Journal of Cybersecurity Education, Research and Practice

Volume 2019 | Number 2 Article 6

January 2020

Divergent student views of cybersecurity

Susan E. Ramlo
University of Akron, sramlo@uakron.edu

John B. Nicholas
University of Akron, jn@uakron.edu

Divergent student views of cybersecurity

Abstract

Cybersecurity is a worldwide issue and concern. Prior studies indicate that many people do not use cybersecurity best practices. Although these prior studies used large-scale surveys or interviews, this study used Q methodology [Q] because Q provides greater insight than Likert-format surveys. In fact, Q was created to scientifically study subjectivity. Within a Q study, various stages as well as philosophical, epistemological, and ontological principles represent a complete methodology. At first, Q researchers collect items that represent the broad range of communications about the topic (called the concourse). Although the items can be pictures, scents, or other means of communication, statements are the most common. Q researchers reduce the items of the concourse to create the Q-sample while preserving the range of communications. Subsequently, participants sort these items into a grid to provide a snapshot of their viewpoint on the topic. Statistical analysis reveals the multiple, diverse viewpoints in a way that allows for detailed descriptions of those views. In this study, the researchers collected statements about cybersecurity. Students in technical degree programs, including computer information systems (CIS), sorted these statements into a grid with a range of “most like my view” to “most unlike my view” of cybersecurity. Items placed on the extreme ends of this grid represent those statements most salient with each student’s views. Analyses revealed three divergent viewpoints: 1) Cybersecurity best practices, 2) No worries, and 3) No sense of urgency. Although the CIS majors identified with View 1, the other technical degree program students were represented across all three views. Certainly, students who hold the No worries and No sense of urgency viewpoints are unprepared to deal with cybersecurity issues in the workplace. The descriptions of these views have implications for cybersecurity course and program development, including assessments. Additionally, this study’s outcomes indicate a need to replicate this investigation in other settings to estimate risk of employees introducing cyber threats at their workplace. Similarly, these outcomes have implications for workforce development training regarding improved cybersecurity viewpoints and, therefore, behaviors.

Keywords

mixed method, cybersecurity, perspectives, subjectivity, Q methodology

INTRODUCTION

Cybersecurity is currently a worldwide issue and concern. Within the United States, various views of cyber security appear to exist based upon a poll by Pew Research Center (Olmstead & Smith, 2017). However, the Pew Research Center used a national survey of opinion and behavior. In contrast, Thompson, Herman, Scheponik, Sherman, Golaszewski, Phatak, and Patsourakos (2018) investigated students' conceptual understanding of cybersecurity qualitative methods (interviews). Somewhere in between a large quantitative study and a small qualitative study, a deep investigation into revealing and describing the divergent views of cybersecurity using Q methodology can be useful in expanding our understanding of views of cybersecurity. The use of Q methodology [Q] allowed us to study and describe college students' divergent views of cybersecurity in relation to the broad impacts, corporations, government policy, personal knowledge, personal policy, and training. Q methodology's creator, William Stephenson (1953), designed Q specifically to scientifically study subjectivity by revealing the multiple, divergent perspectives on a topic within a group of people. In this study, participants were students enrolled in technology-based degree programs at a midsized, public, urban university in the Midwest. Revealing these perspectives will provide important information regarding curriculum and course development in technology-based as well as other university courses and programs. Additionally, views of cybersecurity may provide insight regarding potential cybersecurity risks to future employers of students.

THEORETICAL PERSPECTIVE

The 2018 Verizon Data Breach Investigations Report (DBIR) provides detail regarding cyber-attacks. For instance, in 2018, 92-percent of malware was delivered by email via dubious links and phishing schemes. In fact, phishing attacks are considered a top security threat (Fruhlinger, 2018). Additionally, the 2018 DBIR report found that there were over 53,000 incidents and 2,216 confirmed data breaches in 2018, worldwide. An incident is a security event that compromises the integrity, confidentiality or availability of an information asset. A breach is an incident that results in the confirmed disclosure of data to an unauthorized party. Fruhlinger (2018) reported that the average ransomware attack costs a company about $5 million.

Although few studies exist that investigated views of cybersecurity, we found two studies relevant to this study. The first is a broadly distributed survey by The Pew Research Center (Olmstead & Smith, 2017). The other is a study investigating students' conceptual understanding of cybersecurity by Thompson et al (2018). The Pew Research Center report, by Olmstead and Smith (2017),

indicated that Americans in their study distrust corporations and government entities to protect their personal information. However, these same Americans neglect cybersecurity best practices in their personal lives. That study used a broad sample of people and a survey that revealed percentages of behaviors across their questions. Alternatively, Thompson et al (2018) explain that they desire to develop an assessment tool to evaluate student misconceptions regarding cybersecurity. In their study, 25 students from three different universities participated in think-aloud interviews. The results revealed a taxonomy of misconceptions across the students sampled. The authors state that theirs was the first to explore student cognition and reasoning about cybersecurity.

Certainly, the Pew Research Center (Olmstead & Smith, 2017) and Thompson et al (2018) studies offer valuable information. Additionally, we agree with Thompson et al (2018) that the development of cybersecurity education assessment-tools is necessary. However, our approach differs from the Thompson et al (2018) study in that we are interested in divergent perspectives about cybersecurity. In these other studies (Olmstead & Smith, 2017; Thompson et al, 2018), results indicate an overall view but without differentiation of viewpoints. Q allows us to differentiate and describe the variety of viewpoints that exist within our set of participants (called a P-set in Q).

Our student participants are majoring in technology-based careers (e.g. Mechanical Engineering Technology) including careers that require understanding the issues of cybersecurity (e.g. Computer Information Systems – Cybersecurity track). Thus, the participants would all be familiar with technology and computer use yet could easily possess differing views of cybersecurity. Furthermore, investigating subjective viewpoints offers insight regarding behavior as proposed by Stephenson (1953). Finally, the method used here could prove useful in the development of cybersecurity assessment instruments. Additionally, the findings may help inform universities and businesses about how to address cybersecurity issues related to students and employees' behavior especially related to best practices in data security.

RESEARCH METHODS

William Stephenson developed Q methodology [Q] as a means of scientifically studying subjectivity by revealing and describing the divergent viewpoints within a population (Brown, 1980; Stephenson, 1953). Q has been used to study subjectivity within multiple disciplines within the social and behavioral sciences political science, journalism, marketing, environmental studies, health policy studies, and education (Brown, 1980; McKeown & Thomas, 2013; Newman & Ramlo, 2010). An 80 year-old mixed method (Newman & Ramlo, 2010; Ramlo,

2015, 2016), Q consists of a series of qualitative and quantitative interwoven stages (Ramlo, 2015).

An important strength of Q is the ability to describe the multiple viewpoints on a topic. Thus, Q provides greater insight than the more typical Likert-format surveys where there is a loss of meaning as explained by McKeown (2001). For instance, such Likert-format surveys typically offer the average response (from a scale of 1-5 or similar) or percentages of distributions across the scale, like the Pew Research Study. Additionally, in qualitative studies, like that of Thompson et al (2018) mentioned here, researchers develop general themes from the participants' interviews or other means of data collection rather than offering differentiation of viewpoints. Here we were interested in differentiating the viewpoints across the set of participants and, therefore, selected Q for this study.

In Q, after formulation of the research questions, the researchers next develop the concourse of items that offer a broad compilation of the communications on the topic (Brown, 1980; McKeown & Thomas, 2013; Newman & Ramlo, 2010). In this study, the Pew Research Study, the Best Practices webpage from the Department of Homeland Security (DHS, USA), and cybersecurity education expertise of one of the researchers were used to develop the concourse. We acknowledge that other organizations offer best practices webpages such as the National Counterintelligence and Security Center (NCSC) and the National Institute for Standards and Technology (NIST). However, much of the same information is posted on DHS, NCSC, and NIST. In Q, the focus of the concourse is to find differentiated statements.

Initially, the researchers collected 53 statements. Although some statements may offer multiple ideas (e.g. #35 It is important to set strong passwords, change them regularly, and not share them with anyone) yet this is not a problem within Q methodology or the development of the concourse. A theme analysis revealed six unique themes. Themes were identified by the researchers as they sought common patterns / topics across the original concourse. Items were then coded within a MS Excel spreadsheet for ease of sorting and reducing the concourse. The distribution of items across those themes is as follows: Training (4), Personal policy (16), Personal knowledge (12), Government policy (8), Corporations (5), Broad impact (8). The Q-sample, a subset of the concourse, was selected to offer fewer items for participant sorting that still represent the broad communications on the topic. This selection was done using Fisher's Design of Experiments as recommended by Brown (1980). The Q-sample then had a breakdown of items across themes as follows: Training (4), Personal policy (12), Personal knowledge (12), Government policy (6), Corporations (5), Broad impact (8). In sum, the Q-sample consists of 47 items and participants will sort these items

into a grid provided by the researchers (see Figure 1). Item placement represents the salience of each item for the participant (McKeown & Thomas, 2013).

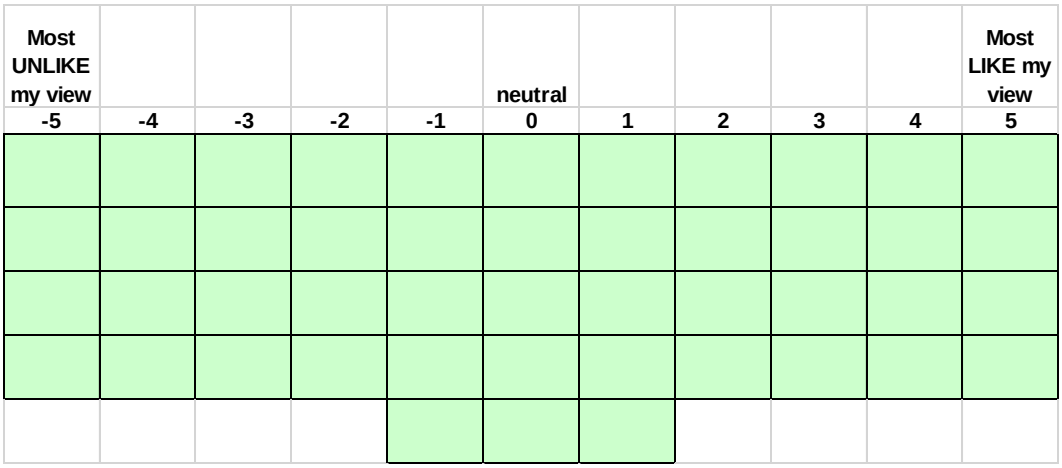

Figure 1 Sorting grid used in this study

It is important to understand that in Q, the sample size is the number of items in the Q-sample (Newman & Ramlo, 2010). It is imperative to have sufficient statements across the range of communications for individuals to sort. Alternatively, the P-set represents the set of participants (Brown, 1980). Although P-sets may use purposive sampling, in this study the researchers were specifically interested in the viewpoints of university students in technology-based degrees including Computer Information Systems and Mechanical Engineering Technology.

The 47, individual Q-sample items were listed within a Microsoft Excel spreadsheet used to collect the concourse, organize the items into themes, and select the Q-sample. The 47 Q-sample items were then randomly numbered using Microsoft Excel's formula =RANDBETWEEN(1,47) and then sorted from lowest to highest. The researchers randomly distributed the items across the Q-sample based upon the recommendations of Brown (1980). Thus, when the researchers offer the Q-sample items, each on an individual slip of paper, to the participants there is no numerical pattern to the items (e.g. Broad Impact items representing consecutive item numbers 1 through 8).

The researchers recruited students to participate by providing their Q-sorts and asking them to sort the 47 items based upon their views of cybersecurity. The researchers provided a grid for distribution of these items. Each sort provides a snapshot of that individual's viewpoint regarding cybersecurity. Participants

typically took approximately 20 minutes to complete their sorts. Factor analysis was used to group similar viewpoints (sorts) into clusters that each represent a unique, divergent viewpoint. Q is such that not only are these viewpoints revealed but also substantial descriptive information is provided for each viewpoint. Additionally, consensus is also revealed within Q studies (Brown, 1980; McKeown & Thomas, 2013; Stephenson, 1953).

The analyses of the sorts in Q involve correlation and factor analysis. The factor analysis groups people with similar views into the same factor based upon their Q sorts; in this way, each factor represents a unique view about the topic (Brown, 1980; McKeown & Thomas, 2013; Stephenson, 1953). Specialized software, in this case PQMethod, is required for data analysis in Q. Specialized Q software provides the required by person factor analysis as well as the detailed tables used for interpretation of each factor (viewpoint) (Newman & Ramlo, 2010). In Q, each factor represents a distinct, divergent viewpoint (Brown, 1980; McKeown & Thomas, 2013). It is important to distinguish Q from R as well. R factor analysis groups items while Q groups people based on their similar viewpoints, as represented by their Q-sorts (McKeown & Thomas, 2013). Post-sort questionnaires and interviews provide additional information to help interpret these viewpoints (factors) (Brown, 1980; McKeown & Thomas, 2013; Newman & Ramlo, 2010). However, demographic information such as race or other characteristics beyond major was not collected because such information is often of little value in Q methodology (Brown, 1980). Additionally, both the CIS and MET degree programs' demographics are predominantly white and male students of traditional college student age. Within this study, students commented on those statements most salient with their viewpoints. The most salient items are those the participant placed at the ends of the Most to Most continuum of Most Like My View to Most Unlike My View. Additionally, students were offered the opportunity to comment on their sorting process including comments about realizations concerning their viewpoint.

RESULTS

Fifteen engineering technology (ET) undergraduates and seven computer-information-systems (CIS) students participated in the study. Two of the ET students self-identified as both ET and computer science (CS) majors. All students were male undergraduates. One faculty member also participated in the study. With the addition of the faculty member, students' views could be judged relative to someone who is known to follow cybersecurity best practices. Additionally, since all other participants were male, due to the male dominance within the majors under study, a female faculty member was added to the study to allow us to also resolve the issue of the overall maleness of the study. Analyses resulted in a three-

factor solution. The post-sort questionnaire responses provided information used during the factor analysis and interpretation stages.

Table 1 contains the factor matrix for the three-factor solution. An X indicates a sorter identified on that factor. Factor 1 represents the faculty member, four ET students, and five CIS students. Factor 2 represents one ET major. Factor 3 represents eight ET majors. Four sorters were not represented by a single factor because they had mixed representation (high correlations with more than one factor).

Table 1 Factor Matrix with an X Indicating a Defining Sort

Q sort	Status	Factor 1 – Best practices	Factor 2 – No worries	Factor 3 – No sense of urgency
1	Faculty	0.6986X	0.0490	0.4123
2	ET	0.0701	0.0314	0.4964X
3	ET	0.5970X	0.0563	-0.0183
4	ET	0.6386X	0.1072	0.2755
5	ET	0.3318	-0.1803	0.5043X
6	ET	0.2393	-0.2788	0.6012X
7	ET	0.3683	-0.0153	0.5374X
8	ET	0.2152	0.5600X	0.0980
9	ET & CS	0.2501	0.0912	0.3327X
10	ET	0.2063	0.4172	0.3970
11	ET	0.3133	-0.3684	0.3791
12	ET	0.4660X	-0.3306	0.1324
13	ET	0.4757X	0.2613	0.1986
14	ET	0.2695	-0.3009	0.5163X
15	ET & CS	0.0375	0.2218	0.4412X
16	ET	0.2285	0.1147	0.5578X
17	CIS	0.4904X	-0.1732	0.2584
18	CIS	0.7320X	-0.0391	0.3335
19	CIS	0.4733	-0.4881	0.2573
20	CIS	0.5837X	0.2242	0.2146
21	CIS	0.5138	0.1907	0.5440
22	CIS	0.7162X	-0.1986	0.1758
23	CIS	0.6464X	0.0438	0.3856

NOTE: ET stands for engineering technology major; CIS stands for Computer Information Systems major. Two of the sorters self-identified as both ET and Computer Science (CS) majors. All sorters, except the faculty member, were male students. The X's indicate sorts that are identified with a factor (viewpoint). Names of factors are based on interpretations described later within this section.

Table 2 Factor array with statement grid positions for each factor, consensus statements (+) and distinguishing statements (*) indicated.

No.	Statement	Factor 1 Grid Position	Factor 2 Grid Position	Factor 3 Grid Position
1+	It is important for everyone to learn how to protect their own personal information.	5	5	5
2+	Screen locks or other security features to access my phone are a nuisance.	-5	-3	-5
3	I feel that it is safe to utilize public WiFi networks for tasks like online banking or e-commerce.	-5	-3	-3
4	It is relatively easy for hackers to infiltrate electronic devices on public WiFi sources like those found in places like coffee shops.	2*	-1*	4*
5	I feel like I am knowledgeable about cybersecurity and preventing a cyber-attack on my electronic devices.	1	2	-3*
6	cyber-attacks and data breaches are facts of life for government agencies, businesses and individuals.	1	3	-2*
7	I do not trust social media organizations to protect my personal data.	2	-3*	1
8	I frequently neglect cybersecurity best practices.	-3*	3*	0*

9	I need cybersecurity training so that I better understand how minor mistakes or simple oversights might lead to a disastrous scenario regarding the security or bottom line of my organization.	0	-5*	2
10	I feel that the U.S. government is at least somewhat prepared to handle cyber-attacks on our public infrastructure.	-1	3*	-2
11+	Major cyber-attacks will be a fact of life in the future.	3	0	2
12+	Technology companies should be able to use encryption tools that are unbreakable even to law enforcement.	-1	-4*	-1
13	The US government should be able to access encrypted communications	-2*	2*	-4*
14+	Everyone who uses a computer or smart-phone should learn about cybersecurity.	4	1	5
15+	It is important to keep critical infrastructure from cyber threats.	5	4	5
16	You should wait to install updates to your operating system, browser, and other critical software until you hear the "bugs" have been worked out.	-1	4*	0
17	I don't see a problem using a social media platform such as Facebook to log in to a third-party site.	-4	-3	-1
18+	Privacy settings on social media and other web-platforms are meaningless.	-3	-5	-1*
19	The U.S. government is prepared to handle future cyber-attacks	-2	2*	-2
20	It is easy to become a victim of an email phishing campaign or other social engineering attack.	0	-2	4*
21+	Sharing passwords with a friend or family member is ok if they are trustworthy.	-2	-2	-2

22	I do not worry about how secure my online passwords are.	-5	5*	-4
23	I trust the federal government to protect my personal data.	-4	5*	-3
24	I don't see a problem using the same password for different accounts. What's the big deal?	-3*	0	1
25+	The government should be able to access encrypted communications when investigating crimes.	-1	1	0
26	I feel that I am careful about how I use the internet and electronic devices.	0	2	4
27	I feel confident that U.S. businesses are prepared to handle attacks on their own systems.	-4*	0	-1
28	I fear I have lost control of my personal information.	-3	-4	-5
29+	Every time we connect to the Internet, we make decisions that affect our cybersecurity.	2	0	3
30+	Passwords are the first line of defense against unauthorized access to user data so I take them very seriously.	4	3	1
31	Companies should maintain robust protocols when it comes to cybersecurity.	5	-2*	3
32	cybersecurity is considered one of the key national security issues of our time.	4	-1*	4
33	Sharing personal information on social media, like your birthdate or best friend's name, is not a threat to your personal cybersecurity.	-4*	-1*	2*
34	The private sector is prepared to handle future cyber-attacks	-1	1	-3*

35+	It is important to set strong passwords, change them regularly, and not share them with anyone.	5	1*	5
36	Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.	4	4	0*
37+	It's worth the hassle to use two-step authentication on at least some of my online accounts.	2	4	3
38	There aren't many careers left that aren't based on technology.	1*	-2*	-5*
39+	Cyber-attackers rely on human error.	1	1	0
40	I worry whether government agencies and major corporations can protect the customer data they collect.	3*	-1	1
41+	Security know-how can advance you in your existing job.	3	-1	2
42	It's a bad idea to write down your passwords on paper.	3*	-4	-5
43+	With attacks becoming more advanced and sophisticated, employee training in cybersecurity is nearly pointless unless you work in IT.	-5	-5	-4
44+	I feel like password management is a stressful and uncertain process.	-2	-5	-1
45	My personal data has become less secure in recent years.	0	0	3
46	It's challenging to keep up with all of the passwords to my various online accounts.	0*	5*	-4*
47	It's a bad idea to have passwords contain whole-words, part of your phone number, etc.	1	-4*	1

Note: Asterisks (*) on grid positions indicate that statement is distinguishing for that factor. A plus (+) after the Q-sample item numbers indicate consensus statements.

Table 2 contains the factor array for this factor solution. The factor array provides the grid position for each Q-sample item for each factor. Thus, each factor array represents the theoretical sort for that viewpoint. Although all three viewpoints (factors) agree that it is important for everyone to learn how to protect their own personal information (Item #1 at +5 for each factor), what that means is different for each of the factors (viewpoints). First, we will briefly describe each viewpoint based on the factor array, including mentioning key distinguishing items for these views. Distinguishing statements are those where the item placement (grid position) is distinct from the others factors' item placement thus differentiating that viewpoint from the others. Next, we will discuss consensus among the viewpoints.

Factor 1 – Cybersecurity Best Practices

Those on the Factor 1 view agree that it is not a good idea to share personal information on social media like birthdates and other information that is often associated with security settings (Statement #33, distinguishing, with factor grid-placements at **-4**, -1, 2, respectively). They agree that they often use cybersecurity best practices (#8, distinguishing, **-3**, 3, 0). They believe in setting strong passwords and changing them regularly as well as not sharing passwords with others (#35, not distinguishing, **5**, 1, 5). Those on this view worry about how secure their online passwords are (#22, not distinguishing, **-5**, 5, -4).

Those on this view believe that companies should maintain robust protocols when it comes to cybersecurity (#31, **5**, -2, 3). However, they do not feel confident that U.S. businesses are prepared to handle attacks on their own systems (#27, distinguishing, **-4**, 0, -1). Similarly, Factor 1 view-holders worry that government and corporations cannot protect the data they keep (#40, distinguishing, **+3**, -4, -5). Sorter #22, a CIS major, commented:

> *I feel that cyber attacks are a fact of life and companies should do their best to stop them. I worry for my online safety and feel that everyone should have some knowledge.*

Similarly, sorter #23, also a CIS major, commented:

> *I believe that everyone should take personal security into their own hands because you have to protect yourself… security features on my phone are extremely important to personal protection. Also, the federal government should not have access to personal encrypted communication unless they have warrants, as that is a violation of privacy.*

Factor 2 – No Worries

Although this view is represented by a single participant, it is important to stress that size is not equivalent to importance especially in Q where the researchers are focused on theoretical importance of the findings, not statistical significance (Brown, 1980). This view frequently neglects cybersecurity best practices (#8, distinguishing, -3, **3**, 0). Unlike the other two views, the Factor 2 view does not worry about how secure their online passwords are (#22, distinguishing, -5, **5**, -4). Unlike the other two views, this view has a neutral response to the importance of setting strong passwords, changing them frequently, and not sharing them with others (#35, distinguishing, 5, **1**, 5). They are not stressed about managing their passwords (#44, distinguishing, -2, **-5**, -1). Yet, only this view does not think they need cybersecurity training to better understand how minor mistakes or simple oversights might lead to a disastrous scenario (#9, distinguishing, 0, **-5**, 2).

The Factor 2 view believes in urban-legends such as waiting to install updates to your operating system, browser and other critical software until you hear the bugs have been worked out (#16, distinguishing, -1, **4**, 0). Similarly, those on this view are somewhat sure that the U.S. government is prepared to handle future cyber-attacks including cyber-attacks on public infrastructure (#10, distinguishing, -1, **3**, -2; #19, distinguishing, -2, **2**, -2). Only those on this view trust the federal government to protect their personal data (#23, distinguishing, -5, **5**, -4). They do not believe that cybersecurity is one of the key national security issues of our time (#32, distinguishing, 4, **-1**, 4). Sorter #8 commented that he trusts the government to protect his personal data. He also stated that the sorting process helped him realize that he does not protect his data as much as he should.

Factor 3 – No Sense of Urgency

The Factor 3 view seems cognizant that they are not very well informed about cybersecurity (#5, distinguishing, 1, 2, **-3**). They feel neutral that they frequently neglect cybersecurity best practices (#8, distinguishing, -3, 3, **0**). Unlike the other two views, the Factor 3 perspective holders believe writing down passwords on a piece of paper is ok (#42, distinguishing, 3, -4, **-5**). Perhaps this is why this view is the only one that does not feel it is challenging to keep up with their passwords to their various online accounts (#46, distinguishing, 0, 5, **-4**). For instance, sorter #2 wrote the following:

> *… I don't see a problem about having the same passwords for different accounts. This is because when you have lots of accounts I might forget them, and writing them on a piece of paper does not help me because I just loose it. Even though I have the same*

> *password on some other account I make sure it's a difficult one that only I can get… If I didn't trust social media organizations then I wouldn't have any social media accounts… I'm not much into cyber security, so I didn't have a clue about some of them. I realized so much things that made me wonder how cyber security is a big problem.*

This view believes that it is easy to become a victim of an email phishing campaign or other social engineering attack (#20, distinguishing, 0, -2, **4**). They believe there are still many careers left that are not based on technology (#38, distinguishing, 1, -2, **-5**). They feel neutral about daily life, economic vitality, and national security depending on a stable, safe, and resilient cyberspace (#36, distinguishing, 4, 4, **0**) yet they are concerned about cybersecurity (#32, 4, -1, **4**). Like Factor 1, they believe that everyone who uses a computer or smart-phone should learn about cybersecurity (#15, not distinguishing, 5, 4, **5**).

Consensus

Consensus is determined when a statement has similar (but not necessarily the same) grid positions between *pairs* of factors. Consensus provides insight into what the divergent viewpoints have in common (Brown, 1980; McKeown & Thomas, 2013). Within this study, consensus includes agreement that it is important to keep critical infrastructure from cyber threats (#15, 5, 4, 5). Screen locks and other security features on smart-phones are not a nuisance (#2, -5, -3, -5). There is agreement that sharing passwords is probably not ok even if that person is trustworthy (#21, -2, -2, -2). The three views are neutral about whether the government should be able to access encrypted communications when investigating crimes (#25, -1, 1, 0). Yet general best practices are not among the consensus statements across all three viewpoints and that is concerning.

Strengths and Limitations of the Study

As Stephenson (1953) explained, one of Q's key strengths is each participant provides their internal viewpoint with their sort without need of a priori assumptions, whereas other methods provide only the external observations of the researcher. Therefore, Q has no need for determining instrument score validity and score reliability (Brown, 1980; McKeown & Thomas, 2013; Newman & Ramlo, 2010; Stephenson, 1953). Additionally, Q was designed specifically to examine the viewpoints of relatively small groups of people or even an individual sorting under multiple conditions of instruction. Q's ability to provide descriptions of the

divergent viewpoints and consensus can provide important related to education, assessment, and other situations (Newman & Ramlo, 2010).

It is important to stress here that generalizability in Q is very different from the generalizability often expected from large-scale quantitative studies. In Q, the Q factors represent generalizations of perspective such that they describe how persons of a certain perspective think about the topic under investigation (Brown, 1980; Thomas & Baas, 1993). This is a type of substantive generalizability and is different from the idea of statistical inference, where the purpose is generalizing to a larger audience from a large, random sample of participants (Thomas & Baas, 1993).

CONCLUSIONS

Few studies have investigated views of cybersecurity. In this study, multiple cybersecurity viewpoints emerged for university students in specific degree tracks that are connected to technology (e.g. Mechanical Engineering Technology) and the cybersecurity track of a Computer Information Systems degree. Because all of these degree tracks should offer informed perspectives concerning cybersecurity, the findings will inform university faculty and administrators about their students' views and lead to discussions about curriculum changes to address certain viewpoints.

Within this study, Factor 1, Cybersecurity best practices, represents five of the seven CIS (Computer Information Systems) students. The remaining two CIS majors had mixed loadings (representation) between Factor 1 and Factor 2 (*No Worries*). No CIS students are represented by the other two factors. This indicates that the CIS program is effective although more data is necessary.

However, Engineering Technology majors are represented across all three factors indicating that although some are aware of and practicing cybersecurity best practices, others have *No Worries* or *No sense of urgency* concerning cybersecurity. Additionally, recall that the Likert-format survey results of Olmstead and Smith (2017) indicated that Americans distrust corporations and government entities to protect their personal information. However, the No Worries view does trust these entities to provide cybersecurity and protect their personal information. This difference helps stress the need to reveal and describe the divergent viewpoints about cybersecurity. Yet, in agreement with Olmstead and Smith (2017), both No Worries and No sense of urgency views neglect cybersecurity best practices in their personal lives. However, the Cybersecurity best practices view strives to always be cognizant of cybersecurity risks. Thus, the use of Q methodology indicates that multiple viewpoints exist within this study. Additionally, these findings indicate a need for college students, even those in technical majors, to take a course that

includes cybersecurity threats and best practices. Fortunately, such a course was introduced within the Mechanical Engineering Technology (MET) program at the institution under study. The effect of this course on future MET students' views of cybersecurity is warranted.

Other future studies are indicated as well, based on our findings. A pretest / posttest study design would provide insight about how views of cybersecurity within the CIS program as well as the new course for MET students change after instruction. Future research could use an expanded set of participants including a broader range of university students, university faculty, and/or business employees. Researchers could use Q to investigate employees' views of cybersecurity, estimate risk for experiencing phishing schemes and other cyber threats, and develop targeted training to address specific deficiencies.

REFERENCES

Brown, S. R. (1980). *Political subjectivity: Applications of Q methodology in political science*. New Haven, CT: Yale University Press. Available for free download from https://qmethod.org/portfolio/brown-1980-political-subjectivity/

Fruhlinger, J. (October 10, 2018). Top cybersecurity facts, figures and statistics for 2018. CSO. Available at https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html.

McKeown, B., & Thomas, D. (2013). *Q methodology*. Newbury Park, CA: Sage Publications.

Newman, I., & Ramlo, S. (2010). Using Q methodology and Q factor analysis to facilitate mixed methods research. In A. Tashakkori, & C. Teddlie (Eds.), *Handbook of mixed methods in social & behavioral research* (2nd ed., pp. 505-530). Thousand Oaks, CA: Sage.

Olmstead & Smith (2017). Americans and Cybersecurity. Pew Research Center. Available at http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf

Ramlo, S. (2015). Theoretical significance in Q methodology: A qualitative approach to a mixed method. *Research in the Schools, 22*(1), 68-81.

Ramlo, S. (2016). Mixed method lessons learned from 80 years of Q methodology. *Journal of Mixed Methods Research, 10*, 28-45. Available at http://mmr.sagepub.com/content/10/1/28.full.pdf+html. DOI: 10.1177/1558689815610998.

Stephenson, W. (1953). *The study of behavior: Q-technique and its methodology*. Chicago: University of Chicago Press.

Thomas, D. B., & Baas, L. R. (1993). The issue of generalization in Q methodology: "Reliable schematics" revisited. *Operant Subjectivity, 16*, 18-36. doi:10.15133/j.os.1992.014

Thompson, J. D.; Herman, G. L.; Scheponik, T.; Oliva, L.; Sherman, A.; Golaszewski, E.; Phatak, D.; and Patsourakos, K. (2018) "Student Misconceptions about Cybersecurity Concepts: Analysis of Think-Aloud Interviews," *Journal of Cybersecurity Education, Research and*

Practice: Vol. 2018 : No. 1 , Article 5. Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/5

Verizon Data Breach Investigations Report (2018). 11th edition. Available at https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf.