

Enhancing Cybersecurity Awareness Among Small Business Owners

An Assessment and Development Strategy



December 14, 2023

Sarah Alhussain

# Abstract

# This research paper investigates the increasing prevalence of cyberattacks and the critical need for cybersecurity awareness among small business owners. Despite recognizing the importance of cybersecurity, many businesses need a more comprehensive understanding of protection methods. The study explores current awareness levels through interviews with small business owners and subject matter experts, aiming to develop an effective cybersecurity awareness program. It examines the effectiveness of various communication strategies, including multimedia, to enhance engagement and education. The findings highlight significant gaps in knowledge and provide recommendations for future communication efforts to equip small businesses with essential cybersecurity practices better.

# Introduction

Cyberattacks are on the rise, with many people being scammed out of their money and businesses because they lack awareness about different protection methods. Typically, cyberattacks happen to corporations and large organizations, with many top Saudi companies targeted in the last few months. Razaque et al. (2021 posit that although people are aware of the need for security, they still show a level of ignorance when it comes to protecting themselves. Razaque et al. (2021) continue to say that “individuals have tunnel vision regarding information security basics” (p. 2). For this reason, it is imperative to educate the public about modes of protection and how to read the warning signs.

These major companies have security systems to help limit the number of successful penetrations. However, small business owners may need to be made aware of the seriousness of the threat or may not be exempt from these attacks.

# Background

The Saudi Government has been working hard to educate the population about methods that could help them protect themselves. De Bruijn et al. (2017) give one method on how governments try to educate the public on cybersecurity. This method is called message framing, which is a strategy for converting complex problems into more understandable messages that the public can understand and use to avoid cyber threats. De Bruijn, et al., (2017). However, it has been difficult to reach most people because their level of knowledge of cybersecurity has yet to be discovered. Cary et al. (2014) state that when the Audience's knowledge level about a particular subject is unknown, it is better to write for most of the Audience than a selected few. It is also advisable to cover the subject in as much detail as the Audience needs. This method will be more straightforward for all audiences and allow expert audiences to learn something new.

Therefore, the project aimed to create a cybersecurity awareness program in which small business owners will be educated about cybersecurity and what method would best help protect their businesses and employees from cyber threats.

For this project, the interview method was used to collect data from small business owners who agreed to participate in the research. The results generated from the interviews were satisfactory, considering the time constraints and limitations of the project. The results give some idea about their level of awareness. The interviews also show where the program needs to focus on content creation.

# Research Objectives

The objectives of the Interview Research Plan were to

* Identify the topics of the awareness program by:
  + They interviewed users to gain perspective on their thoughts and ideas about their interest in cybersecurity and the topics they would like to learn more about.
  + I am interviewing subject matter experts (SMEs) about cybersecurity-related topics such as protection methods and types of threats and attacks.

Results from Secondary Research

The secondary research focused on generating results from three categories: Audience, content, and means of communication. The following section focuses on these three categories separately to answer the following questions:

1. Who is the target audience?
2. What do they need to know?
3. Which means of communication should we use to convey the information?

## Audience

There are a few things technical communicators can do to understand their intended Audience. Some methods include distributing surveys, conducting interviews, and developing a profile of the Audience (Johnson-Sheehan, 2018). For this project, we used the interview research plan to collect qualitative information that could aid in the creation of a cybersecurity awareness program. Compelling content, design, and communication methods were considered during the interview. The information collected from the interviews will help identify the content that most benefits the Audience and what means of communication to use to begin creating the awareness program.

## Content

Collecting content for the awareness program was challenging because it was unclear what information was relevant to the target audience and what was not. Knowing the objectives and outcomes of the proposed project is the best way to understand where to begin researching for collecting the content (Johnson-Sheehan, 2018). According to (Cary et al., 2014), content must be arranged on a communication piece to make sense. Content must also be helpful and valuable to keep the audience engaged during the program. The subject matter expert interviews were conducted to gain the information needed to begin creating and arranging the content necessary to develop the awareness program.

## Means of Communication

Determining which form to use for the information once the content was gathered and completed was difficult. s finally decided to use mixed methods incorporating audio, video, and visuals to engage the senses in multimedia. Amadieu et al. (2017) define multimedia as the presentation of material in both verbal and pictorial forms. Using different forms to relay information allows learner engagement and prompts active learning. Using multimedia to transfer knowledge to learners helps them feel connected to the text and supports learning outcomes (Robles et al., 2019). According to (Amadieu et al., 2017), multimedia learning involves researching appropriate content and organizing it into different formats.

# Participants and Setting

As the program targets small business owners, seven interviews with business owners were scheduled and conducted to gain insight into their current level of knowledge on cybersecurity. The purpose of these interviews is to aid in determining what areas the research needs to explore profoundly and what topics need to be focused on.

In addition to the business owner interviews, three interviews with subject matter experts were conducted to answer any content-related questions that could help create the cybersecurity awareness program. Amadieu et al. (2017) say that to form meaning from content, the writer or program developer needs to have some background knowledge of the subject being delivered to the Audience. These interviews will help gain details and more understanding about the topics and themes brought up in the interviews.

Research Method

For this project, the qualitative method collected data about the awareness of small business owners about cybersecurity. This method also measured their understanding of the systems they could use to add security to their network and server to protect their business and employees from cyberattacks and threats.

Qualitative data was collected through interviews with seven business owners representing the target audience, as well as from 3 subject matter experts (SMEs). The SMEs provided a more in-depth clarification about the topics brought up during the audience interviews.

All interviews were conducted quietly, away from distraction and noise. Interviews were set up in advance at a time and place that suited the interviewees. There was an option for virtual interviews via Teams, Zoom, or Skype, and two interviewees chose this option. Interviewees were asked for permission and consent to have the interview recorded to allow for later review of the answers provided. Each interview took approximately 30-40 minutes. All interviews were conducted with no difficulty.

# Analysis of Results from Primary Research

The interviews generated interesting results that focused the research. The data was collected and arranged by asking the interviewees questions, which mainly focused on content and mode of delivery. This report will focus on the highlights of the interview, which measure the level of awareness when it comes to Cybersecurity knowledge.

## Defining Cybercrime

Researching cybercrime found that it is defined as an illegal computer-mediated activity that is achieved through interfering in global systems and networks (Razaque et al., 2012). When asked what cybercrime was, the seven interviewees viewed it as:

* Threats
* Spying
* Theft
* Crisis

Figure 1: Statistics of Cybercrime Meaning

When asked to clarify what was meant by crisis, the interviewee posited that it was a crisis because it causes unwanted disruption in the system, which interferes with business. Secondary research mentioned similar findings when it came to the definition of cybercrime. For example, Puthal et al. (2017) list three major possibilities for potential threats: server exploitations, credential theft from users, and attacks during communication. De Bruijn et al. (2017) also states that cyberattacks come in different forms, including hacking, stealing data, manipulating data, identity theft, and taking over control of a system. SMEs clarified that cybercrime is all the listed above and can range from no impact to severe impact (De Bruijn et al., 2017). No impact means that it does not harm the user in any way but causes annoyance until removed.

## Modes of Protection

When asking the interviewees what they used to protect their systems, they answered as follows:

|  |  |  |
| --- | --- | --- |
| **Protection Methods Used** | **Yes** | **No** |
| Antivirus | 7 | 0 |
| Antispyware | 7 | 0 |
| Firewall | 7 | 0 |
| Encrypted passwords | 7 | 0 |
| Authentication System | 3 | 4 |

Table 1: Protection Method Used by Audience

The table above shows the number of interviewees who have used the protection method indicated in each row. According to (Puthal et al., 2017), the traditional method used to protect systems is IP security (IPsec.), which protects data flows between hosts and networks. According to our SMEs, IP security can be done using a Fly-Away kit, which works as an airplane black box. It records all the happenings on the network and allows experts to find breaches to eliminate threats and attacks. It also enables them to find weaknesses to make the system more robust.

Furthermore, (Puthal et al., 2017) explain another method in which entry to applications of accounts must be authenticated via a code or message sent to the owner on their devices. SDP is suitable for office servers, systems, and personal and remote work. The SMEs posit that using an authentication system is the best way to limit attacks. The data collected shows that most of our target audience still needs an authentication system at their businesses. When asked why they do not implement an authentication system, most replied that it was too costly for them as their new business is new. It would be advisable to inform them of the awareness program about the importance of investing in an authentication system to decrease the potentiality of a cyberattack.

These interviews show that our Audience knows a little about cybersecurity but needs more in-depth knowledge of how to protect their business. The content created for the awareness program should focus on server and network protection, how cyberattacks occur, and the importance of using the proper security method to log into and protect their employees and systems.

# Limitations and Recommendations for Future Communication

This project aimed to measure the level of awareness that small business owners have regarding cybersecurity before creating a cybersecurity awareness program. However, as the company intends to bring awareness to a larger population in the future, there may be more than this research method for a broader target audience. This is due to the time constraints that limited the number of participants during the small business owner interview phase. This may have constricted the results to reduced answers that generated limited topics. Even though the interviews generated satisfactory results for this project, it is recommended that a formal survey be conducted to reach a larger target population to measure a more precise awareness level in Saudi Arabia before developing an awareness program that will reach the public.

Conclusion

This study emphasizes the need to bolster cybersecurity awareness among small business owners, who are increasingly targeted by cyberattacks despite their critical role in the economy. The interviews and secondary research reveal a clear gap in understanding the depth of cybersecurity threats and effective protection strategies. While small business owners are generally aware of basic security measures, they often need more comprehensive knowledge about advanced protection methods and the importance of investing in robust security systems.

The findings highlight the need for an engaging and informative cybersecurity awareness program to address these gaps. By leveraging multimedia and varied communication methods, the proposed program aims to make complex cybersecurity concepts accessible and actionable for a broader audience. This approach will not only enhance the immediate security posture of small businesses but also foster a culture of vigilance and proactive defense against cyber threats.

Moving forward, it is crucial to expand the scope of this research to encompass a larger audience and refine the program based on feedback and evolving cybersecurity trends. Through continuous education and the implementation of adequate security practices, small business owners can better protect their assets and contribute to a more resilient digital landscape.

## References

Amadieu, F., Lemarié, J., & Tricot, A. (2017). How may multimedia and hypertext documents support deep processing for learning? *Psychologie Française*, *62*(3), 209–221. https://doi.org/10.1016/j.psfr.2015.04.002

Carey, M., Lanyi, M. M. F., Longo, D., Radzinski, E., Rouiller, S., & Wilde, E. (2014). *Developing quality technical information: A handbook for writers and editors* (3rd ed.). IBM Press.

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. <https://doi.org/10.1016/j.giq.2017.02.007>

Johnson-Sheehan, R. (2018). *Technical communication today* (6th ed.). Pearson.

Puthal, D., Mohanty, S. P., Nanda, P., & Choppali, U. (2017). Building security perimeters to protect network systems against cyber threats [future directions]. *IEEE Consumer Electronics Magazine*, *6*(4), 24–27. https://doi.org/10.1109/mce.2017.2714744

Razaque, A., Al Ajlan, A., Melaoune, N., Alotaibi, M., Alotaibi, B., Dias, I., Oad, A., Hariri, S., & Zhao, C. (2021). Avoidance of cybersecurity threats with the deployment of a web-based blockchain-enabled Cybersecurity Awareness System. *Applied Sciences*, *11*(17), 7880. <https://doi.org/10.3390/app11177880>

Robles, V. D., & Baker, M. J. (2019). Using case-method pedagogy to facilitate audience awareness. *IEEE Transactions on Professional Communication*, *62*(2), 192–207. https://doi.org/10.1109/tpc.2019.2893464