**DCJ 720 Perceptions of security in cybersecurity**

Robert Chapa

Saint Leo University

**Abstract**

This paper aims to uncover cybersecurity professionals' perceptions of why cybersecurity attacks on U.S. infrastructure have significant efficacy. The study will use the recent 2021 colonial pipeline attack as a reference point for discussion. However, the study will focus on a qualitative semi-structured interview methodology guided by interpretivism and its subcomponent symbolic interactionism. Twenty professional cybersecurity experts currently employed within a 100-mile radius of Newport Richie, Florida, will be interviewed to highlight areas of cybersecurity vulnerability due to policy non-compliance. Latent themes from the interviews will be discussed and analyzed to retrieve potential reasons for the non-compliance and complacency of cybersecurity professionals asserted in cybersecurity research. Critical content analysis will be conducted on all the codes to develop these themes. Due to the projected increase in ransomware attacks on critical American infrastructure, this type of research is essential for self-analysis and the development of new and vital policies in cybersecurity.

**Introduction**

In cybersecurity, professionals are often caught unprepared by ransomware attacks or other cyber-attacks on systems. Critical infrastructure is often targeted, and attacks are expected to increase in the near future. Organizations are known to hire the most vital cybersecurity experts and pay them high salaries, yet breaches continue to expose security flaws. The attack on the Colonial Pipeline in 2021 exemplifies the problem. The ransomware attack on Colonial Pipeline paralyzed the eastern seaboard and caused billions of damages. Although the entire investigation is ongoing, cybersecurity experts assert that the breach could have been prevented if the federal guidelines regarding critical infrastructure security had been followed. Additionally, some of the vulnerabilities were created by a lack of common protocol enforcement. These security violations are not exclusive to Colonial Pipeline.

**Literature Review**

On May 8, 2021, the Colonial pipeline was breached by malicious actors in a ransomware cyber-attack. The attackers were able to disrupt the oil flow impacting the entire eastern coast. Gas prices increased dramatically, and thousands of canceled or stopped flights. The effect was not only financial dollars lost revenue for businesses but was also psychological because they form cyber was able to initiate attacks from thousands of miles away, impacting critical American infrastructure. Business owners and the general population began panic buying causing even more goods and services shortages. Ransomware attacks continue to be a formidable threat to businesses, academia, government, and critical infrastructure (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Colonial Pipeline Co. attack: What happened*, 2021; Gallagher et al., 2021; Menn & Bing, 2021; Osborne, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021).

In the United States, the TSA is responsible for security guidelines of pipeline infrastructure. Unfortunately, these are not legal consequences if not followed. The government relies on the integrity of for-profit privately-owned companies to follow the procedures to secure their computer systems, hardware, and physical infrastructure. Problems arise, however, when even the policies are not in force. Investigations into Colonial pipeline and other breaches have found that the primary culprit is the security team becoming complacent and feeling to secure the entrusted computer systems. CEOs and senior administrators of these companies are usually non-technical and therefore do not understand cybersecurity. They fail to implement good policy, and worse, they do not know the right questions to ask their cybersecurity experts. This administrative disconnect allows for a significant lack of oversight of the cybersecurity team and adds to the organization's vulnerabilities (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Colonial Pipeline Co. attack: What really happened*, 2021; Gallagher et al., 2021; Pankov, 2021; Parfomak & Jaikaran, 2021).

An additional issue that impacts all areas of cybersecurity is the lack of sufficient understanding and urgency regarding cybersecurity from lawmakers. Malicious actors and their technical abilities far outpace the legal system's ability to react. There is an issue regarding lawmakers' cognitive abilities to comprehend these high-end issues. The procedure itself is not geared for rapid reaction. The legal system is a slow-moving mechanism incompatible with the speed of technological advances. This creates an additional vulnerability by hamstringing law enforcement and allowing to threaten critical infrastructure further. The lack can see an example of this of legislative enforcement over the use of drones. There have been attempted infrastructure attacks or surveillance by malicious actors using drone technology. Malicious actors are becoming more and more sophisticated in using new technologies informed not only by drones and ransomware, combining different cyber-recognized tools to increase the efficacy of their attacks (Heen et al., 2018; Helmer, 2019; Matiteyahu, 2015; Pupillo, 2018; Reynolds, 2020; West & Bowman, 2016).

Ransomware on critical infrastructures, such as the colonial pipeline incident, requires an in-depth malware review. The discussion must include the source of ransomware and the threat vector, and its countermeasures. Currently, organizations fear ransomware attacks for a good reason. This malware has been used effectively against organizations in all sectors to generate profits and cybercriminal groups. Ransomware is allowed to penetrate firewalls of the computer system and is difficult to detect and remove. It will propagate itself through a network infecting all of the systems. It will encrypt all folder files and even entire hard drives with unbreakable encryption. Afterward, the malware will post a message to the victims demanding payment for the release of their information. Additionally, the ransom must be paid in cryptocurrency such as bitcoin, making the transaction invisible. Law enforcement has had limited success in tracing these transactions and bringing criminals to justice (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Colonial Pipeline Co. attack: What really happened*, 2021; Gallagher et al., 2021; Osborne, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Sallinen, 2021).

Criminal gangs with state support have had success in attacking American infrastructure. These malicious actors work with the help of state sources and without fear of retribution or consequences. In the case of the Colonial pipeline, the criminal gang Revil was supported by the Russian government. Additionally, much of the hacking code was purchased on the dark web. Entities on the dark web sell ransomware (RaaS)for anyone to buy. A criminal entity called DarkSide is notorious for offering hacking software, including ransomware as a service (RaaS), on the dark web for purchase. Reveal utilized Darkside's ransomware hacking software and its attack on Colonial pipeline. In the Revils attack on the Colonial pipeline, a set of credentials was also purchased from Darkside. Many criminal hacks have been supported by software offered by Darkside on the dark web (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Colonial Pipeline Co. attack: What really happened*, 2021; Gallagher et al., 2021; Osborne, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

Many products can be purchased with malicious intent on the dark web. In addition to ransomware software, the dark web offers a marketplace for buying cybercrime services. For example, ransomware kits are sold for as little as $66. Collections of compromised personal computers used for launching attacks can be purchased for $0.13 a system. Denial of service attacks is available for $311. The set of credentials used by Revil in its attack on the Colonial pipeline was purchased for under $150. Because cybergangs do not have to worry about consequences from the governments in which they reside, there is minimal risk of deterring them. They have a high benefit to cost value(*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Colonial Pipeline Co. attack: What really happened*, 2021; Gallagher et al., 2021; Osborne, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

I.T. personnel must maintain a vigilant watch over the systems they are responsible for due to the many computer assets that offer threat vectors. Computer assets and vectors consist of routers, networks, and various computer systems. The problem is that many of these computer systems are connected to the Internet and thus provide different vectors for compromise. I.T. personnel can never become complacent, falling into the trap of not worrying about an attack since one has not happened up to that point. Every day the Thomas Botts search the Internet for vulnerable systems to compromise. Occasionally specific sites, organizations, or entities are explicitly targeted. Even so, if I.T. personnel were to follow the recommendations provided by the government and other security professionals, most could be sufficiently protected. In the case of Colonial pipeline, the previous I.T. member had used their VPN credentials for various other accounts. Using a single password is shared among the general population, as people want to remember a single password and use it for multiple accounts. When one of those accounts is compromised, a Thomas Botts or malicious actors will assume that that password is used in other systems. Often this proves to be correct and provides easy hacking for malicious actors (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Colonial Pipeline Co. attack: What really happened*, 2021; Gallagher et al., 2021; Osborne, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

Furthermore, they must follow suitable protocols and disable former employees' VPN access credentials when no longer employed. The colonial pipeline ransomware attack would not have happened if this single step had been implemented, costing billions of dollars. The second criticism of I.T. personnel is not providing sufficient backup or gapped backups to prevent corruption or compromise of systems. Had a backup system been gapped and adequately secured, Colonial pipeline would have been able to recover from the hack more quickly with a clean backup database. These oversights by I.T. personnel are common, costing companies millions of dollars every year. They stem from a sense of security that encourages them to say we are too small of a company or non-threatening for anyone to take the time to target us (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Colonial Pipeline Co. attack: What really happened*, 2021; Gallagher et al., 2021; Johnson, 2015; *Microsoft digital defense report*, 2021; Osborne, 2021; Parfomak & Jaikaran, 2021; *Ransomware guide*, 2020; Turton & Mehrotra, 2021).

Many companies still do not report hacks or breaches on their systems in the private industry due to fear of losing their clients. More recently, bills have been proposed in Congress to require reporting breaches or hacks. Policy or even the laws that require this type of reporting is difficult to get organizations to comply with due to the difficulty of proving that the laws or policies were ignored. In the case of the Colonial pipeline, ministration made a fast decision to report the ransomware attack. Reporting proved to be the right decision, and the authorities reacted quickly. Moreover, although the Colonial pipeline did pay a $5 million ransom, law enforcement was able to recover a few million dollars of it (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Colonial Pipeline Co. attack: What really happened*, 2021; Gallagher et al., 2021; Johnson, 2015; *Microsoft digital defense report*, 2021; Osborne, 2021; Parfomak & Jaikaran, 2021; *Ransomware guide*, 2020; Turton & Mehrotra, 2021).

The current Biden administration has been aggressive in retaliating against cybercriminals. In the case of the Colonial pipeline, the Biden ministration authorized the U.S. military, the TSA, the U.S. Department of Justice, and other agencies to counter with cyberattacks and even direct means. Working together, these government departments attacked Revil and DarkSide, significantly impacting their operations and funding. Furthermore, the Biden ministration via the U.S. State Department offered $10 million bounties for actionable information on the members of DarkSide and Revil. The U.S. government has provided bitcoin instead of American dollars as payment. By doing so, the U.S. government ensured for the witnesses who claimed the bounties. These actions marked a paradigm shift in how the U.S. government handles critical infrastructure attacks. Before, such a fast and interagency collaborative effort was made using bitcoin and military/civilian hacking countermeasures. The United States waged an invisible war in the cyber world against DarkSide and Revil. DarkSide's business websites were taken offline, their newsgroup feeds were interrupted, and even their leader had to go into hiding. There can be little doubt that state-sponsored cyber warfare will continue to cause significant damage to the United States and its interests. Only through solid vigilance and countermeasures can we remain secure (Chipolina, 2021; *Colonial Pipeline Co. attack: What really happened*, 2021; Fung, 2021; Johnson, 2015; Khraisat et al., 2019; Turton & Mehrotra, 2021; XiaoLing, 2020).

All of the research sources provided information on the significant breaches of organizations. A deep discussion of the Colonial pipeline breach was examined in several of the articles. The issues and preventable causes were also discussed in depth. Other sources discussed in-depth technical hacking methodology. A few sources addressed the government's response and the difficulties of lawmakers keeping up with fast-moving technology. For the literature review sources, no references could be found that did a qualitative interview of security experts to search for common traits or actions leading to the failure or success of cybersecurity in an organization.

**Importance**

I.T. professionals' perceptions of security in cybersecurity are critical for organizations' safety, particularly essential infrastructure entities. Why I.T. professionals fail to implement continuous vigilant management of the computer systems in their domain of responsibility is a question that has not been answered. In nearly every hack or breach, professional cybersecurity investigations reveal complacency and lack of concern by I.T. staff. The ongoing behind-the-scenes war between the United States' critical infrastructure and hostile foreign enemies has only begun. Cybersecurity staff must consider themselves soldiers in an undeclared war with multiple enemies that will strike without provocation or notice. The first step to addressing adequate cybersecurity actions is understanding the underlying reasons for complacency and lack of effort.

**Theoretical Perspective**

The theoretical perspective for this study will use interpretivism and its subcomponent symbolic interactionism. Interpretivism falls under the epistemology of constructionism. It uses the methodology of survey research and an interpretive approach. It will be used in this study with observations, discussions, and interviews. This perspective relies heavily on the idea that truth or meaning depends on the mind; therefore, its existence relies on a person's engagement with reality. An individual's perspectives, perceptions, and experiences are critical in constructing their view world. Interpretivism aims to reveal the subjects' interpretations of reality within their social and cultural context. This perspective requires details about the subject's background in the studied context. The issue is critical for the events and situations which are being investigated. It is common for interviews, observations, and a review of records and documentation in this theoretical perspective. The socialization process is fluid and dynamic in its application (Crotty, 1998; Mertens & Wilson, 2012).

Cybersecurity professionals in critical infrastructure organizations encounter attempted hacks and breaches while dealing with various policies, guidelines, and oversight from multiple authorities, including their administrators. The symbolic interactionism perspective allows for the investigation of cybersecurity professionals' perceptions and an examination of their comprehension and decision-making during their defense of the cyber-attack. Included with these actions is the influence of their biases, assumptions, and ideas that have been developed or constructed throughout their careers. These traits play a critical role in their actions before and after a cyber-attack. This study seeks to examine and tease out the perceptions, biases, and ideas using interview methodology to identify underlying correlations with reported cybersecurity weaknesses. Ultimately, the goal is to uncover why complacency, lack of action, and disregard for policy continue to plague I.T. departments.

**Research Questions**

Non-technical administrative executives make false assumptions about the security implementations by their I.T. departments. Additionally, some I.T. departments have a single cybersecurity manager with little to no oversight over this one all-powerful person. Research examining this question reveals areas of cybersecurity weaknesses. There was often a single point of failure in several breaches or hacks that allowed the malware to infect the systems. Investigations reveal continuous complacency and lack of preparation for cyberattacks. Research needs to be conducted to assist with teasing out some of the correlations and potential explanations for these deficiencies in cybersecurity (*Cyber storm 2020: After-action report*, 2021)

Q1. What were the gaps between the senior administrators and technical staff's understanding of countermeasures for cyber threats?

Additional blame can be laid at the feet of lawmakers. Research reveals that Congress fails to understand the weaknesses in the current infrastructure protection laws that led to inadequacies, such as the colonial pipeline ransomware attack 2021. Congresses' lack of understanding extends into a technological disconnect that prevents them from fully understanding cybersecurity vulnerabilities. Furthermore, this lack of knowledge has allowed Congress to create current infrastructure laws that weaken enforcement and let private infrastructure consider their guidelines as recommendations or suggestions with little to no consequence (Colonial Pipeline Co. attack: What happened.

Q2. How did U.S. Congress's lack of technological understanding impact the laws that have been implemented to secure American infrastructure against cyberattacks?

Given the increasing cyber threat, it is surprising that many I.T. departments are reluctant to implement appropriate countermeasures. Investigations into cyberattacks often show that senior I.T. administrators have become complacent and dismiss the cyber threat altogether. Additionally, a false sense of security is often embraced. Policies that promote compliance must be implemented. Studies have also shown that executives responsible for America's infrastructure must understand the importance of funding their I.T. departments and the severe consequences of non-compliance. There has been insufficient research to tease out the reasons for non-compliance and complacency (*Cyber storm 2020: After-action report*, 2021).

Q3. Why do some I.T. departments fail to take appropriate countermeasures for ransomware and other cyber-attacks?

Evidence collected by various cybersecurity organizations in the U.S. government confirmed that the cybercriminal gang used ransomware to compromise the Colonial pipeline, understanding which technical applications are available and how they are used to create countermeasures for other infrastructure cybersecurity. Additionally, the U.S. Department of State offered a bounty for the information leading to the rest of those involved in the crimes. In the past, they have been successful in identifying criminals. Understanding new techniques and methodologies can help focus on where to implement these bounties. Furthermore, evidence suggests that cybercriminals utilize the methods to authenticate their activities and transactions. It is critical to understand which technology cybercriminals use for law enforcement to bring cybercriminal to justice (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021)

Q4 How did new cyber threat techniques and methodologies contribute to recent ransomware attacks?

**Methodology**

Semi-structured interviews were selected as the choice of methodology because of their malleable nature. It also is a natural methodology for interpretivism and its subcomponent symbolic interactionism theoretical perspective. Additionally, it allows for focused questions but will encourage the subject to answer openly and branch off into other discussion points. Sub-topics are prepared in advance with the goal of specific questions emerging as the interview progresses (Arksey & Knight, 1999). The method also allows the researcher to re-focus or follow along with the new thread created by the subject. Semi-structured interview methodology also works exceptionally well for small groups (Drever, 1995). Since this study will use only 20 cybersecurity professionals, semi-structured interviews are the best choice for retrieving data. The methodology is concerned with flexibility and deriving helpful information during the interview (Alvarez & Urla, 2002).

The data source will be interviews conducted on a sample of the cybersecurity professional population. These are defined as individuals employed through private contracts or full-time staff as cybersecurity professionals in industry or the public sector. The study population will consist of selected convenience sampling from the cybersecurity professional population. Twenty cybersecurity professionals will be contacted to participate in the interviews. The 20 cybersecurity professionals are identified as working in industry or education information technology departments located 100 miles from New Port Richey, Florida. Contact with the interview candidates will be initiated via a phone call. Emails will not be used until after the phone call contact because too many working professionals will not answer unsolicited emails. After contact is made via a phone call, emails will be exchanged to further communication and coordinate a date, time, and place for the interview.

The IRB may have issues with the interview study, confidentiality, and anonymity of the interview participants. Confidentiality is critical for the participants because of the possibility of retribution, including termination from the respective employers. Anonymity is equally essential due to the likelihood of information technology administrators learning about the research study. Ensuring the employment security of the subjects is a primary concern in this research. Anonymity is also essential because the subjects will be encouraged to open up about sensitive topics that, if they became known, could also cause damage to the respective employers. Although less likely, there is also a concern of stress and anxiety induced by uncomfortable questions in the interviews. The safety and mental well-being of the subjects is paramount (e.g., “see Appendix B”).

The interviews will be administered in person and off-site from their employment. Ideally, a quiet coffee shop in midafternoon would work well for these interviews. Hopefully, the relaxing atmosphere and coffee aroma will ease these tensions and assist subjects with relaxation. Midafternoon in the coffee shops tends to be quiet as the researcher has noticed that there are few people in the coffee shops and plenty of space for privacy. The choice coffee shop for these interviews would be Panera or Starbucks. The discussion will be conducted informally using a semi-structured interview question methodology. Opening questions will be used to establish rapport and explain the interview process.

The interview length will be anywhere from 45 minutes to one hour. The size of the interview was chosen average length of a lunch break. The discussions will begin on June 1 and be completed by August 15. The dates correspond with a typical summer break for colleges and educational institutions. Summer tends to be the slowest time for this population group. There is a lull regarding workload and assignments for most I.T. staff in the summer months.

The cost of the study should be minimized to transportation costs in terms of gas. A cup of coffee or beverage will also be included in the survey's price for both the researcher and the subject. The use of a hybrid vehicle will help minimize the cost of fuel. $1000 will be allocated for this study. However, the study will likely only cost $500 to $600. The cost of lunch will not be included in the studies budget since lunch would have to be purchased regardless of the study being conducted. No lunch will be offered to the subjects.

The semi-structured interview instrument will consist of 10 cybersecurity questions. The questions were designed to prompt the subject to discuss a different aspect of their work. An iPhone will be used to record the interview. The interviewer will also use a computer for quick note-taking. For an easy ice breaker, the interviewer will introduce himself as a fellow cybersecurity professional conducting research for a doctoral program. The purpose is to create rapport with the subject. Some shop talk about cybersecurity will help with the goal of establishing common ground and experiences. After the ice breaker, the interviewer will ask open-ended questions about why the subject chose the field of cybersecurity. Each of the following questions is designed to allow for sub-questions and prompts for clarification. The goal will encourage cybersecurity experts to freely discuss all the topics they deem essential to their world. Although the interview questions will start with broad and general inquiries, they will progress to in-depth questions focusing on clarity. The interviewer will do interjections of thought-provoking questions. Furthermore, the cybersecurity expert will be asked to sign an informed consent to participate in the research form (e.g., “see Appendix A”). The purpose of the study and assurances of ethical use of the work will be given, and a promise to share the research findings (e.g., “see Appendix B”).

Start codes for this study will be technology, cybersecurity, mobile cell phone, fear, hackers, victims, and administration. Technology was chosen to encompass multiple mentions of technical equipment such as servers, routers, switches, computers, and cables. Cybersecurity was chosen to code for the mention of different countermeasures and active tasks to prevent hacks or breaches. Mobile cell phones were included to code for the mention of cell phones as they are used commonly for notifications of system failures and warnings. Fear was chosen as an open code for listing moments when the subject expressed the emotion of fear regarding compromise systems or retribution from the administration through words or action. Hackers were chosen as an open code for assigning malicious actors or malware that may cause harm by infecting the system. Victims were selected to code for moments when the subjects mentioned an attack that might have harmed an employee, colleague, or other individuals. The administration was chosen as an open code for the mention of administrators who either help or hurt cybersecurity goals and missions.

After the interview, extensive field notes will be written. Later, the recorded interview will be transcribed. The transcription will be the source and unit of observation. Open codes created during the interviews will be reviewed for any themes and topics that emerge along with focus or axial coding. Manifest and latent content will be derived from the source and field notes. The observations and coding for body language will be taken from the field notes. Memos will assist with clarifications of the interviews and evaluate concerns and insights. Afterward, the review methods will use qualitative content analysis for the coding and interpretation. Content analysis is a method for classifying and assessing the interview-coded material to discover the hiding meaning of the data. Additionally, latent themes will be considered. Re-coding will be done as the codes are synthesized. Lastly, the source data will be kept on a secured laptop with a single copy located on a secured external backup drive. After the study, all of the source material will be destroyed (e.g., “see Appendix A”).

**Possible limitations**

Limitations of this study are funds, access to professional cybersecurity workers, and time. Because the funding for this study is coming from the researcher, the scope of the study must be limited to the minimum number of interviewees that will still return reliable information. The number is limited to the minimum number of 20 subjects, but the distance traveled is also limited. The researcher cannot travel beyond a hundred-mile radius without incurring high costs in terms of gas and possible hotel stays. Funding also impacts the ability to hire a professional transcriber for transcribing interviews. Therefore, all discussions have to be transcribed by the researcher. This limitation extends into the barrier of time. With the limitation of likely agreements to be interviewed by working substrate professionals to the summer months, the timeframe of the interviews is limited to three months. It is also possible that the subjects' perceptions would differ if they were being interviewed at other times of the year.

Furthermore, access to working professionals is also hampered by multiple factors such as willingness to discuss cybersecurity issues. Cybersecurity professionals are, by nature, private and closed-mouth individuals. Additionally, finding the sample population who would be willing to meet and discuss these issues while being recorded may be a severe limitation to the scope of the study. Additionally, even though the summer months are less impactful to cybersecurity professionals, their workload may still inhibit them from wanting to take time out of their day to meet. Further limitations include the possibility of skewed data because the convenience sample represents a small group in central Florida. The findings of the study may not extend to cybersecurity professionals nationwide. Limiting researcher bias may also be a problem. Although the researcher has extensive knowledge in cybersecurity, this knowledge may bias the interpretation of data in the development of latent codes. Furthermore, the small sample size may limit the validity of the findings.

**Core Value**

My personal development while being a student at St. Leo is evidenced by the changes I experienced in my attitude towards my classmates over the four classes I have taken here. As a practicing Catholic, I believe in continued personal development and strive for the acceptance of all people regardless of differences in beliefs. When I started as a student here, I had difficulty connecting with my classmates because most were right-wing Republicans. I find it challenging to communicate with a group of people who tend to be close-minded and unaccepting of those who are different from themselves. However, as classes have progressed, we have developed mutual respect regardless of these differences. One person I respect immensely because of her academic excellence is Jessica. Even though we have sparred repeatedly over our time at St. Leo, she has earned my respect and admiration. I have also developed a close relationship with Sal. Despite our differences in our political and social beliefs, we have a common background from our military service.

**Conclusion**

Using the theoretical framework of interpretivism ended subcomponent symbolic interactionism for this qualitative semi-structured interview is essential to research for uncovering cybersecurity professional perceptions of why cyber-attacks on the U.S. critical infrastructure have efficacy. The methodology suits a small sample size perfectly. Critical content analysis will reveal latent themes and meaning from the 20 transcribed interviews. The interview questions will discover why cybersecurity professionals and administration fall into non-complacency and a false sense of security. Although the convenience sample of cybersecurity professionals will be from a 100-mile radius of Newport Richie, the study results may apply to cybersecurity professionals nationwide. Furthermore, cybersecurity research on non-compliance is slim. This is disturbing when one considers that ransomware attacks and other cyber attacks are projected to increase significantly in the near future.

**.**

**References**

Alvarez, R., & Urla, J. (2002). Tell me a good story: Using narrative analysis to examine

information requirements interviews during an ERP implementation. *The DATABASE for Advances in Information Systems*, 33(31), 38-35

Arksey, H., & Knight, P. (1999). Interviewing for social scientists: An introductory resource with examples. *Thousand Oaks: SAGE Publications.*

*Back to basics: A deeper look at the Colonial Pipeline hack*. (2021). Government technology. Retrieved December 3 from <https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack>

Chipolina, S. (2021, August 16, 2021). *U.S. Government to offer dark web informants bounties in crypto*. Decrypt. Retrieved November 21 from <https://decrypt.co/78609/us-government-offer-dark-web-informants-bounties-crypto>

*Colonial Pipeline Co. attack: What really happened*. (2021). cybertalk.org. Retrieved November 4 from <https://www.cybertalk.org/2021/06/09/colonial-pipeline-co-attack-what-really-happened/>

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*. Sage.

*Cyber storm 2020: After-action report*. (2021). Cybersecurity and Infrastructure Security Agency. Retrieved November 4 from <https://www.cisa.gov/sites/default/files/publications/Cyber_Storm-2020_After-Action-Report_01052021_Final.pdf>

Drever, E. (1995). Using semi-structured interviews in small-scale research. A teacher's guide. *Edinburgh: Scottish Council for Research in Education*.

Fung, B. (2021). *Colonial Pipeline says ransomware attacks also led to personal information being stolen*. CNN. Retrieved November 21 from <https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html>

Gallagher, S., Loman, M., Mackenzie, P., & Pollat, Y. (2021). *A defender's view inside a DarkSide ransomware attack*. Sophos News. Retrieved December 2 from <https://news.sophos.com/en-us/2021/05/11/a-defenders-view-inside-a-darkside-ransomware-attack/>

Heen, M. S. J., Lieberman, J. D., & Miethe, T. D. (2018). The thin blue line meets the big blue sky: perceptions of police legitimacy and public attitudes towards aerial drones [Article]. *Criminal Justice Studies*, *31*(1), 18-37. <https://doi.org/10.1080/1478601X.2017.1404463>

Helmer, J. (2019). Drone units serve as eyes in the sky for campus police [Article]. *University Business*, *22*(6), 11-11. <https://saintleo.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=ehh&AN=138425246&site=ehost-live&scope=site>

Johnson, R. (2015). *Security policies and implementation issues* (2nd ed.). Jones & Bartlett Learning.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets, and challenges. *Cybersecurity*, *2*(1), 1-22. <https://doi.org/10.1186/s42400-019-0038-7>

Matiteyahu, T. (2015). Drone regulations and fourth amendment rights: The interaction of state drone statutes and the reasonable expectation of privacy [Article]. *Columbia Journal of Law & Social Problems*, *48*(2), 265-307. <https://saintleo.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=101109410&site=ehost-live&scope=site>

Menn, J., & Bing, C. (2021, Friday, October 22). Exclusive: Governments turn tables on ransomware gang revil by pushing it offline -sources. *The Star*. <https://www.thestar.com.my/tech/tech-news/2021/10/22/exclusive-governments-turn-tables-on-ransomware-gang-revil-by-pushing-it-offline--sources>

Mertens, D. M., & Wilson, A. T. (2012). *Program evaluation theory and practice: a comprehensive guide* (1st ed.). Guilford Press.

*Microsoft digital defense report*. (2021). Microsoft. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi>

Osborne, C. (2021). *DarkSide explained: The ransomware group responsible for the Colonial Pipeline attack*. Zero Day. Retrieved December 2 from <https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/>

Pankov, N. (2021). *How Colonial Pipeline managed its ransomware attack: Should you contact authorities about ransomware?* Kaspersky. Retrieved November 4 from <https://www.kaspersky.com/blog/pipeline-ransomware-mitigation/39907/>

Parfomak, P. W., & Jaikaran, C. (2021). *Colonial Pipeline: The DarkSide strikes*. Congressional Research Service. Retrieved November 4 from <https://crsreports.congress.gov/product/pdf/IN/IN11667>

Pupillo, L. (2018). E.U. Cybersecurity and the Paradox of Progress. *CEPS Policy Insight*(2018/06).

*Ransomware guide*. (2020). Multi-State Information Sharing & Analysis Center Retrieved from <https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf>

Reynolds, M. (2020). Do police drones foster trust or threaten civil rights and privacy? [Article]. *ABA Journal*, *106*(3), N.PAG-N.PAG. <https://saintleo.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=143450703&site=ehost-live&scope=site>

Sallinen, M. (2021). Weaponized malware, physical damage, zero casualties–what informal norms emerge in targeted state-sponsored cyber-attacks?: The dynamics beyond causation: an interpretivist-constructivist analysis of the U.S. media discourse regarding offensive cyber operations and cyber weapons between 2010 and 2020. In.

Turton, W., & Mehrotra, K. (2021). *Hackers breached Colonial Pipeline using a compromised password*. Bloomberg. Retrieved November 21 from <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>

West, J. P., & Bowman, J. S. (2016). The domestic use of drones: An ethical analysis of surveillance Issues [Article]. *Public Administration Review*, *76*(4), 649-659. <https://doi.org/10.1111/puar.12506>

XiaoLing, W. (2020). Criminal law protection of cybersecurity considering AI-based cybercrime. *Journal of Physics: Conference Series*, *1533*(3). <https://doi.org/10.1088/1742-6596/1533/3/032014>

**Appendix A**

**Semi-structured cybersecurity questions:**

Topic: Organizational perceptions of cybersecurity

Interview subject: Cybersecurity professional employed at a local college

1. Why did you choose the occupation of cybersecurity professional?
   1. How did your family influence your decision?
   2. Discuss if movies or the media influenced your decision?
2. Please walk me through a cybersecurity incident that has recently occurred.
   1. What was the context of the incident?
   2. How did you react to the incident?
   3. How did you work with administrators to address the incident?
3. Discuss what your biggest fears are when reviewing security alerts.
   1. Talk about the impact of the security monitoring software on the amount of time you spend checking on security alerts and notices.
   2. Discuss the level of confidence in your organization's security monitoring software.
4. How does your administration demonstrate its commitment to cybersecurity.
   1. What actions have they taken or not taken to make you feel this way?
5. How do you think IT should be budgeted for cybersecurity?
   1. What areas of cybersecurity have sufficient or insufficient funding for the increase in cyber-malware?
6. Explain the IT plan for dealing with a ransomware attack?
   1. Explain what conditions the administration would pay hackers to remove the ransomware?
7. How has the IT administration adjusted for the increased risk to college data security?
   1. Discuss the use of external IT auditors and their perceived effectiveness.
   2. How has an increase or decrease in funding impacted IT cybersecurity?
8. What training has been offered to faculty, staff, and students to counter cyberattacks?
   1. Walk me through the impact of this training?
   2. Discuss improvements that could be made for cybersecurity training.
9. How has the college adjusted the physical security of sensitive computing devices, such as data centers, server rooms, routers, cable connections, etc.?
   1. Discuss the administration's understanding of the importance of physical security.
   2. What policies have been implemented to counter a physical cyber-attack?
10. What changes or modifications have accommodated new laws and policies?
    1. How have these changes or modifications impacted the IT budget?
    2. Discuss the level of commitment from organizational administration to implement changes to the IT/organization to comply with new laws.

**Appendix B**

A picture containing text

Description automatically generated

**INFORMED CONSENT TO PARTICIPATE IN RESEARCH**

Investigator: Robert Chapa, 12345 Sesame ST. 727-277-4748

Title of Study: Why do some IT departments fail to take appropriate countermeasures for ransomware and other cyberattacks?

Purpose of Study: To identify areas of improvement by the administration/organization for increasing cybersecurity countermeasures.

Procedures: You will be asked to participate in a face-to-face interview that will be recorded and then transcribed.

Benefits: None.

Risks: None more significant than those of daily life.

Costs/incentives: None.

Confidentiality There will be no identifying information in the study. You will be referred to by a pseudonym throughout the interview. No mention of your place of employment. or your geographical location. All data will be kept on a personal laptop and in a Kaspersky vault with a strong password. There will be two layers of security. The systems CMOS password, the windows login password, and the vault password. All the passwords are different. All backups will be kept on the laptop's secondary hard drive. After the end of the DJC-720 class, all collected data will be destroyed.

Use of information: The information will be used only for the DCJ 720 class assignment.

Voluntary: The participants may withdraw from the study at any time or decline to participation participates without any penalty. The data is for the class DCJ 720. No data will be used outside of the class.

Signature: The investigator has discussed the project with me and answered all my questions. I understand that additional questions regarding the study, participant rights, or other concerns should be directed to Cheryl Chambers at cheri.chambers@saintleo.edu. I agree with the terms above and acknowledge that I have been given a copy of the consent form. I agree to participate in this research project by signing this consent form.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of the Participant Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Investigator Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Reader/Translator Date