Paper Analysis
Paper Name: Determining Small Business Cybersecurity Strategies to Prevent Data Breaches
Author's Name: Jennifer A. Saber (Walden University, 2016)

1. Summary of the Introduction

The introduction establishes the critical and growing threat of cybercrime, noting that the internet's ease of access and anonymity are exploited for crimes like data and identity theft, which cause global economic damage. It highlights that while large corporations receive media attention, small-to-medium enterprises (SMEs) are increasingly becoming primary targets. The introductory context frames the research as essential due to the profound, often catastrophic, financial and reputational harm that data breaches inflict on small businesses and their customers.

2. Summary of the Problem Statement

The core problem statement is clearly defined by the author:
Small business leaders often lack the necessary financial resources, specialized technical expertise, and foundational knowledge required to adequately implement effective cybersecurity strategies, leaving their organizations and customer data highly vulnerable to damaging data breaches and cyberattacks.
This lack of tailored resources and knowledge creates a persistent security risk that cybercriminals readily exploit.

3. Objectives

The study's objectives were designed to bridge the gap between known threats and practical, resource-conscious solutions for small businesses.

Main Objective:
To investigate and identify effective cybersecurity strategies currently used by small business leaders to protect their organizational systems and customer data from breaches and cyber attacks.

Specific Objectives:
a.To discover what specific cybersecurity strategies small business leaders implement to protect data.

b.To explore the challenges and constraints small business leaders face when trying to implement effective cybersecurity.

c.To determine the resource-efficient practices that lead to measurable success in data breach prevention for small businesses.

4. Research Gap Addressed

The gap this study addressed lies in the existing body of knowledge regarding cybersecurity for small businesses:
Despite general awareness of cyber threats, the research literature lacked empirically validated, specific, and affordable cybersecurity strategies tailored to the unique financial and personnel

limitations of small businesses.

The research intended to provide a practical, evidence-based roadmap, moving beyond general warnings to offer actionable and accessible strategies for small business owners.