed that it is difficult to find time to take a course outside of work, given that it may interfere with their family life or other responsibilities. Several participants would like to have the ability attend courses either online or in person during their lunch hour at work. With respect to costs, the participants were willing to spend about $20 for a seminar. The comments pointed out that there is free material / training and that they expect their employer to pay for training. With that mindset, it is unsurprisingly that the humans are considered to be the weakest link in regards to cybersecurity; many successful attacks occur due to human error.

A follow-up survey could be conducted to understand what adults think of cybersecurity, whether or not they find it interesting or believe it is trivial. Also, since many were not interested in paying for cybersecurity training and when ranking the most interesting topics, it would be useful to see if employers would also be willing to pay for training and offer it to their employees.

Acknowledgments

This work was funded by the University of New Haven's Summer Research Grant.

References

Abela, R. (2017). Consumer survey. https://www.netsparker.com/blog/news/consumers-web-applications-most-risk-hacked/.

Air Force Association (2009). Cyberpatriot national youth cyber education program. https://www.uscyberpatriot.org/home.

American Association of Retired Persons (2016). 2016 aarp cyber security survey of adults age 18 and older. https://www.aarp.org/content/dam/aarp/research/surveys_statistics/general/2016/2016-national-cyber-security-annot-res-gen.pdf.

Bradford, L. (2017). How to start a lucrative career in cybersecurity. https://www.forbes.com/sites/laurencebradford/2017/02/27/how-to-start-a-lucrative-career-in-cybersecurity.

Brooks, C. (2016). Career success depends on your willingness to learn. https://www.businessnewsdaily.com/9256-career-boost-learning.html.

Charness, N., & Boot, W. R. (2009). Aging and information technology use: Potential and barriers. *Current Directions in Psychological Science*, *18*, 253–258.

Concise AC (2017). Learn how to start a career in cybersecurity: Interviews, resources, tips. https://breakingintocybersecurity.com/.

Enough is Enough (2017). Internet safety 101. http://internetsafety101.org/.

Fiegerman, S. (2017). The biggest data breaches ever. http://money.cnn.com/2017/09/07/technology/business/biggest-breaches-ever/index.html. Online; accessed 19 October 2017.

Forbes Coaches Council (2014). Changing careers? here's whether you should return to school first. https://www.forbes.com/sites/forbescoachescouncil/2017/04/14/changing-careers-heres-whether-you-should-return-to-school-first/#32d7404d31fa.

Franceschi-Bicchierai, L. (2016). The worst hacks of 2016. https://motherboard.vice.com/en_us/article/wnxkz9/the-worst-hacks-of-2016. Online; accessed 19 October 2017.

Furman, S., Theofanos, M. F., Choong, Y.-Y., & Stanton, B. (2012). Basing cybersecurity training on user perceptions. *IEEE Security & Privacy*, *10*, 40–49.

Gibson, C. (2013). Internet safety courses teach parents dangers of digital realm. https://www.washingtonpost.com/local/internet-safety-courses-teach-parents-dangers-of-digital-realm/2013/03/05/2c676aa6-7b79-11e2-9a75-dab0201670da_story.html?utm_term=.ed719cb6207e.

Hill, M. (2016). Walmart confirms card data theft. https://www.infosecurity-magazine.com/news/walmart-confirms-card-data-theft/. Online; accessed 19 October 2017.

Hinduja, S., & Patchin, J. W. (2011). Summary of our cyber bullying research from 2005–2010. *Retrieved on January29*, .

Internet Safe Education (2017). Courses for parents. https://www.internetsafeeducation.com/courses-for-parents/.

Jeffers, T. M. (2016). *Maximizing adult learning methodologies in corporate cyber security training programs*. Ph.D. thesis Utica College.

Kaspersky Lab (2016). Elderly people online: habits and concerns. https://www.kaspersky.co.uk/blog/older-people-internet/7736/.

Kidspot.com.au (2016). Dad horrified to find vile messages in popular game on son's ipad. http://www.kidspot.com.au/parenting/real-life/in-the-news/dad-horrified-to-find-vile-messages-in-popular-game-on-sons-ipad.

Krebs, B. (2017). Source: Deloitte breach affected all company email, admin accounts. https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/. Online; accessed 19 October 2017.

Li, Y. B., & Perkins, A. (2007). The impact of technological developments on the daily life of the elderly. *Technology in Society*, *29*, 361–368.

McCoy, K. (2017). Target to pay $18.5m for 2013 data breach that affected 41 million consumers. https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/. Online; accessed 19 October 2017.

Murnane, K. (2017). If you don't know much about cybersecurity, you're not alone. https://www.forbes.com/sites/kevinmurnane/2017/03/29/if-you-dont-know-much-about-cybersecurity-youre-not-alone/.

National Cyber Security Alliance (2017). Keeping up with generation app: Ncsa parent/teen online safety survey. https://staysafeonline.org/wp-content/uploads/2017/10/Generation-App-Survey-Report-2017.pdf.

National Institute of Standards and Technology (2016). National initiative for cybersecurity education (nice). https://www.nist.gov/itl/applied-cybersecurity/nice.

NSA / NSF (2017). Gencyber summer camp. https://www.gen-cyber.com/about/.

Olmstead, K., & Smith, A. (2017). What the public knows about cybersecurity. http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/.

Phoenix, U. o. (2017). Why you should consider a career change to cybersecurity (paid content by university of phoenix). https://mashable.com/2017/05/24/career-change-cybersecurity/.

Roberts, J. J. (2017). Home depot data breach costs top $179 million after latest settlement. http://fortune.com/2017/03/09/home-depot-data-breach-banks/. Online; accessed 19 October 2017.

Sheridan, K. (2016). 8 steps to building a successful cyber-security career. https://www.informationweek.com/strategic-cio/security-and-risk-strategy/8-steps-to-building-a-successful-cyber-security-career/d/d-id/1326691.

Spafford, E. H. (2009). Cyber security: assessing our vulnerabilities and developing an effective defense. In *Protecting Persons While Protecting the People* (pp. 20–33). Springer.

Symantec, N. (2015). Norton cybersecurity insights report. https://us.norton.com/norton-cybersecurity-insights-report-global.

Xie, B., Watkins, I., Golbeck, J., & Huang, M. (2012). Understanding and changing older adults' perceptions and learning of social media. *Educational gerontology*, *38*, 282–296.