**Extended Abstract**

This document describes the protocol applied in a qualitative interpretive study on the Cybersecurity challenges faced by telehealth service providers and the lessons learned during Covid 19 pandemic by conducting interviews with the cybersecurity and privacy professionals and leaders from telehealth organizations. This work presents the different parts of such protocol, the interview guide used in the study, and population characteristics.

Keywords — Cybersecurity, Covid-19, telehealth, Privacy, Security

Introduction

Telehealth services have witnessed an unprecedented surge in adoption during Covid 19. A prior study notes that claims from telehealth services increased by 4000% during the pandemic. Studies also suggest that some telehealth practices adopted during the pandemic are likely to stick in the post-pandemic world and get accepted as the new normal [3]. However, the transition to telehealth services has also led to several cybersecurity incidents and breaches. This study explores challenges faced by cybersecurity professionals in telehealth organizations during Covid 19 and the emergent lessons learned from this experience. Subsequently, it recommends cybersecurity controls and best practices for telehealth organizations to prepare for mainstream adoption of these services.

The protocol is classified into the following parts.

* Goal of the study and research questions

The principal objective of this study is to understand the cybersecurity challenges faced by contemporary telehealth organizations during the covid 19 pandemic. It also attempts to uncover the emergent lessons learned by telehealth organizations to develop cybersecurity recommendations for mainstream adoption of telehealth services. Specifically, it addresses the following research questions

* + What are the common types of cybersecurity attacks faced by telehealth organizations? What is the frequency and impact of these attacks?
  + How are telehealth organizations addressing these cybersecurity challenges?
  + What are some of the emergent best practices that are critical to the success of implementing cybersecurity for telehealth organizations in the post pandemic world?
* Study selection (conduct semi-structured interviews)

This study used qualitative and interpretive research methodology to explore the research questions. We interviewed professionals involved in managing and securing telehealth platforms such as cybersecurity engineers, security analysts, consultants, chief information security officers (CISO). Semi-structured interviews helped uncover profound insights into the proposed research areas. They encouraged the interviewers to seek more information through discussions and clarifications while collecting data, making it possible to refine and elaborate on interesting perspectives. Also, the open nature of semi-structured interviews revealed interesting additional inputs to the study not targeted by the research questions presented above.

* Research team

|  |  |  |  |
| --- | --- | --- | --- |
| Member | Interviews | Coding & Memoing | Analysis and Writing |
| Pavankumar Mulgund | Yes | Yes | Yes |
| Banashri Mulgund | Yes | Yes | Yes |
| Raghavendra Singh | Yes | Yes | Yes |
| Dominic Stellato | Yes |  | Yes |

* Population sampling strategy

Cybersecurity is a critical aspect of telehealth organizations. With HIPAA and other data privacy regulations in place for telehealth organizations, implementing cybersecurity for telehealth platform is important. Therefore, this study is aimed to include practitioners involved in several cybersecurity projects around telehealth applications. We chose the target population from US-based telehealth clinics for convenience. We included as many diverse characteristics as possible concerning their teams’ size, domain expertise, and business process. It was aimed to get insights from the experiences and challenges they faced during pandemic in implementing cybersecurity. A total of X interviews with professionals from these Y telehealth clinicals was conducted.

* Procedure and instruments

We conducted three pilot interviews to test the interview guide and allow researchers to practice interview flow and style. Questions were fine-tuned in terms of phrasing and ordering after the pilot interviews. To resemble an actual interview, we conducted the pilots with researchers doing the role of interviewees. To simulate a real interview environment, the interviewer did not meet the chosen researchers ahead of time. The interview guide was divided into different sections, and most questions were open-ended.

* Data collection

The interview session was organized and prepared as per the interview guide. The interview guide was emailed to all interviewees a week before the interview. All interviewees were requested to review the interview questions and fill in Section A of the interview guide (i.e., personal information, organization, role). The answers collected were sent to the interviewers before the interview, which helped them assess the interviewee's background.

At the beginning of the meeting, interviewees were asked descriptions of the telehealth services offered by their organization (corresponding to Section B of the guide). Subsequently, data related to corresponding research questions were gathered. The interviews were conducted using zoom or similar tools. Each meeting lasted for about 1 hour, of which 15 minutes were used for introductions (if necessary); 45 minutes were used to answer interview questions.

* Data analysis techniques

We performed data analysis by combing through the data in several iterations. In early iterations, we performed ‘open coding’ to dissect the interview transcripts for keywords and phrases. In subsequent iterations, we grouped related phrases and keywords into concepts. We used axial coding to explore salient attributes. Further, we weaved these concepts together to identify emergent themes. We also integrated the reflections captured by the researchers throughout the coding process to derive our findings.

* Threats to validity
* The interview guide (as an appendix)

Also, even if not part of the protocol, this document includes a second appendix with details about the population.

**Appendix: Questions exploring cybersecurity issues with telehealth organizations**

1. Could you please tell us about your professional journey into cybersecurity profession?
2. Could you elaborate on the type of telehealth applications you are working on?
3. What kind of cybersecurity risks have emerged in the telehealth field due to COVID 19 pandemic?
4. What are some of the most frequent cybersecurity issues/attacks faced by the telehealth organizations during pandemic?
5. How are healthcare firms addressing these emerging cybersecurity challenges?
6. What kind of countermeasures are being put in place? How do organizations prioritize among these countermeasures?
7. What are some of the bottlenecks faced by cybersecurity teams within the telehealth services?
8. What are some of the biggest gaps that exist with regards to cybersecurity of telehealth applications?
9. What are some of the key lessons learned in terms of cybersecurity from the pandemic experience?
10. As we transition to post pandemic world, what will be key cybersecurity priorities of organizations offering telehealth services?
11. What are some of the emergent best practices in securing telehealth services?