RANKING SOCIAL ENGINEERING ATTACK VECTORS IN THE HEALTHCARE AND PUBLIC HEALTH SECTOR

by

Gaurav Sachdev

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer and Information Technology

West Lafayette, Indiana

May 2023

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. J. Eric Dietz, Co-Chair

School of Computer and Information Technology

Dr. Tatiana Ringenberg, Co-Chair

School of Computer and Information Technology

Dr. Julia Taylor Rayz

School of Computer and Information Technology

Dr. John A Springer

School of Computer and Information Technology

Approved by:

Dr. Eugene H. Spafford

ACKNOWLEDGMENTS

I am immensely grateful to my advisors, Dr. J. Eric Dietz and Dr. Tatiana Ringenberg, for their invaluable guidance, support and mentorship throughout my research journey. Their unwavering motivation, belief and constant support have been instrumental in making the experience enjoyable and fulfilling. I express my profound gratitude to my committee members, Dr. Julia Rayz and Dr. John Springer for their invaluable advice, expert guidance and support throughout my tenure at Purdue University. I extend my sincere thanks for their interest in my research and for their availability whenever I required their help. I am deeply grateful to my parents, sister, family members and friends for their tremendous support, encouragement and belief throughout my degree program and this research. Without their support and belief, I would not have been able to accomplish what I have today.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

HPH	Health and Public Health
NIST	National Institute of Standards and Technology

ABSTRACT

The National Institute of Standards and Technology defines social engineering as an attack vector that deceives an individual into divulging confidential information or performing unwanted actions [1]. Different methods of social engineering include phishing, pretexting, tailgating, baiting, vishing, SMSishing, and quid pro quo. These attacks can have devastating effects, especially in the healthcare sector, where there are budgetary and time constraints. To address these issues, this study aimed to use cybersecurity experts to identify the most important social engineering attacks to the healthcare sector and rank the underlying factors in terms of cost, success rate, and data breach. By creating a ranking that can be updated constantly, organizations can provide more effective training to users and reduce the overall risk of a successful attack. This study identified phishing attacks via email, voice and SMS to be the most important to defend against primarily due to the number of attacks. Baiting and quid pro quo consistently ranked as lower in priority and ranking.

1. INTRODUCTION

1.1 Historical Context

The most recognizable instance of social engineering is the ruse of the Trojan Horse employed by the Greeks in the Trojan War. The Greeks constructed a giant wooden horse and secretly housed several warriors within. The Greeks staged a fake departure and the Trojans took the wooden horse into their city. In the dead of night, the secret troops emerged from the horse and opened the city gates, allowing the Greek army, which had returned, to enter and secure victory in the war [2]. The National Institute of Standards and Technology (NIST) maintains guidelines and standards for several sectors.They hold significance because their standards and regulations are widely adopted across both government and industries. NIST defines social engineering as "the act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust" [1]. Over the last few years, social engineering attacks have grown. According to the 2021 Verizon Data Breach Report [3], 85% of breaches involved a human element in the breach. The growing trend is that training and awareness are used to combat social engineering attacks.

Social engineering attacks are evolving constantly, countermeasures are not able to keep up with the adaptability of these attacks [4]. After the COVID-19 pandemic began there were more social engineering attacks themed around it [5]. This is an example of how volatile the different attack vectors within social engineering can be. Even if the scope is narrowed to just email-based phishing it can vary from fake websites that are for booking non-existing vaccine appointments to fake bank password reset emails. At this time the most effective defense against Social Engineering attacks consists of a mixture of both technical measures as well as user training and awareness [6]. A mix of both is ideal but technical preventive measures may be futile if the user is tricked into circumventing it, which is why these training programmes are imperative to implement.

1.2 Project Goals

NIST defines social engineering as the the act of tricking a person into disclosing sensitive information, acquiring illegal access, or defrauding the person in order to win that person's confidence and trust [1]. While some elements of it require technical expertise to perform, the crux of these attacks is that they attack the users of the system rather than the system itself. A majority of countermeasures include awareness and training regimes for the end users in various situations [7] [8]. This remains true for health facilities' approaches to prevent Social Engineering [9]. Healthcare workers may not have enough time to devote to training practices.Organizational constraints implyăthe absence of variation in awareness campaigns that target particular staff groups with varying degrees of knowledge [4]. Similarly, for organizations with monetary limitations, there is a lack of effective training regimes that are both time and cost-efficient[10]. Social Engineering consists of a broad range of attacks.

The ranking of the social engineering attacks would aid the creation of time and monetarily efficient training programmes by focusing more on those deemed to be more devastating and less on those that are not as potent. The factors such as cost to the attacker, number of attacks, effectiveness of the attacks in terms of both monetary value and data, the successful number/percentage of attacks are being considered to rank these attacks. Not all factors contribute to the same extent and therefore, a weighted distribution of the factors is used. The sum of the weighted factors for each attack generates a value that is termed the r value. A higher r value implies that the attack is more potent. This provides a template-like structure for understanding the nuances of these attacks.

1.3 Contribution of the study

This study aims at aiding the creation of low-cost yet effective training and awareness programs for both end-users and employees of organizations. Training and awareness programmes do require targeted plans according to the situation. This study would help create a template that would make it easier to assess situations and build these training and awareness programmes to better fit the situation. This can help those who are creating the programs understand which attacks are more important to prevent in certain situations. This is especially applicable for trainees that do not have large amounts of time to devote to training and awareness programmes, thus not only being low cost and effective, they must also be time efficient. Modeling these programmes from scratch in every scenario will require a large workforce to both understand and implement it. Having the framework proposed would significantly reduce that task. Once it is understood what the environment is, the framework can generate a list of attacks in order of importance specific to the context. Thereafter, training methods can be fine-tuned to better fit the situation.

2. LITERATURE SURVEY

2.1 What is Social Engineering?

Peltier stated that the majority of social engineering attacks are carried out by outsiders who employ various psychological methods to persuade the user of the system to provide the information necessary for them to gain access to a computer or network [11]. Since 2006, this definition has evolved into an umbrella term that encompasses any attack that involves using a person's confidence and trust to conduct fraud, get unlawful access, or coerce them into disclosing critical information [1]. Now, it also considers insider threats within the organization, such as disgruntled employees.Social engineering is considered the most challenging form of attack to protect against as it cannot be prevented through technology but rather requires a robust information security architecture, including established policies and standards, and ongoing vulnerability evaluations. [11]. This is an important point that will be looked into further defending against social engineering attacks which is not simple and has no one size fits all defense.

According to the Verizon Data Breach Report [3], 85% of data breaches have a human factor involved. The most common pattern for breaches included Social Engineering methods. These statistics only involved incidents that were with data breaches and didn't include attacks on individuals that include scams and data disclosure. Social engineering is considered a superior threat compared to others because it is a simple, cost-effective, powerful, and frequently successful method for criminals to achieve their goals [12]. According to the 2020 Annual Report from the Internet Crime Complaint Center IC3 [13], Phishing, Vishing, Smishing, and Pharming had the most victims with 241,342 in number. A report published by a cybersecurity company Barracuda looked into spear phishing attacks between May 2020 and June 2021. They found an average organization is targeted by social engineering attacks over 700 times a year [14]. This report only monitored email-based attacks, they did not include voice-based, SMS-based or physical-based social engineering attacks.

2.2 Types of Social Engineering Attacks

Social engineering attacks cover a variety of different attack vectors. These can be subdivided into many categories but the criteria for subdivision also is important. According to Ivaturi and Janczewski, [15] there are two types of social engineering attacks that are Person-Person attacks and Person-Person via media attacks.The former refers to an attack where the attacker and victim have direct personal contact, while the latter refers to an attack where there is no physical interaction between the attacker and victim. It further divides the latter into text, voice, and video subcategories. Internet-based attacks like Phishing, Cross-Site Request Forgery, SMSishing and Malware fall under the text-based subdivision. While this is a good start to creating a taxonomy, it needs further distinguishing between the various types of attacks as they keep growing in number. Moreover, since this was written in 2011 there have been too many changes in social engineering to have just these categories which were addressed in further attempts at taxonomies [16] [7] [6].

Salahdine and Kaabouch [6], categorize social engineering attacks into technical, social, and physical attacks based on the method of execution. Social-based attacks use psychological manipulation of victims through relationships, while technical-based attacks are carried out through the internet or other technological means. Lastly, physical based attacks involve the attacker physically having to perform actions like checking dumpsters for valuable documents. This is important as social engineering can also be used to obtain access to a network and then use technical or socio-technical techniques after that to pivot for more access, as referenced in the Mitre ATT&CK framework which lists phishing techniques as a method to gain beginning access to a system [17]. This paper also brings up a distinction between the different types of phishing attacks, because of how prevalent phishing attacks have become the same concept has been applied to more aspects than just email based phishing attacks indicating how much it has evolved over the years. Phishing has evolved from a stand-alone attack vector to give rise to several attack vectors using the same concept in the medium of Smishing, Website, Wifi and so on [18]. This paper along with Krombholz [19] introduces the concept of hybrid social engineering attacks that combine across various categories of social engineering attacks.

Krombholz [19] also differentiated between types of social engineering attacks based on the method of attack delivery. This is an additional step further as the technical channel was broken down even further rather than encompassing all technical-based delivery systems under that heading. They divided it into email, instant messenger, telephone or voip, social network, cloud, website and physical forms of channels [19]. The paper from 2014 emphasized that the decrease in personal interaction and the abundance of communication tools have increased the opportunities for social engineering attacks.

Due to the changes in the workplace after COVID-19 this seems more relevant than ever. There is a growing group of organizations that are considering working from home which would entail more opportunities for attackers to acquire credentials that would be available easiest by social engineering attacks directed toward employees. Aldawood and Skinner [20] also add another medium to the channel subdivision by adding mobile-based social engineering attacks to the list. This is significant as there are instances of malware disguised as applications available on verified app distributors like the Google Play Store [21]. Smartphones have led to an increase of opportunities for attacker to carry out social engineering attacks.

2.3 Impact of Social Engineering Attacks

As mentioned earlier, human hacking seems to be the preferred method for threat actors due to its effectiveness and cost. This section will look into the impact that Social Engineering attacks have on organizations and individuals by taking a look at successful attacks that have taken place.

2.3.1 Twitter Security Incident 2020

In July 2020, Twitter employees were victims of a Social Engineering attack [22]. Employees were victims of a spear phishing attack that allowed attackers to gain access to internal support tools. They then proceeded to identify other employees who possessed access to account support tools. This allowed them to tweet from 45 accounts, access the direct messaging inbox of 36 accounts and download the data from 7 accounts.

The attackers tweeted out from popular accounts like Elon Musk, Bill Gates and Kanye West offering double the value back of bitcoin sent to a particular address. It was estimated that the account received more than $118,000 [23].

This particular incident involved Social Engineering methods on two levels, targeted vishing to employees to gain access to internal tools and then widespread phishing to get money. The aftermath of the attack involved temporarily shutting down the ability of verified accounts to tweet. There was also a forensic investigation that Twitter conducted. There were economic costs associated with the investigation, the direct monetary damage to users as well as reputational damage to Twitter and the accounts to which the attackers gained access.

2.3.2 Twilio Security Incident 2022

Twilio is an American company that is primarily used by businesses to communicate with their clients using voice, text, chat, video and email. These are integrated into businesses using API's. In August 2022, they suffered a Social Engineering attack [24]. The attacker used SMSishing. The attackers targeted current and former employees of Twilio through text messages, falsely informing them that their passwords were no longer valid, their schedules had altered, and directing them to log in to a URL that was under the attacker's control. They were then able to steal the credentials of employees that fell for it. Using these credentials they gained access to their internal systems gaining access to customer data.

A majority of Twilios customers are other businesses which means that other businesses had their data and privacy affected for no fault of their own. While there are supplemental costs of forensic investigations, fines and so on, the primary affected component was data leakage and privacy.

2.3.3 Covid-19 Social Engineering Attacks

Since the outbreak of the Covid-19 pandemic, there has been an increase in social engineering attacks. There has been an increase in remote work, online education, and online entertainment, the overall broadband usage has increased and so has the number of users on the internet [5]. These are all contributing factors to the increase in Social Engineering attacks. A report by Google [25], found that the primary mode for Social Engineering attacks was Phishing attacks via emails and websites.

Hijji and Alam conducted a multivocal literature survey of social engineering attacks during the intial years of the Covid-19 pandemic [26]. The study discovered that Ransomware was the most frequently utilized malicious software in combination with Social Engineering attacks. The investigation also uncovered that healthcare organizations and hospitals were the primary targets of these attacks, primarily due to their inadequate security measures. A report by Accenture indicates that companies spent over $110 billion worldwide in 2021 on cyber protection [27]. One well-known example of a successful Social Engineering and Ransomware attack is the case of the University of California San Francisco School of Medicine, which was hit by hackers and had to pay a ransom of $1.14 million to regain control of their systems [28].

Researchers at Proofpoint [29] identified Iran-aligned APT actor TA451 (APT33) using COVID-19 themed phishing attacks against United States defense contractors. They pretended to be the World Health Organization to get their malicious downloads which could act as a reverse shell which gave remote access to those machines. Nation-state attackers with a lot of technical skills using these techniques point to the potency of social engineering attacks.

Unprecedented global events that take place like the Covid-19 pandemic allow malicious entities more opportunities to conduct social engineering attacks. There was an increase in scams that extracted medicare information from people [30] under the pretense of vaccinations. In instances like these, one of the most important thing is keeping an updated awareness in being able to identify legitimate opportunities and fraud attempts, a difficult task to uphold in targeted individuals and organizations.

2.4 Cybersecurity in Healthcare and Public Health

The Cybersecurity & Infrastructure Security Agency (CISA) has categorized healthcare and public health as a critical infrastructure sector, with assets that are deemed so crucial that their "disruption or destruction would have a devastating impact on our physical, economic security, public health, or safety" [31]. A study on the Influence of Human Factors on Cyber Security within Healthcare Organizations by Nifakos et al. [32] found that cyber-attacks in the healthcare sector result not only in data loss and financial theft, but also pose a threat to medical devices and infrastructure, which in turn is endangering human lives [33]. Additionally, healthcare data is considered to be significantly more valuable than other types of data [34].

Coventry and Branley [34] identified that an increase in connected technology and the introduction of mobile consumer devices in the ecosystem allows for more surface area where attackers can find and exploit vulnerabilities. While there has been a move to introduce more technology in this sector there is also an issue with legacy technologies being used which are prone to more hackers and malware, for example, the Wannacry Ransomware [35].

The Healthcare and Public Health sector has seen a surge in cyber attacks, which can be classified into three main categories: IT infrastructure exploitation, ransomware, and exploiting human vulnerabilities [32]. Research by Hijji and Alam [26] found that healthcare companies and hospitals were particularly vulnerable during the Covid-19 pandemic, with their weak security systems making them attractive targets. The resulting damage has been significant given the high frequency of attacks and the potential rewards for the attackers.

2.5 Social Engineering Prevention Strategies

Social Engineering attacks cannot be mitigated or reduced through technical solutions the same way it is relatively straightforward to do so for hardware or software vulnerabilities [36]. Organizations can use a combination of different defenses to prevent social engineering attacks. An effective strategy to combat the threat of social engineering is the implementation of multi-layer defense, also known as defense in depth. This approach was coined by Conteh and Schmick [37] and involves a combination of security policy, employee training, network guidance, audits and compliance, technical procedures, and physical guidance. All these measures are essential in countering the threat, however, training employees on the dangers of phishing and other social engineering attacks is especially crucial. Despite the importance of employee training, a study found that only seven percent of organizations in the United States invest in providing phishing education to their employees [37].

Parthy and Rajendran looked into the preventing social engineering attacks in an enterprise which requires identifying the potential threats and taking measures to prevent them. [7]. They mapped out categories of victims as employees, infrastructure and policy and technical components. They then sub-divided each victim category into the type of attack that they could face. Each of these attacks had a countermeasure that could be implemented to reduce the effectiveness of the attacks. Looking at the countermeasures stated reinforces the idea that there must be a multi-layer defense involved that cannot only involve one type of defense mechanism. There were some technical countermeasures like blockers for SMSishing but many of the countermeasures included either awareness, education or training. Employee monitoring can prove challenging compared to monitoring security systems, as they are more prone to falling victim to social engineering attacks [16]. This is important to note as technical countermeasures will fail if users can be deceived into performing actions for attackers.

Bowen et al [38] looked into the susceptibility of humans within large corporations and government agencies to social engineering attacks. The participants of this study were repeatedly tested against four types of phishing emails modeled after real phishing emails. The participants were educated each time to improve their ability to detect these emails. They were repeatedly tested until the participants stopped falling prey to these attacks. The authors found that users could be trained or coached to stop falling for these attacks implying that training could be an effective countermeasure.

A study conducted in a town in Netherlands examined how likely a victim was to be vulnerable to a social engineering attack had they been exposed to either a priming or a warning [39]. The participants were prepared for the study by being given questions related to social engineering, including whether they were familiar with the term "phishing" and whether they were conscious of the personal information they share on the internet. Warnings involved handing leaflets to the subjects that had warnings including not to share personal data with other people. The results of this study found that neither the warnings nor the priming were an effective countermeasure to social engineering attacks. These results suggest that an awareness campaign will not be as effective as dedicated training to defend against social engineering attacks.

Further, continued training is crucial in countering social engineering attacks. A research report from 2014 [40] indicates that most employees tend to forget a significant portion of the information acquired in a business training session. Within an hour, half of the information is forgotten, by the end of a day, 70% is forgotten, and by the end of a week, 90% of the information is lost. Given the intensive and costly nature of preparing for and delivering training, it is imperative for companies to remain vigilant in the fight against social engineering attacks and to maintain updated defenses [41]. A good example of this is Coronavirus social engineering attacks that emerged once the pandemic started in 2019 [42]. The Coronavirus pandemic gave attackers more opportunities as more people were working from home, and there was a lot of unemployment that was leveraged with fake job opportunities. Later, the vaccine availability and the desperation for it caused a lot of people to fall for these kinds of attacks.

2.6 Problems in Social Engineering Training and Awareness Programs

An article by Aldawood looked into the pitfalls and ongoing issues in training and awareness programs[4]. One of the main challenges as stated was that of trying to keep a step ahead of the attackers. The factors that affect the road to providing adequate training were listed as follows. Business Environmental which was that the employee of an organization often works in different locations within the organization premises and outside the area as well. This means that the employee could be targeted on personal emails and areas outside the domain of the organization where they work. Social factors include the fact that often communication with clients may involve informal communication and that may lead to a breakdown in defense mechanisms for social engineering attacks. There is an organizational as well as a governmental factor to it as well. There are economical considerations to look into as well when dealing with social engineering training. It needs to be cost-effective otherwise organizations do not invest in security and social engineering is often neglected even more. The personality of a victim also plays a role in who are susceptible to social engineering attacks [43]. Each person has different traits that attackers can use to tailor methods toward successfully executing social engineering attacks. Some attackers use a strategy to map defense mechanisms against the psychological principles that would cause a user to be a victim of social engineering [41]. Since the entire concept of social engineering revolves around deceiving the user, it differs from person to person. The personality and past experiences of a user may cause the effectiveness of the same social engineering attack to vary from person to person[43].

When we consider modern training programs there are several solutions to increase the effectiveness of the training. However, effective training requires a higher amount of coordination among the teams of trainees. The variability of individual personalities and their adoption of learning materials can pose a challenge in team-based training. Interactive games and virtual labs offer solutions, however, they also come with the challenge of coordination, as the order of identification and mitigation must be maintained. Traditional Social Engineering Training and Awareness Programs utilize various methods such as onsite training, posters, manual reminders, and online courses, but they often face the challenge of limited training budgets.

The University of Phoenix conducted a study to find ways to tackle deception in social engineering attacks [44]. The study involved 20 Information System Security Association experts who participated in a Delphi study to gather and distill expert opinions. The study sought to identify common concerns among the experts and discovered three major issues: data breach, ineffective strategies, and a lack of ongoing education. These issues pointed towards three main areas for improving practices in preventing social engineering attacks. The results emphasized the importance of education, security policies, procedures, and continuous training. Additionally, the authors asked the experts to prioritize the top ten issues based on their significance. The results showed that not all attacks have the same level of importance [44]. Thus, it is important to focus on specific types of attacks when creating a training program.

2.7 Most important Social Engineering Attacks

Not all the social engineering attacks should be given the same importance when developing a training program. This is relevant when monetary and time constraints would not allow extremely extensive or frequent training regimes. For example, there has been a recent surge in ransomware attacks in hospitals. In these attacks, there is some form of social engineering that is used to carry out these attacks [45]. In situations like these where it will not be able to create a training regime that is extensive due to time constraints, the training regimes need to dynamically adjust to emphasize certain social engineering vectors. Disrupting the normal functioning of a hospital will have far more repercussions than monetary damage.

In the study by Campbell [44], the rankings were made by taking into consideration the opinion of experts. These attack vectors can be ranked based on monetary damage, data leaked and number of attacks. This would give a holistic view of which attack vectors under the umbrella of social engineering would be imperative to defend against when developing a training regime for organizations. It is important to note that there will be distinctions between various sectors such as the banking sector that would have a difference to which social engineering attacks are most prevalent as here the monetary damage would be more impactful than a disruption in daily functioning as in the study of social engineering Attacks and Countermeasures in the New Zealand Banking System [46].

3. Methodology

3.1 Identification of Social Engineering Attack Vectors

There are several taxonomies of Social Engineering attacks available [12] [15] [19] [20] [7]. Using these available taxonomies, the attacks that were the most prevalent and claimed to be the most damaging were chosen. These were identified to be Phishing, Pretexting, Baiting and Quid Pro Quo. Due to the emphasis placed on Phishing in the Healthcare and Public Health Sector, Phishing was divided into Email-Phishing, SMS-Phishing and Voice/VOIP Phishing[47]–[49].

3.2 Study Design

Due to the lack of detailed data and the constant evolving nature of Social Engineering attacks, a Delphi study was chosen. Delphi studies are used to obtain consensus on a particular issue or topic using the knowledge and experience of experts in a particular field [50]. The methodology described subsequently received approval from the Institutional Review Board (IRB-2022-1361). The IRB approved the survey questions, method of data collection and assistance from a member of the state.

3.2.1 Participants

Experts were individuals with 5 years or more of experience in either the Healthcare and Public Health sector or the Information Security/Cybersecurity sector. By having input from both healthcare professionals and cybersecurity professionals, we are able to consider the users in the system and gain a holistic perspective. A member from the state of Indiana was used to identify individuals who fit the criteria. A survey was sent out to the individuals that fit the criteria. There were 17 participants that consented to the survey but eight participants that fit the criteria and completed the survey.

3.2.2 Procedure

The goal of the survey was to identify relevant factors that affect the impact caused by social engineering attacks and weigh them. This would create an r-value, the higher the r-value, the more the Social Engineering attack vector is destructive. There will be several factors that go into what makes an attack formidable. A review of the literature on social engineering attacks provided these factors. These were identified to be financial loss caused [26], sensitive data exposure/privacy loss caused [4], number of attacks [49] and success percentage of attacks [49]. All of these factors either were listed as reasons for social engineering being used by attackers. The defense mechanisms for these attacks have been identified to be Training and Awareness Programs [10], Compliance based standards and regulatory bodies [33] and technical countermeasures [45].

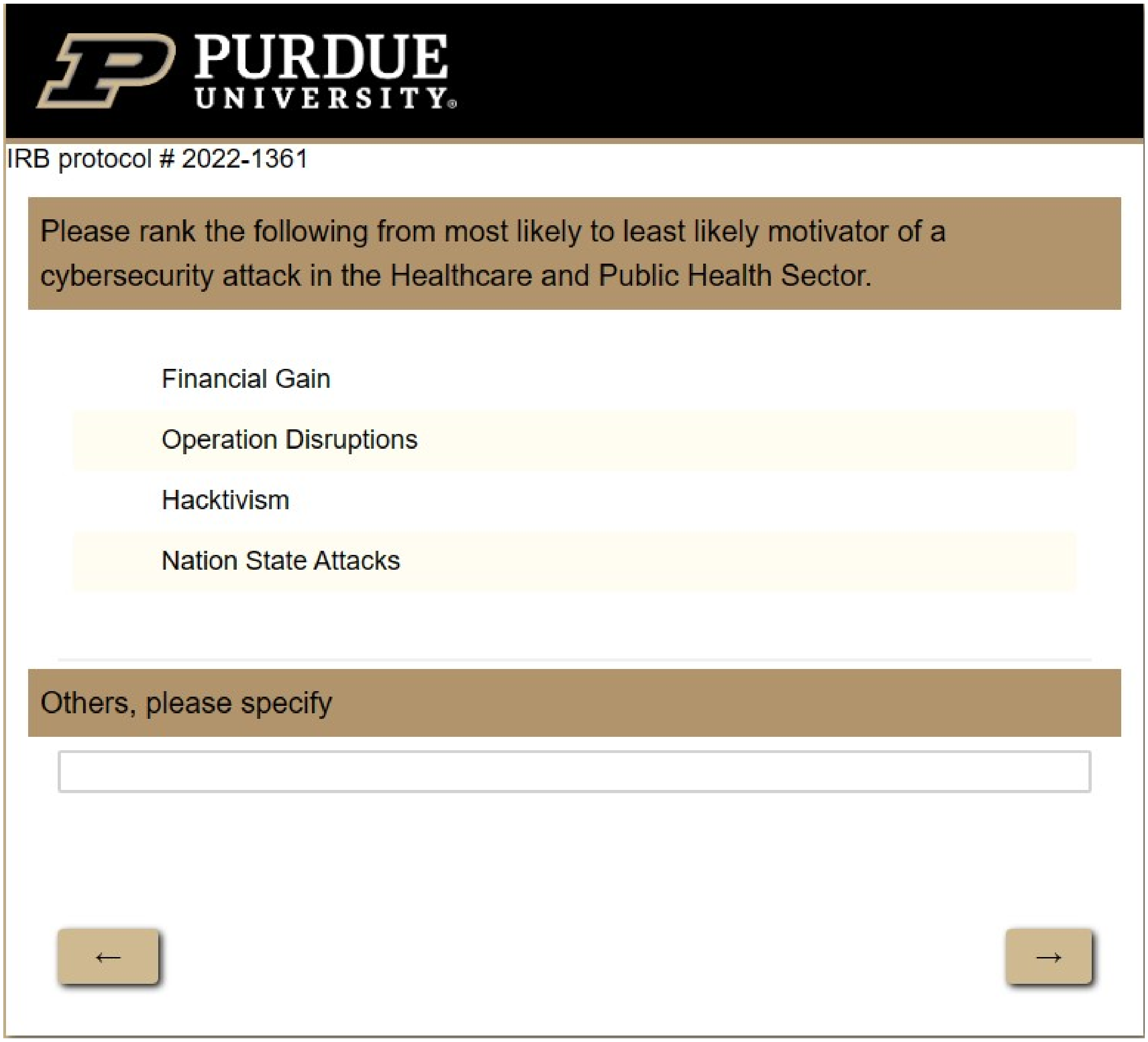
The participants of the survey were asked to rank the factors. They were assigned values from 4 to 1. The higher the importance, the higher the value. The average values of each factor was the assigned weight for that particular factor. The participants were asked to rank the Social Engineering attack vectors in order of most to least impactful according to each of the factors stated above. The highest was assigned a score of 5 and the lowest a score of 1, the average scores from all the respondents were taken. The factors were also ranked, the average scores were the assigned weightage. The r-factor will be calculated as follows:

$$r = \sum (weight\ of\ factor\ ) * \ (average\ score\ of\ attack\ vector\ of\ that\ factor)$$

The participants were asked to rank the social engineering attacks. This would provide a reliability check to see whether the r-value results vary significantly from the participants opinions.

3.2.3 Survey

The survey is 22 questions long, including the informed consent question and demographics questions. The questions were formulated to gain a better understanding of the circumstances that make a social engineering attack more successful. Additional questions were asked to understand the damage caused by these attacks, the forensic investigation that can take place and ultimately to create a ranking for these attacks. Lerums[51] looked into assessing the state of Indiana's cybersecurity practices. Thomas [52] took it further to develop training programs based on the scorecard that Lerums had created. These papers provided insight to focus the same concepts to social engineering, and make it more fine-tuned. Questions were asked concisely with clarity to prevent confusion. An example is given below. A complete list of the survey questions can be found in Appendix A.



IRB protocol # 2022-1361

Please rank the following from most likely to least likely motivator of a cybersecurity attack in the Healthcare and Public Health Sector.

Financial Gain

Operation Disruptions

Hacktivism

Nation State Attacks

Others, please specify

Figure 3.1. Sample Question

The survey begins with a consent form, informing participants of the details of the survey, what information is being collected, IRB information and asking whether they consent to be a part of the study.

The next section consists of demographic questions, the participants are asked whether they have experience and how many years in the Healthcare and Public Health or the Cybersecurity/Information Security industry. Participants that had over 5 years of experience in either industry were qualified to be participants of the survey. The rest were shown the End Survey page.

The qualified participants were asked how prepared they believe the Healthcare and Public Health sector is to deal with Cybersecurity related threats. They were asked to rank the factors financial loss caused ,sensitive data exposure/privacy loss caused ,number of attacks and success percentage of attacks. They were then asked to rank the social engineering attacks, Email Phishing, Vishing and Smishing, Baiting, Pre-texting and Quid Pro Quo according to each factor. They were asked to rank the financial, privacy and operational impact to organizations, employees and patients. At the end of the survey the participants were asked if they had any feedback or any attacks that were not included that were important to consider.

The survey tool used was qualtrics. The survey was distrubuted electronically. Any questions that had similar or the same options had randomized order of options.

4. Results

In this chapter, the results of the survey will be presented. This chapter will be divided into sections based on the results being presented.

4.1 Demographic Questions

There were 17 respondents but eight people that fit the criteria for the study. Three participants had five or more years of experience in the Healthcare and Public Health Sector. The remaining five participants had five or more years of experience in the Cybersecurity or Information Security sector. Four of the participants had over ten years of experience in their roles. The other four had between five and ten years of experience. The results were collected through the participation and input of individuals within the Healthcare and Public Health sector, ensuring their accuracy and representation of the user perspectives.

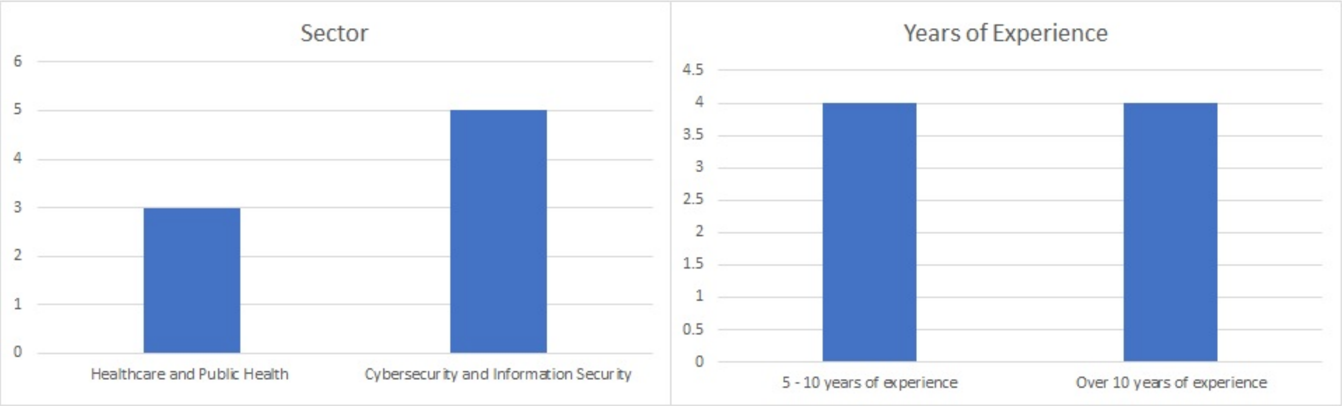


Figure 4.1. Demographic Information

4.2 Ancillary Questions

Participants were asked how prepared they believe the Healthcare and Public Health Sector is for cybersecurity related threats. Four participants believed that the HPH sector was somewhat prepared for cybersecurity related threats. Two participants believed that the HPH sector was unprepared and two believed that the HPH sector was slightly prepared.

The participants were asked to rank the motivators for a cybersecurity attack in the HPH sector. The options for these questions were Financial Gain, Operations Disruptions, Hacktivism and Nation State Attacks. The table below lists the frequency of positions in the ranking that each individual motivator was found.

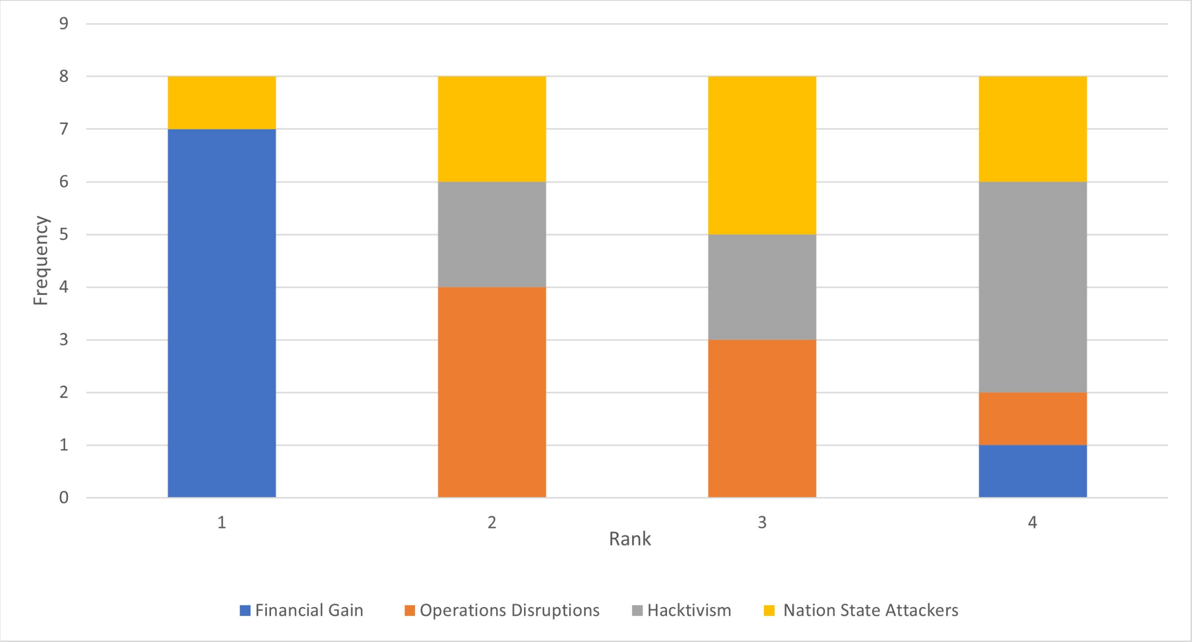


Figure 4.2. Frequency of Ranks for Motivators of an Attack

Rank	Financial Gain	Operations Disruptions	Hacktivism	Nation State Attackers
1	7	0	0	1
2	0	4	2	2
3	0	3	2	3
4	1	1	4	2

Table 4.1. Frequency of the ranking for motivators of attacks

Participants were asked to rank what they believed were the most effective countermeasures to social engineering attacks. The most important countermeasures to these attacks were training and awareness programmes followed by technical countermeasures. The least important countermeasure was compliance and standards.

Rank	Training and Awareness	Technical Countermeasures	Standards and Regulatory Bodies
1	5	2	1
2	2	5	1
3	1	1	6

Table 4.2. Frequency of the ranking for Countermeasures of Social Engineering Attacks

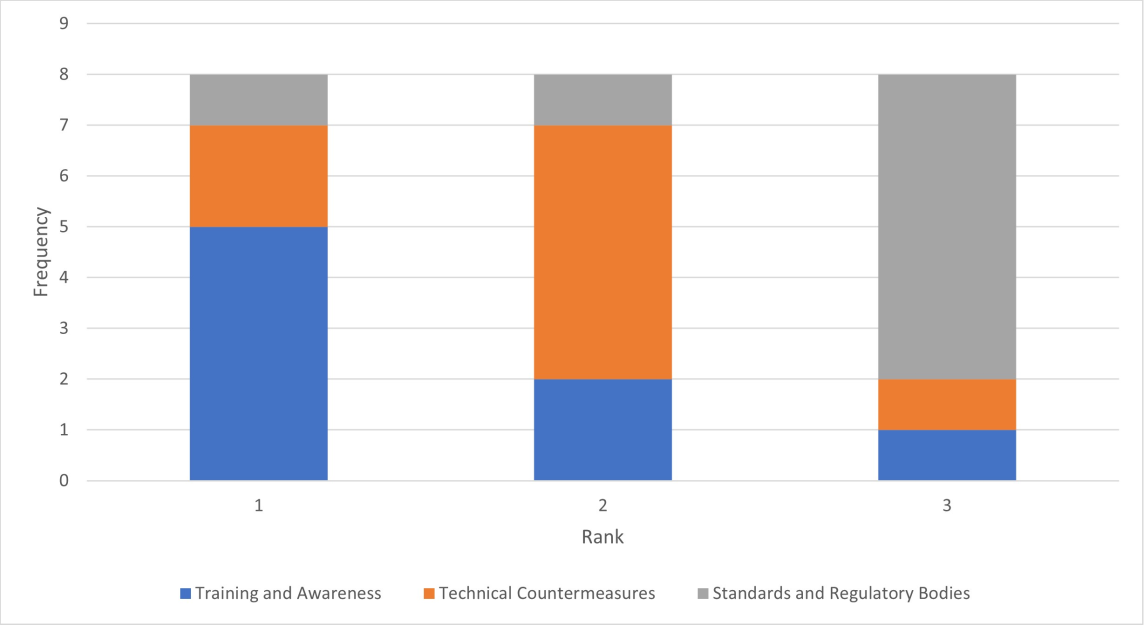


Figure 4.3. Frequency of the ranking for Countermeasures of Social Engineering Attacks

4.3 Impact of Social Engineering Attacks

In the study, participants were asked to evaluate and rank the impacts that the Healthcare and Public Health (HPH) sector has on different groups. The groups included organizations that operate within the HPH sector, employees who work in the HPH sector, and patients who use the services provided by the HPH sector. The participants were asked to consider the effects of social engineering attacks on each of these groups and rank them accordingly. This information was used to understand the overall impact of the HPH sector on different stakeholders and to identify areas for improvement. For organizations, Table 4.3 ,the results show that Financial Losses is the option that was almost evenly split evenly across the ranks, appearing two to three times across all ranks. Operations Disruptions and Brand Damage have similar frequencies, with Operations Disruptions ranking higher more frequently. Data Loss and Exposure also has some split opinions across the rankings.

Rank	**Operations Disruptions**	**Data Loss & Exposure**	**Brand Damage**	**Financial Losses**
1	3	1	1	3
2	0	3	3	2
3	4	2	0	2
4	1	2	4	1

Table 4.3. Frequency of the ranking for impact on Organizations

For patients, Table 4.4, data loss and exposure appear considerably higher frequencies at the first rank. There is a divided view regarding the ranking of financial losses and scheduling disruptions, with some placing them at the second rank and others at the third without tilting explicitly in any direction.

Rank	**Data Loss & Exposure**	**Financial Losses**	**Scheduling disruptions**
1	5	1	2
2	1	3	4
3	2	4	2

Table 4.4. Frequency of the ranking for impact on Patients

For Employees, Table 4.5, there was a lot more clarity for the ranking. The most important impact was scheduling disruptions. This was followed by data loss and exposure. The least important was judged to be financial losses.

Rank	Data Loss & Exposure	Financial Losses	Scheduling disruptions
1	2	0	6
2	3	4	1
3	3	4	1

Table 4.5. Frequency of the ranking for impact on Employees

4.4 Ranking Social Engineering Vectors

The factors that were most important in judging the potency of social engineering attacks were ranked. Those with higher scores were more important. Data loss and exposure was convincingly ranked towards the top from the respondents. The least important was the number of attacks as it ranked fourth or third throughout the responses with only one response ranking it first. Financial losses and success percentage were equally spread out throughout the ranks, however the financial losses had more ranking towards the bottom when compared to success percentage of the attacks. This is represented by the scores as follows, 3.5 for data exposure and privacy loss, 2.75 for success percentage of attacks, 2 for financial loss and 1.75 for number of attacks..The formula for calculating the r-value of the attack is demonstrated in 4.1,

$$\begin{aligned}
r = {} & 1.75\,(average \quad score \quad of \quad number \quad of \quad attacks) \\
& + 2\,(average \quad score \quad of \quad financial \quad loss) \\
& + 2.75\,(average \quad score \quad of \quad success \quad percentage \quad of \quad attacks) \\
& + 3.5\,(average \quad score \quad of \quad privacy \quad or \quad data \quad loss)
\end{aligned} \tag{4.1}$$

Rank	Financial Losses	Data Loss & Exposure	Number of Attacks	Success Percentage of Attacks
1	0	5	1	2
2	3	2	0	3
3	2	1	3	2
4	3	0	4	1

Table 4.6. Frequency of the ranking for factors that make attacks potent

Using this formula, the scores of the five attacks were as follows:

Factor	Email Phishing	Vishing & Smishing	Pretexting	Baiting	Quid Pro Quo
Data Loss & Exposure	0.4375	0.3375	0.275	0.25	0.2
Success % of Attacks	0.3875	0.3625	0.3625	0.25	0.1375
Financial Losses	0.4875	0.35	0.2625	0.2	0.2
Number of Attacks	0.475	0.375	0.2375	0.2625	0.15
r value	4.403125	3.534375	2.9	2.421875	1.740625
r, ranking independently	4.375	3	3	2.125	2.5

Table 4.7. Ranking social engineering attack vectors

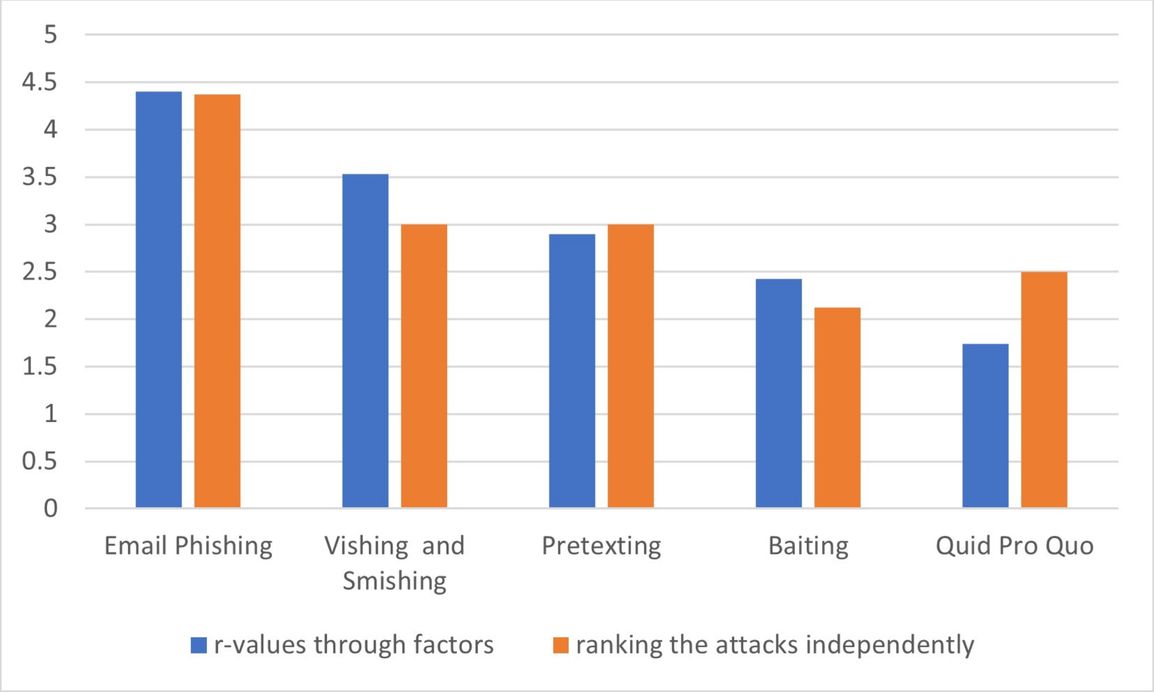


Figure 4.4. r-value scores and average scores of ranking the attacks

5. Discussion

5.1 Interpretation of Results

There were 17 respondents that worked in the desired industries but only eight had enough experience to qualify as experienced. While more data points would enhance the accuracy of the research there is the possibility of less experienced individuals skewing the results. The survey had representation from the HPH sector, as three of the respondents were from that industry, ensuring that the perspectives and insights of those who work within it were included and not just from the cybersecurity industry. Since there were definitions provided at the beginning of the survey and also short notes wherever needed as reminders it was clear that individuals not familiar with these terms still had holistic information about the topic.

Given the numerous successful cybersecurity attacks on the HPH sector [26] [32] [33] [34] [35], it is not surprising that no participants believed that the sector was sufficiently prepared to deal with such threats. It was almost unanimous that financial gain was the important motivator with only one response not at the first rank. Due to the valuable nature of healthcare records and data [34], it was predictable that financial gain was the biggest motivator for attacks against the HPH sector. Four respondents believed that operations disruptions was the second most important motivator, three believed it was the third ranked and only one last ranked. Within the United States, the HPH sector is classified as critical infrastructure [31], which explains why operations disruptions and nation-state attackers are closely the second and third motivations for attacks. Given that only two responses had nation state attackers at the second position while three had it at the third position and two at the last position it can be inferred that operations disruptions deserves to be ranked higher. There was one response that put nation state attackers as the most important motivator, however the overall majority seemed to favor the lower half of the rankings. Lastly, there were five respondents that placed hacktivism as the least important and not a single as the most important, it can be concluded that it was least important.

The results of the survey on the ranking of countermeasures to social engineering attacks have shown that training and awareness programs are deemed the most important. Technical countermeasures ranked second, while compliance-based standards and regulatory bodies were ranked last. Although there were some differing opinions among the respondents, the majority ranked similarly. The results indicate that while organizations may fulfill the requirements set by governing bodies, they may not place significant emphasis on preventing or reducing the number of attacks.

The results of the survey on the impact of cybersecurity-related attacks on organizations, employees, and patients revealed marked differences in the rankings. For employees, scheduling and operational disruptions were deemed the most significant impact, followed by data loss and exposure, with financial losses ranked last. This highlights the priority of the employees in the healthcare sector to prioritize the well-being of others and preserve human life. Patients, on the other hand, ranked data loss and exposure as the most important impact, followed by scheduling disruptions and financial losses. This emphasizes the value that medical and health records as data posses. The rankings for organizations, however, were less clear-cut. Both operations disruptions and financial losses were ranked first three times, with financial losses appearing slightly higher as it was ranked second more often. Brand damage was considered the least important by four respondents, while data loss and exposure was evenly distributed. These results suggest that for organizations, the order of impact may be financial losses, operations disruptions, data loss and exposure, and finally brand damage, though further research with a larger data collection is needed to confirm these findings.

As seen in several studies and papers [36] [7] [37] [16], the most important defense was awareness and training programmes followed by technical countermeasures. The least important was compliance based standards and regulatory bodies. Organizations may do the bare minimum to meet requirements for these standards or regulatory bodies but it doesn't imply there are effectively protecting against these attacks.

Since the participants of the survey were asked independently to rank the attack vectors there was a baseline to compare the weight of factors. Phishing and its subdivisions of Email, Vishing and SMSishing unanimously were the most potent attacks to defend against. The results of the ranking of the different types of social engineering attacks showed that phishing attacks are seen as the most dangerous due to their high frequency and the potential for financial loss and sensitive data exposure. However, the success rate of phishing attacks was rated lower, indicating that their prevalence may be the main contributor to their perceived threat. In contrast, the pretexting and baiting attacks were rated higher in terms of their success rate, indicating that these more sophisticated attacks pose a significant threat despite their lower frequency. The quid pro quo attack ranked the lowest, suggesting that it is neither a common nor a particularly sophisticated type of attack. These results highlight the importance of focusing on preventing phishing attacks and addressing the threat posed by more sophisticated social engineering tactics such as pretexting and baiting. Future research could also aim to expand the categories of social engineering attacks to better understand the evolving threat landscape in this field.

5.2 Limitations of the study

The limitations of this study are primarily related to the limited number of data points available. In order to produce more accurate results, a more extensive data collection phase with a target of at least 1000 data points would be ideal. This would allow for the use of non-parametric bootstrapping techniques to gain a deeper understanding of the population data. Although the best results would come from actual cybersecurity incident data, it may not be feasible to collect this information due to its sensitive nature. In this study, the data was collected through the use of a Likert scale and the r-values were calculated based on the average scores. It is important to note that the study only took into account the experiences of individuals within the state of Indiana and may not be representative of the entire population. To improve the results, the study could expand its data collection to include a wider geographic region and separate the results based on region. Additionally, the potency of social engineering attacks was judged based on four factors, and including more factors could lead to more precise results.

6. Conclusion

The goal of this study was to create a framework to help training and awareness programs become more efficient. Having a framework that lets organizations evaluate their security posture with respect to social engineering attacks eliminates the need to hire external consultants or security teams to help reduce the monetary costs for small to mid-size organizations. Social Engineering has been labeled as one of the most important cybersecurity threats to protect against, thus adequate emphasis must be placed on it. The Health and Public Health sector is a highly targeted area due to its status as critical infrastructure and the value of data and records. The highest priority to protect against was found to be phishing, email-based, Vishing and SMSishing. The high volume of attacks contribute most to the potency of phishing attacks. The most effective countermeasure to social engineering attacks is a mixture of both user training and technological measures. However, effective training and awareness programmes could prove to be the most important defence to these attacks if administered with the proper attention.

REFERENCES

[1] C. C. Editor. "Social engineering - glossary CSRC." (2023), [Online]. Available: https://csrc.nist.gov/glossary/term/social_engineering.

[2] H. DeVries. "How to get consulting clients using a trojan horse marketing strategy," Forbes. Section: Leadership Strategy. (), [Online]. Available: https://www.forbes.com/sites/henrydevries/2019/04/12/how-to-get-consulting-clients-using-a-trojan-horse-marketing-strategy/.

[3] "2021 DBIR master's guide," Verizon Business. (2021), [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/.

[4] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programspitfalls and ongoing issues," *Future Internet*, vol. 11, no. 3, p. 73, 2019, Num Pages: 73 Place: Basel, Switzerland Publisher: MDPI AG. DOI: http://dx.doi.org/10.3390/fi11030073. [Online]. Available: https://www.proquest.com/docview/2429965624/abstract/12B7D8CCAA97480BPQ/1.

[5] S. Venkatesha, K. R. Reddy, and B. R. Chandavarkar, "Social engineering attacks during the COVID-19 pandemic," *SN Computer Science*, vol. 2, no. 2, p. 78, Feb. 6, 2021, ISSN: 2661-8907. DOI: 10.1007/s42979-020-00443-1. [Online]. Available: https://doi.org/10.1007/s42979-020-00443-1.

[6] K. Salahdine Fatima and Naima, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, 2019, Num Pages: 89 Place: Basel, Switzerland Publisher: MDPI AG. DOI: http://dx.doi.org/10.3390/fi11040089. [Online]. Available: https://www.proquest.com/docview/2430007328/abstract/813A9612D55043B9PQ/1.

[7] P. P. Parthy and G. Rajendran, "Identification and prevention of social engineering attacks on an enterprise," in *2019 International Carnahan Conference on Security Technology (ICCST)*, ISSN: 2153-0742, Oct. 2019, pp. 1–5. DOI: 10.1109/CCST.2019.8888441.

[8] A. Smith, M. Papadaki, and S. M. Furnell, "Improving awareness of social engineering attacks," in *Information Assurance and Security Education and Training*, R. C. Dodge and L. Futcher, Eds., vol. 406, Series Title: IFIP Advances in Information and Communication Technology, Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 249–256. DOI: 10.1007/978-3-642-39377-8_29. [Online]. Available: http://link.springer.com/10.1007/978-3-642-39377-8_29.

[9] S. T. Argaw, J. R. Troncoso-Pastoriza, D. Lacey, *et al.*, "Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks," *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, p. 146, Jul. 3, 2020, ISSN: 1472-6947. DOI: 10.1186/s12911-020-01161-7. [Online]. Available: https://doi.org/10.1186/s12911-020-01161-7.

[10] H. Aldawood and G. Skinner, "Challenges of implementing training and awareness programs targeting cyber security social engineering," in *2019 Cybersecurity and Cyberforensics Conference (CCC)*, May 2019, pp. 111–117. DOI: 10.1109/CCC.2019.00004.

[11] T. R. Peltier, "Social engineering: Concepts and solutions," *Information Systems Security*, vol. 15, no. 5, pp. 13–21, Nov. 1, 2006, Publisher: Taylor & Francis _eprint: https://doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95427.3, ISSN: 1065-898X. DOI: 10.1201/1086.1065898X/46353.15.4.20060901/95427.3. [Online]. Available: https://doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95427.3.

[12] M. R. Arabia-Obedoza, G. Rodriguez, A. Johnston, F. Salahdine, and N. Kaabouch, "Social engineering attacks a reconnaissance synthesis analysis," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, Oct. 2020, pp. 0843–0848. DOI: 10.1109/UEMCON51285.2020.9298100.

[13] "Internet crime complaint center(IC3) annual reports." (2023), [Online]. Available: https://www.ic3.gov/Home/AnnualReports.

[14] "Report: Best practices to defend against evolving spear-phishing attacks," Journey Notes. (Dec. 16, 2020), [Online]. Available: https://blog.barracuda.com/articles/2020/12/17/report-evolving-spear-phishing-attacks/.

[15] K. Ivaturi and L. Janczewski, "A taxonomy for social engineering attacks," p. 12, Jun. 2011. [Online]. Available: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=confirm2011.

[16] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Computing Surveys*, vol. 48, Feb. 1, 2016. DOI: 10.1145/2835375.

[17] "MITRE ATT&CK." (2023), [Online]. Available: https://attack.mitre.org/.

[18] “A survey of phishing attacks: Their types, vectors and technical approaches elsevier enhanced reader.” (2021), [Online]. Available: https://reader.elsevier.com/reader/sd/pii/S0957417418302070?token=D9DABF0E3A0217229114153C09F4185B7C6796E9826512F05D9F2BCCECC41D5C86EF9717805390454DD8A3E01DCB9DD2&originRegion=us-east-1&originCreation=20211018004259.

[19] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” *Journal of Information Security and Applications*, vol. 22, Oct. 24, 2014. DOI: 10.1016/j.jisa.2014.09.005.

[20] H. Aldawood and G. Skinner, “An advanced taxonomy for social engineering attacks,” *International Journal of Computer Applications*, vol. 177, pp. 975–8887, Jan. 16, 2020. DOI: 10.5120/ijca2020919744.

[21] P. Kotzias, J. Caballero, and L. Bilge, “How did that get in my phone? unwanted app distribution on android devices,” *arXiv:2010.10088 [cs]*, Oct. 20, 2020. arXiv: 2010.10088. [Online]. Available: http://arxiv.org/abs/2010.10088.

[22] “An update on our security incident.” (2020), [Online]. Available: https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.

[23] “Twitter says hacking of high-profile twitter accounts was a "coordinated social engineering attack".” (2022), [Online]. Available: https://www.cbsnews.com/news/twitter-hack-verified-accounts-social-engineering-bitcoin-scam/.

[24] “Incident report: Employee and customer account compromise - august 4, 2022,” Twilio Blog. (), [Online]. Available: https://www.twilio.com/blog/august-2022-social-engineering-attack.

[25] “Findings on COVID-19 and online security threats,” Google. (Apr. 22, 2020), [Online]. Available: https://blog.google/threat-analysis-group/findings-covid-19-and-online-security-threats/.

[26] M. Hijji and G. Alam, “A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions,” *IEEE Access*, vol. 9, pp. 7152–7169, 2021, Conference Name: IEEE Access, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3048839.

[27] “Cyber resilient business accenture.” (2023), [Online]. Available: https://www.accenture.com/ca-en/insights/cyber-security-index.

[28] B. News. "California university paid $1.14 million after ransomware attack - BNN bloomberg," BNN. Section: Technology. (Jun. 27, 2020), [Online]. Available: https://www.bnnbloomberg.ca/california-university-paid-1-14-million-after-ransomware-attack-1.1457176.

[29] "The 2021 ponemon cost of phishing study Proofpoint US," Proofpoint. (Jul. 28, 2021), [Online]. Available: https://www.proofpoint.com/us/resources/analyst-reports/ponemon-cost-of-phishing-study.

[30] "Fraud alert: COVID-19 scams," Office of Inspector General Government Oversight U.S. Department of Health and Human Services. (Dec. 24, 2020), [Online]. Available: https://oig.hhs.gov/fraud/consumer-alerts/fraud-alert-covid-19-scams/.

[31] "INFRASTRUCTURE SECURITY CISA." (2023), [Online]. Available: https://www.cisa.gov/infrastructure-security.

[32] S. Nifakos, K. Chandramouli, C. K. Nikolaou, *et al.*, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, p. 5119, Jan. 2021, Number: 15 Publisher: Multidisciplinary Digital Publishing Institute, ISSN: 1424-8220. DOI: 10.3390/s21155119. [Online]. Available: https://www.mdpi.com/1424-8220/21/15/5119.

[33] M. S. Jalali and J. P. Kaiser, "Cybersecurity in hospitals: A systematic, organizational perspective," *Journal of Medical Internet Research*, vol. 20, no. 5, e10059, May 28, 2018, Company: Journal of Medical Internet Research Distributor: Journal of Medical Internet Research Institution: Journal of Medical Internet Research Label: Journal of Medical Internet Research Publisher: JMIR Publications Inc., Toronto, Canada. DOI: 10.2196/10059. [Online]. Available: https://www.jmir.org/2018/5/e10059.

[34] o. Object, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," [Online]. Available: https://core.ac.uk/reader/157854043?utm_source=linkout.

[35] "Investigation: WannaCry cyber attack and the NHS - national audit office (NAO) report," National Audit Office (NAO), Oct. 27, 2017. [Online]. Available: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/.

[36] R. Luo, R. Brody, A. Seazzu, and S. Burd, "Social engineering: The neglected human factor for information security management," *IRMJ*, vol. 24, pp. 1–8, Jul. 1, 2011. DOI: 10.4018/irmj.2011070101.

[37] N. Conteh and P. Schmick, "Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks," *International Journal of Advanced Computer Research*, vol. 6, pp. 31–38, Feb. 12, 2016. DOI: 10.19101/IJACR.2016.623006.

[38] B. M. Bowen, R. Devarajan, and S. Stolfo, "Measuring the human factor of cyber security," in *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, Nov. 2011, pp. 230–235. DOI: 10.1109/THS.2011.6107876.

[39] M. Junger, L. Montoya, and F. .-. Overink, "Priming and warnings are not effective to prevent social engineering attacks," *Computers in Human Behavior*, vol. 66, pp. 75–87, Jan. 1, 2017, ISSN: 0747-5632. DOI: 10.1016/j.chb.2016.09.012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0747563216306392.

[40] art-kohn. "Brain science: The forgetting curvethe dirty secret of corporate training," Learning Solutions Magazine. (Mar. 13, 2014), [Online]. Available: https://learningsolutionsmag.com/articles/1379/brain-science-the-forgetting-curvethe-dirty-secret-of-corporate-training.

[41] J. Saleem and M. Hammoudeh, "Defense methods against social engineering attacks," in *Computer and Network Security Essentials*, K. Daimi, Ed., Cham: Springer International Publishing, 2018, pp. 603–618, ISBN: 978-3-319-58424-9. DOI: 10.1007/978-3-319-58424-9_35. [Online]. Available: https://doi.org/10.1007/978-3-319-58424-9_35.

[42] A. Alzahrani, "Coronavirus social engineering attacks: Issues and recommendations," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 5, 2020, ISSN: 21565570, 2158107X. DOI: 10.14569/IJACSA.2020.0110523. [Online]. Available: http://thesai.org/Publications/ViewPaper?Volume=11%5C&Issue=5%5C&Code=IJACSA&SerialNo=23.

[43] J.-H. Cho, H. Cam, and A. Oltramari, "Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis," in *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, ISSN: 2379-1675, Mar. 2016, pp. 7–13. DOI: 10.1109/COGSIMA.2016.7497779.

[44] C. C. Campbell, "Solutions for counteracting human deception in social engineering attacks," *Information Technology & People*, vol. 32, no. 5, pp. 1130–1152, Jan. 1, 2018, Publisher: Emerald Publishing Limited, ISSN: 0959-3845. DOI: 10.1108/ITP-12-2017-0422. [Online]. Available: https://doi.org/10.1108/ITP-12-2017-0422.

[45] D. Sittig and H. Singh, “A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks,” *Applied Clinical Informatics*, vol. 07, no. 2, pp. 624–632, Apr. 2016, ISSN: 1869-0327. DOI: 10.4338/ACI-2016-04-SOA-0064. [Online]. Available: http://www.thieme-connect.de/DOI/DOI?10.4338/ACI-2016-04-SOA-0064.

[46] D. Airehrour, N. Vasudevan Nair, and S. Madanian, “Social engineering attacks and countermeasures in the new zealand banking system: Advancing a user-reflective mitigation model,” *Information*, vol. 9, no. 5, p. 110, May 2018, Number: 5 Publisher: Multidisciplinary Digital Publishing Institute. DOI: 10.3390/info9050110. [Online]. Available: https://www.mdpi.com/2078-2489/9/5/110.

[47] W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire, “Phishing in healthcare organisations: Threats, mitigation and approaches,” *BMJ Health & Care Informatics*, vol. 26, no. 1, e100031, Sep. 4, 2019, ISSN: 2632-1009. DOI: 10.1136/bmjhci-2019-100031. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7062337/.

[48] M. S. Jalali, M. Bruckes, D. Westmattelmann, and G. Schewe, “Why employees (still) click on phishing links: Investigation in hospitals,” *Journal of Medical Internet Research*, vol. 22, no. 1, e16775, Jan. 23, 2020, Company: Journal of Medical Internet Research Distributor: Journal of Medical Internet Research Institution: Journal of Medical Internet Research Label: Journal of Medical Internet Research Publisher: JMIR Publications Inc., Toronto, Canada. DOI: 10.2196/16775. [Online]. Available: https://www.jmir.org/2020/1/e16775.

[49] W. Gordon, A. Wright, R. Aiyagari, *et al.*, “Assessment of employee susceptibility to phishing attacks at US health care institutions,” *JAMA Network Open*, vol. 2, e190393, Mar. 8, 2019. DOI: 10.1001/jamanetworkopen.2019.0393.

[50] D. Barrett and R. Heale, “What are delphi studies?” *Evidence-Based Nursing*, vol. 23, no. 3, pp. 68–69, Jul. 1, 2020, Publisher: Royal College of Nursing Section: Research made simple, ISSN: 1367-6539, 1468-9618. DOI: 10.1136/ebnurs-2020-103303. [Online]. Available: https://ebn.bmj.com/content/23/3/68.

[51] J. E. Lerums, “Measuring the state of indiana’s cybersecurity,” thesis, Purdue University Graduate School, Jan. 16, 2019. DOI: 10.25394/PGS.7449230.v1. [Online]. Available: https://hammer.purdue.edu/articles/thesis/Measuring_the_State_of_Indiana_s_Cybersecurity/7449230/1.

[52] M. R. Thomas, “DEVELOPING TRAINING MATERIALS TO SUPPLEMENT THE INDIANA CYBERSECURITY SCORECARD,” thesis, Purdue University Graduate School, Jul. 20, 2022. DOI: 10.25394/PGS.20321634.v1. [Online]. Available: https://hammer.purdue.edu/articles/thesis/DEVELOPING_TRAINING_MATERIALS_TO_SUPPLEMENT_THE_INDIANA_CYBERSECURITY_SCORECARD/20321634/1.

A. Survey

Below are the definitions of the terms used in the questionnaire. The sources for the definitions have been mentioned.

Social Engineering is a general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious (NIST SP 1800-21B).

Phishing: A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person (NIST SP 800-114).

Vishing/Voice Phishing: Vishing refers to phishing attacks that involve the use of voice calls, using either conventional phone systems or Voice over Internet Procotol (VoIP) systems (https://www.cisa.gov/uscert/ncas/tips/ST04-014).

Smshing/SMS Phishing: Smishing refers to phishing attacks that involve the use of messages sent using SMS (Short Message Service) (https://www.cisa.gov/uscert/ncas/tips/ST04-014).

Pretexting: Pretexting is a type of social engineering attack that involves a situation, or pretext, created by an attacker to lure a victim into a vulnerable situation and to trick them into giving private information, specifically information that the victim would typically not give outside the context of the pretext (NIST SP 800-12 Rev. 1).

Baiting: A type of social engineering attack where an attacker uses a false promise to lure a victim into a trap which may steal personal and financial information or inflict the system with malware (https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html).

Quid Pro Quo: Quid pro quo involves an attacker requesting the exchange of some type of sensitive information such as critical data, login credentials, or monetary value in exchange for a service (https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html).

Q How prepared is the Healthcare and Public Health Sector for cybersecurity related threats?

- Always Prepared

- Somewhat Prepared
- Slightly Prepared
- Unprepared

Q Please rank the following from most likely to least likely motivator of a cybersecurity attack in the Healthcare and Public Health Sector.

- Financial Gain
- Operation Disruptions
- Hacktivism
- Nation State Attacks
- Others, please specify

Q Please rank the following from most important to least important impacts of a cybersecurity attack to **organizations** in the Healthcare and Public Health Sector.

- Operation Disruptions
- Data Loss/Exposure
- Loss of Trust and Brand damage
- Financial Damage inclusive of fines
- Others, please specify

Q Please rank the following from most important to least important impacts of a cybersecurity attack to **users (Patients)** in the Healthcare and Public Health Sector.

- Data Loss/Exposure
- Financial Damage

- Loss of time and schedule disruptions
- Others, please specify

Q Please rank the following from most important to least important impacts of a cybersecurity attack to **employees (E.g., Doctors, Administrative Employees)** in the Healthcare and Public Health Sector.

- Data Loss/Exposure
- Financial Damage
- Loss of time and schedule disruptions
- Others, please specify

Q Please rank the following from the easiest to the most difficult type of social engineering attacks in the Healthcare and Public Health Sector for an attacker to perform.

- Email Phishing
- Vishing and Smishing
- Pretexting
- Baiting
- Quid Pro Quo

Q Please rank the following social engineering attacks from the highest to lowest success rate in the Healthcare and Public Health Sector.

- Email Phishing
- Vishing and Smishing
- Pretexting
- Baiting

- Quid Pro Quo

Q Please rank the following social engineering attacks with respect to potential for direct financial losses in the Healthcare and Public Health Sector (e.g. records of bills being removed).

- Email Phishing
- Vishing and Smishing
- Pretexting
- Baiting
- Quid Pro Quo

Q Please rank the following social engineering attacks which causes the most amount of sensitive data exposure in the Healthcare and Public Health Sector.

- Email Phishing
- Vishing and Smishing
- Pretexting
- Baiting
- Quid Pro Quo

Q Please rank the following social engineering attacks which would require the most extensive forensic investigation after an attack has occurred.

- Email Phishing
- Vishing and Smishing
- Pretexting
- Baiting

- Quid Pro Quo

Q Please rank the following attacks in order of how dangerous you perceive them to be to the Healthcare and Public Health Sector.

- Email Phishing
- Vishing and Smishing
- Pretexting
- Baiting
- Quid Pro Quo

Q Please rank the following criteria in terms of most important when judging which type of social engineering attack is the most dangerous to the Healthcare and Public Health Sector.

- Financial or monetary loss
- Sensitive data exposure or privacy loss
- Number of attacks
- Success percentage of attacks
- Others, please specify

Q Please rank the following preventive measures do you believe is the most effective against social engineering based cybersecurity incidents in the Healthcare and Public Health Sector.

- Training and Awareness for users
- Compliance based standards and regulatory bodies
- Technical countermeasures (Eg. Firewalls, Access Control)

- Others, please specify

Q What other social engineering attack vectors have we not included that may impact organizations in the Healthcare and Public Health Sector?

Q What other social engineering attack vectors have we not included that may impact individuals in the Healthcare and Public Health Sector?

Q Any comments, advice or suggestions?