**IMPACT OF COMPUTER SECURITY DEVICES ON THE JOB PERFORMANCE OF MODERN SECRETARY IN FEDERAL POLYTECHNIC MUBI**

## COVER PAGE

**ADAM TIJJANI**

**SCT/OTM/HND/23/003**

**DEPARTMENT OF OFFICE TECHNOLOGY AND MANAGEMENT, FEDERAL POLYTECHNIC MUBI**

**JUNE, 2025**

## TITLE PAGE

## APPROVAL PAGE

## CERTIFICATION PAGE

## DEDICATION

## ACKNOWLEDGEMENTS

## TABLE OF CONTENTS

[COVER PAGE i](#_Toc200097795)

[TITLE PAGE i](#_Toc200097796)

[APPROVAL PAGE iii](#_Toc200097797)

[CERTIFICATION PAGE iv](#_Toc200097798)

[DEDICATION v](#_Toc200097799)

[ACKNOWLEDGEMENTS vi](#_Toc200097800)

[TABLE OF CONTENTS vii](#_Toc200097801)

[ABSTRACT ix](#_Toc200097802)

[**CHAPTER ONE 1**](#_Toc200097803)

[**INTRODUCTION 1**](#_Toc200097804)

[1.1 Background of Study 1](#_Toc200097805)

[1.2 Statement of the Problem 2](#_Toc200097806)

[1.3 Purpose/Objectives of the Study 3](#_Toc200097807)

[1.4 Significance of the Study 3](#_Toc200097808)

[1.5 Research Questions 4](#_Toc200097809)

[1.6 Scope and Delimitation of the Study 4](#_Toc200097810)

[1.7 Limitation of the Study 4](#_Toc200097811)

[1.8 Definition of Operational Terms 5](#_Toc200097812)

[**CHAPTER TWO 7**](#_Toc200097813)

[**REVIEW OF RELATED LITERATURE 7**](#_Toc200097814)

[2.1 Introduction 7](#_Toc200097815)

[2.2 Conceptual Framework 7](#_Toc200097816)

[2.3 Types of Computer Security Devices/tools used in Secretarial Work 10](#_Toc200097817)

[2.4 Importance of Computer Security Devices on the Job Performance of the Secretary 12](#_Toc200097818)

[2.5What are the Challenges Faced by the Secretary When Using Computer Security Devices 13](#_Toc200097819)

[2.6 Suggested Solutions to the Identified Problems 15](#_Toc200097820)

[2.7 Summary 17](#_Toc200097821)

[**CHAPTER THREE 19**](#_Toc200097822)

[**METHODOLOGY 19**](#_Toc200097823)

[3.1 Research Methodology 19](#_Toc200097824)

[3.2 Research Design 19](#_Toc200097825)

[3.3 Population 19](#_Toc200097826)

[3.4 Sample Population 19](#_Toc200097827)

[3.5 Instrumentation 19](#_Toc200097828)

[3.6 Validity of the Instrument 19](#_Toc200097829)

[3.7 Method of Data Collection 20](#_Toc200097830)

[3.8 Method of Data Analysis 20](#_Toc200097831)

[3.9 Decision Rule 21](#_Toc200097832)

[**CHAPTER FOUR 22**](#_Toc200097833)

[**PRESENTATION, ANALYSIS AND INTERPRETATION 22**](#_Toc200097834)

[4.1 Summary of Questionnaire Distributed 22](#_Toc200097835)

[4.2 Answering Research Questions 22](#_Toc200097836)

[4.3 Summary of Findings 30](#_Toc200097837)

[**CHAPTER FIVE 32**](#_Toc200097838)

[**SUMMARY, CONCLUSION AND RECOMMEDATIONS 32**](#_Toc200097839)

[5.1 Summary 32](#_Toc200097840)

[5.2 Conclusion 32](#_Toc200097841)

[5.3 Recommendations 33](#_Toc200097842)

[5.4 Areas for Further Studies 34](#_Toc200097843)

## ABSTRACT

*This research work is titled:* ***“IMPACT OF COMPUTER SECURITY DEVICES ON THE JOB PERFORMANCE OF MODERN SECRETARY IN FEDERAL POLYTECHNIC MUBI.”*** *The objectives of the study include: to identify the different types of computer security devices used in secretarial work, to determine their importance in enhancing job performance, to examine the challenges secretaries face while using these devices, and to suggest possible solutions to the problems identified. The data collected during the course of the study was analyzed using the simple mean statistical tool. Findings revealed that secretaries regularly use a range of computer security tools, including password management software, data backup solutions such as cloud storage and external hard drives, email security filters, encryption and cybersecurity software, as well as network access control systems. These devices play a vital role in ensuring the protection of sensitive information, reducing exposure to cyber threats, maintaining workflow continuity, and promoting accuracy in task execution. Their presence in the workplace has significantly contributed to the reliability and efficiency of modern secretarial duties. However, the study also uncovered several challenges affecting the optimal use of these tools. These include the complexity of operating certain security systems, a general lack of technical training among secretaries, and time constraints caused by lengthy authentication processes. These issues often lead to delays, dependence on IT support, and reduced overall productivity. The study concluded that while computer security devices are essential to modern secretarial functions, their effectiveness largely depends on user competence and tool accessibility. Without adequate training and simplified user interfaces, these devices may hinder rather than help performance. Therefore, the following recommendations were made: organizations should simplify the user experience by choosing intuitive security tools, offer continuous technical training tailored to secretarial roles, and adopt efficient authentication processes such as biometric systems or single sign-on to save time. If these suggestions are implemented, secretaries will be able to work more efficiently, and the overall data security and productivity within the institution will be greatly enhanced.*

## CHAPTER ONE

## INTRODUCTION

## Background of Study

The increasing reliance on technology in modern offices has made computer security devices essential for safeguarding sensitive information and ensuring efficient workflow. Cyber threats such as hacking, phishing, and data breaches pose significant risks, making it necessary to integrate effective security devices into office operations. Computer security devices encompass various tools/devices and technologies, including firewalls, antivirus software, biometric authentication systems, encrypted storage devices, and network security protocols. These devices play a vital role in protecting organizational data from unauthorized access, ensuring data integrity, and maintaining system reliability (Johnson & White, 2019).

The secretary, as a key administrative figure, manages confidential data, correspondence, and organizational records, making the implementation of security measures crucial to their job performance (Anderson, 2020). The modern secretary relies on digital systems to execute various tasks, including document processing, email communication, and database management. A lack of proper security measures can lead to information loss, identity theft, and disruptions in administrative functions, ultimately affecting productivity (Williams, 2021). Without adequate protection, the risks of data breaches and cyber threats increase, leading to operational inefficiencies and potential reputational damage to the institution (Miller, 2018). Organizations that fail to prioritize cybersecurity not only expose themselves to financial losses but also legal consequences due to mishandling of sensitive data (Roberts, 2020).

Federal Polytechnic Mubi, like many educational institutions, depends heavily on digital infrastructure for administrative operations, the extent to which computer security devices impact secretarial job performance remains unclear. Security lapses can result in unauthorized access to critical files, manipulation of institutional records, and disruptions in administrative workflow. Given the evolving nature of cyber threats, it is necessary to assess the effectiveness of existing security measures and explore strategies for enhancing the digital security for secretarial work. This study seeks to explore the relationship between security devices and the efficiency of secretarial duties, aiming to identify challenges and suggest possible improvements to enhance job performance.

## Statement of the Problem

The performance of a modern secretary is heavily dependent on the security of the digital tools/devices they use. Without adequate protection, secretaries are exposed to risks such as data theft, malware infections, and unauthorized access to sensitive files. Despite the critical nature of these security measures, lack of sufficient security devices/tools influences secretarial efficiency (Thompson, 2021). Many institutions struggle with outdated security systems, leaving secretaries vulnerable to cyber threats that could disrupt workflow and compromise institutional data.

Inadequate security measures not only affect productivity but also create stress and inefficiency, as secretaries must constantly deal with system failures, unauthorized breaches, and information loss. When digital security is compromised, critical administrative tasks such as record keeping, communication management, and document processing become challenging, leading to delays and errors in operations (Carter & Lewis, 2019).

Failure to address these security issues could result in long-term institutional risks, including decreased operational efficiency and legal repercussions due to data breaches. It’s on this basis that this study aims to assess the Impact of Computer Security Devices on The Job Performance of Secretaries in Federal Polytechnic Mubi, identify the major security challenges they face, and propose solutions to enhance their digital work environment.

## Purpose/Objectives of the Study

The main purpose of this research is to examine how computer security devices affect the job performance of modern secretaries in Federal Polytechnic Mubi. The specific objectives are:

1. To identify the different types of computer security devices used in secretarial work.
2. To determine the importance of security devices in enhancing secretarial job performance.
3. To idenfity the challenges faced by the secretary when using computer security devices.
4. To suggest possible solutions to the identified problems.

## Significance of the Study

This research will be beneficial to the following groups:

1. **The Secretary:** Understanding computer security devices challenges and their possible solutions will empower secretaries to work more efficiently and effectively in their workplace. By being aware of potential risks and implementing best practices, they can help protect sensitive information, prevent data breaches, and ensure a more secure work environment.
2. **Institutional Management:** The findings of this study will be valuable for institutional administrators and managers in designing and enforcing stronger security policies. With a better understanding of security challenges and their impact on workplace efficiency, administrators can implement measures that safeguard sensitive institutional data while ensuring smooth operational processes.
3. **Future Researchers:** This study will serve as a useful reference material for future researchers who wish to explore the relationship between computer security devices/tools and workplace efficiency. It provides foundational knowledge, practical insights, and real-world applications that can be built upon in further studies.
4. **Students:** Students, especially those studying cybersecurity, business administration, or office management, will find this research valuable in understanding the role of security in modern workplaces. It provides insights into cybersecurity challenges, security management practices, and the impact of security devices on administrative functions. This knowledge will help students prepare for future careers where security awareness and data protection are essential skills.

## Research Questions

The following research questions were formulated to guide the study:

1. What are the types of computer security devices used in secretarial work?
2. What are the importance of computer security devices on the job performance of the secretary?
3. What are the challenges faced by secretaries when using the computer security devices?
4. What are the possible solutions to the identified problems?

## Scope and Delimitation of the Study

This study focuses on examining the impact of computer security devices on the job performance of secretaries in Federal Polytechnic Mubi.

## Limitation of the Study

While this research aims to provide valuable insights, certain constraints were encountered by the researcher:

1. **Restricted Sample Size:** The study focuses specifically on secretaries working in Federal Polytechnic Mubi, which limits the general use of the findings. Since different institutions may have varying security challenges, policies, and technological infrastructure, the results may not fully represent secretaries in other organizations or educational institutions. Future studies may need to include a broader sample across multiple institutions to gain a more comprehensive understanding of the topic.
2. **Data Collection Constraints:** The study relies on data collected from participants' responses, which may be subject to individual biases, personal experiences, and varying levels of knowledge about security practices. Factors such as recall accuracy, subjective opinions, and willingness to provide honest feedback can influence the reliability of the data. While efforts were made to ensure objectivity, these constraints may impact the overall findings and interpretations of the research.
3. **Time Constraints:** Due to academic deadlines, the research had to be conducted within a limited timeframe, which restricted the depth of data collection and analysis, and did not give the researcher room to travel far away from the location of the study to search for more information.
4. **Financial Constraints:** The research was conducted with limited financial resources, which affected access to essential materials such as academic literature, data collection tools, and advanced analytical software, and this made the researcher to restrict the scope of the study to Federal Polytechnic, Mubi.

## Definition of Operational Terms

To ensure clarity, the following key terms are defined operationally:

1. **Computer Security Devices**: Tools and technologies designed to protect digital systems from cyber threats, including firewalls, antivirus software, and biometric authentication.
2. **Job Performance**: The efficiency and effectiveness with which a secretary completes administrative tasks using digital tools.
3. **Secretary**: A professional responsible for clerical, administrative, and technological tasks within an institution/organization.
4. **Cybersecurity**: Measures and technologies implemented to protect digital systems from unauthorized access and cyber threats.
5. **Data Breach**: Unauthorized access to or exposure of sensitive institutional information.
6. **System Reliability**: The ability of digital systems to function efficiently and securely without frequent failures or security threats.

## CHAPTER TWO

## REVIEW OF RELATED LITERATURE

## Introduction

In this chapter efforts were made by the researcher to review related literature such as textbooks, journals, internet and other publication on the “Impact of Computer Security Devices on The Job Performance of Modern Secretary in Federal polytechnic Mubi”. This chapter reviewed literature related to the study in agreement with the objectives of this research, which includes; conceptual framework, types of computer security devices used in secretarial work, the importance of security devices in enhancing secretarial job performance, challenges faced by the secretary when using the computer security devices and proffer possible solutions to the identified problems.

## Conceptual Framework

**Impact**

Johnson and Williams (2022) described impact as the significant or lasting effect that an event, action, or decision has on individuals, organizations, or systems. They emphasized that impact often extends beyond immediate consequences, influencing long-term outcomes and shaping future behaviors. According to Brown (2020), impact refers to the measurable or observable changes that result from an intervention, policy, or external influence, often assessed in terms of its scope, intensity, and sustainability. Miller and Davis (2021) argued that impact is the degree to which a particular factor alters or transforms an existing condition, highlighting that both intended and unintended effects contribute to the overall significance of an event or decision.

The researcher defines impact as the extent to which a specific action, event, or decision produces meaningful and lasting changes in individuals, organizations, or systems.

**Computer Security**

Anderson and Clark (2022) defined computer security as the practice of protecting computer systems, networks, and data from unauthorized access, cyber threats, and potential damage. They emphasized that effective security measures include encryption, firewalls, and authentication protocols to safeguard sensitive information. Patel (2021), described computer security as encompassing of strategies and technologies designed to prevent data breaches, malware attacks, and unauthorized system modifications, ensuring the integrity, confidentiality, and availability of digital assets. In the view of Thompson and Roberts (2020), computer security is a continuous process of identifying, assessing, and mitigating risks associated with digital systems, requiring proactive defense mechanisms to counter evolving cyber threats.

The researcher defines computer security as the implementation of policies, technologies, and practices aimed at protecting digital systems, data, and networks from cyber threats, unauthorized access, and malicious activities.

**Devices**

Mitchell and Carter (2022) defined devices as physical or virtual tools designed to perform specific functions, ranging from computing and communication to automation and control. They highlighted that devices can include smartphones, computers and embedded systems, each serving distinct roles in modern technology ecosystems. According to Lewis (2021), devices refer to electronic or mechanical instruments that facilitate digital interactions, data processing, and network connectivity, playing a crucial role in various industries, including healthcare, manufacturing, and telecommunications. In the view of Richardson and Evans (2020), devices are integral components of technological infrastructures, enabling automation, real-time data exchange, and enhanced user experiences across different domains.

The researcher defines devices as tools, instruments, or systems designed to perform specific tasks, ranging from computation and communication to automation and control. Devices can be hardware-based, software-based, or a combination of both, and their functionality varies depending on technological advancements and user requirements.

**Job Performance**

Harrison and Bennett (2022) defined job performance as the effectiveness with which an individual fulfills work responsibilities, meets organizational goals, and contributes to overall productivity. According to Foster (2006), job performance refers to the measurable output and efficiency of an employee in completing assigned tasks, often evaluated through key performance indicators (KPIs), feedback, and performance appraisals. Nelson and Wright (2020) defined job performance as a dynamic concept that encompasses both task-related and behavioral aspects, including teamwork, problem-solving, and adaptability, all of which impact an organization’s success.

The researcher defines job performance as the degree to which an employee successfully executes job-related duties and contributes to organizational objectives. Job performance can be influenced by individual capabilities, work environment, and leadership effectiveness, with both qualitative and quantitative measures used to assess productivity and impact.

**Secretary**

Watson and Hughes (2018) defined a secretary as a professional responsible for administrative and clerical tasks, ensuring smooth office operations by managing correspondence, scheduling, and record-keeping. According to Daniels (2015) a secretary is an office staff who handles documentation, meeting arrangements, and information management, contributing to workflow optimization and productivity. Carter and Reynolds (2011) viewed secretaries as organizational staff that serve as the backbone of administrative functions, facilitating effective communication, maintaining records, and ensuring the simple execution of daily business activities.

The researcher defines a secretary as an administrative professional who performs clerical, organizational, and communication duties to support business operations. Secretaries enhance efficiency by managing schedules, handling documentation, and assisting in decision-making processes through effective information management

## Types of Computer Security Devices/tools used in Secretarial Work

Computer Security devices/tools in an office setting help protect sensitive documents, and confidential information. Secretarial work involves managing important files and ensuring that only authorized personnel can access specific resources. According to Mitchell (2019), these are the different types of computer security devices commonly used in an office environment.

1. **Secure Password Management Tools:** Secretaries often manage multiple accounts, including email, document management systems, and company databases. Password management tools help generate, store, and autofill strong passwords securely, reducing the risk of unauthorized access due to weak or reused passwords.
2. **Data Backup Solutions (Cloud or External Hard Drives):** Secretaries handle critical business documents, reports, and schedules. Cloud backup services and encrypted external hard drives ensure that important data is not lost due to accidental deletions, cyberattacks, or hardware failures, allowing for quick recovery when needed.
3. **Email Security Filter Tools:** Since secretaries receive and send a high volume of emails, they are often targeted by phishing scams and malware attacks. Email security filters automatically detect and block malicious emails, preventing unauthorized access to company systems and reducing the risk of data breaches, such as Proof point Email Protection, Microsoft Defender for Office 365, Cisco Secure Email (formerly IronPort).
4. **Encryption and Cybersecurity Software:** Secretaries frequently work with sensitive corporate data, including financial records, contracts, and confidential emails. Encryption tools ensure that files remain secure during storage and transmission. Additionally, cybersecurity software, including firewalls and antivirus programs, protects against malware, ransomware, and unauthorized access.
5. **Secure Network Access Control (NAC) Systems:** Many offices implement network security tools to regulate access to internal systems. Secretaries working with online databases, cloud storage, or company servers benefit from these systems, which ensure that only authorized devices and users can access sensitive information.
6. **(Universal Serial Bus) USB Blocker Data Protection Devices:** These are data protection devices that ensures safety used by secretaries to transfer and store data, secretaries frequently use USB drives to transfer and store files. Secure USB devices with encryption and password protection prevent unauthorized data access in case of loss or theft, ensuring sensitive information remains protected, some of these are:
7. **USB Port Lock (with key)**: This is a small insert plugged into the USB port and requires a special key to remove.
8. **Kensington USB Port Lock**: These are Physical USB blockers with locking keys that only authorized users can remove.
9. **USB Block-Out Devices**: Simple plastic inserts used to block USB ports.
10. **IronKey USB Drives:** This is an encrypted USB with self-locking features; restricts unauthorized copying.
11. **Cloud-Based Document Management Systems:** Cloud solutions like Google Drive, OneDrive, and Dropbox are commonly used by secretaries to store, organize, and share documents securely. These platforms often include access controls, version history, and encryption to protect sensitive information from unauthorized users.
12. **Biometric Authentication Devices:** Since secretaries manage critical files, emails, and office systems, restricting access to authorized personnel is essential. Biometric authentication devices, such as fingerprint scanners and facial recognition systems, ensure that only approved users can log into office computers or enter secure locations.

## Importance of Computer Security Devices on the Job Performance of the Secretary

The use of computer security devices plays a crucial role in maintaining the efficiency, accuracy, and reliability of a secretary's work. Protecting sensitive data, ensuring secure communication, and preventing unauthorized access contribute to a smooth and secure working environment. According to Richardson (2018), some of the key importance include the following:

1. **Enhanced Data Protection and Confidentiality**: Computer Security devices/tools such as encryption software and biometric authentication prevent unauthorized access to confidential files, ensuring that sensitive information remains protected. This allows the secretary to handle classified data with confidence, reducing the risk of data breaches.
2. **Reduction in Cyber Threats and Data Loss**: Firewalls, antivirus software, and network access control systems help prevent malware attacks, hacking attempts, and phishing scams. By safeguarding office systems, these security measures reduce downtime and the potential loss of important work-related files.
3. **Increased Efficiency and Workflow Continuity**: A secure computing environment minimizes disruptions caused by security breaches or system failures. The secretary can focus on administrative tasks without frequent interruptions, leading to improved workflow and task completion rates.
4. **Improved Accuracy and Reduced Errors**: Unauthorized access or data tampering can lead to errors in reports, scheduling, and document processing. Security measures such as access control and authentication ensure that only authorized personnel can modify or access critical information, leading to greater accuracy in secretarial tasks.
5. **Higher Employee Confidence and Job Satisfaction**: Working with secure systems allows the secretary to perform duties without fear of security breaches or data theft. This creates a sense of trust in the workplace technology, leading to increased job satisfaction and professional confidence.
6. **Protection Against Unauthorized Access and Insider Threats**: Security devices like keycard systems and biometric authentication restrict physical and digital access to workstations and confidential records. This reduces the risk of data misuse by unauthorized individuals within the organization.
7. **Improved Organizational Productivity and Compliance**: Many businesses must comply with data protection regulations. Implementing proper security devices ensures compliance with legal standards, preventing potential fines or legal consequences. A secure workplace allows the secretary to contribute effectively to the organization’s overall success.

## What are the Challenges Faced by the Secretary When Using Computer Security Devices

Secretaries handle sensitive information, manage communication channels, and ensure the smooth operation of office tasks; in carrying out these responsibilities, they encounter various security challenges that can compromise data integrity, confidentiality, and overall workplace efficiency. When security measures are inadequate, secretaries may fall victim to cyber threats, unauthorized access, and data breaches, leading to disruptions in workflow, loss of critical information, and legal consequences for the organization. According to Martinez (2016), some of the key security challenges secretaries face when using computer security devices in their daily task are as follows:

1. **Complexity of Security Devices:** Modern security systems such as biometric scanners, encrypted drives, and multi-factor authentication tools can be complex to operate. Secretaries, who may not have a technical background, might find these devices confusing to navigate, especially when the interfaces are not user-friendly or require specific sequences to operate. This can lead to delays and errors during routine tasks.
2. **Lack of Technical Training:** Many secretaries receive limited or no formal training on how to use advanced security devices. As a result, they may struggle with troubleshooting problems, understanding error messages, or following security protocols correctly. This lack of knowledge increases dependence on IT support, reducing overall efficiency.
3. **Time Constraints**: Secretaries often manage tight schedules with multiple responsibilities. Taking extra time to deal with slow authentication processes, re-enter security codes, or reset passwords can interrupt workflow. These delays may impact important tasks such as document handling, scheduling, or communication with executives.
4. **Frequent Password Updates**: Security policies often require regular password changes for enhanced protection. Remembering multiple complex passwords or managing them securely without writing them down can be difficult. This increases the risk of lockouts or security breaches if passwords are stored improperly.
5. **Device Compatibility Issues:** Some security tools may not work seamlessly across all devices or software used in the office. For instance, a fingerprint scanner might not be supported on certain laptops or older operating systems, leading to workarounds or reliance on less secure alternatives, thereby reducing security effectiveness.
6. **Balancing Security and Convenience:** There is often a trade-off between maintaining strong security and ensuring ease of access. Overly strict security measures may hinder the secretary’s ability to perform their duties efficiently, while lenient measures may expose the organization to risks. Secretaries must constantly balance these demands while ensuring compliance with security policies.
7. **Limited Authority or Access:** Secretaries may not have the administrative privileges needed to resolve issues with security devices themselves, such as resetting access or updating permissions. This dependence on higher authorities or IT departments slows down problem resolution and hampers autonomy.
8. **Keeping Up with Updates**: Security technologies evolve rapidly, with frequent software and firmware updates to patch vulnerabilities. Secretaries may struggle to keep up with these updates or may not be informed when changes occur, leading to incompatibility issues, confusion, or security lapses due to outdated systems.

## Suggested Solutions to the Identified Problems

Some of the suggested solutions to the challenged in this project work include:

1. **Simplifying the User Experience with Security Tools:** Choose security gadgets that are simple to use and straightforward, requiring few steps to operate. Organizations should offer non-technical roles defaults or simpler user interfaces when complex technologies are required. Tooltips, on-screen instructions, and visual tutorials can all greatly lessen misunderstanding.
2. **Bridging the Skills Gap with Practical Training:** Provide frequent, position-specific technical training that focuses on the tools secretaries really use. Quick reference sheets, practical exercises, and on-demand learning materials like video lectures and frequently asked questions should all be part of this. Every time there are significant system changes, refresher training can be offered.
3. **Simplifying Processes to Save Time:** Adopt fast and efficient authentication systems such as biometric logins or single sign-on (SSO) to reduce the number of steps and time required to access tools. Allow session persistence within secure timeouts to minimize repeated logins throughout the day.
4. **Easing the Burden of Password Management:** Introduce secure password managers to help secretaries store and manage passwords efficiently. Encourage the use of passphrases instead of complex alphanumeric (alphabets + numbers) text, and wherever possible, replace frequent password changes with multi-factor authentication (MFA) for enhanced security without added stress.
5. **Ensuring Smooth Integration Across Devices:** Conduct compatibility testing before deploying new security technologies. Provide secretaries with standardized equipment known to work with security systems, or ensure that alternative secure access paths are available if primary devices are incompatible. IT support should be readily available for configuration help.
6. **Finding the Right Balance Between Safety and Usability:** Use role-based access control to ensure security policies are tailored to each employee’s responsibilities. For secretaries, this means granting enough access for their tasks while still enforcing necessary restrictions. Involve secretaries in policy feedback loops to improve the balance between protection and ease of use.
7. **Empowering Secretaries with Limited Administrative Capabilities:** Provide secretaries with limited, safe administrative capabilities, such as resetting their own passwords or updating profile information. If that’s not feasible, create a priority support channel for administrative staff so their requests are resolved promptly without long wait times.
8. **Making System Updates Understandable and Manageable:** Ensure all updates to security systems are well-communicated through clear and concise meetings. Provide summaries of changes and their impacts on daily tasks. I.T departments should maintain open communication and offer tutorial guides or office hours to help staff adjust smoothly to updates.

## Summary

This chapter explored the security challenges secretaries face in their daily tasks and their impact on workplace efficiency, conceptual framework of key terms such as impact, computer security, job performance, secretary from different scholars’ perspectives. The chapter also examined the types of security threats secretaries encounter, highlighting both cyber and physical vulnerabilities. The consequences of poor security practices, including data breaches, financial losses, and reputational damage, were discussed. Suggested solutions were presented to address these security risks, ensuring better data protection, compliance with legal regulations, and overall workplace security.

## CHAPTER THREE

## METHODOLOGY

## 3.1 Research Methodology

This chapter deals with the methodology approach and various strategies employed in the research such as research design, population of the study, sample population, instrumentation, validity, method of data collection, method of data analysis and decision rule.

## 3.2 Research Design

The research design to be adopted for this study is the survey design, the design is appropriate for this study because the opinions of the secretaries are required to solve the problem at hand.

## 3.3 Population

The population of the study is made up of seventy (70) secretaries in Federal Polytechnic Mubi.

## 3.4 Sample Population

The researcher will study the entire population of secretaries in Federal Polytechnic Mubi, which are seventy (70) in number because of the small size of the entire population.

## 3.5 Instrumentation

The research will use a twenty (20) item self-developed questionnaire titled “**Impact of Computer Security Devices on the Job Performance of Modern Secretary in Federal Polytechnic Mubi**” in order to elicit information from the respondents.

## 3.6 Validity of the Instrument

To ensure the validity of the instrument, questionnaire will be given out to the supervisor and three other professionals for face and content validity.

## 3.7 Method of Data Collection

The method of data collection that will be employed by the researcher will be primary and secondary data. The primary sources of data include the questionnaire while the secondary sources of data include text books, journals and articles.

## 3.8 Method of Data Analysis

The researcher will use mean and standard deviation to analyze the data obtained, using a 5-point likert type scale to analyze the questions to which values were assigned. The formular for calculating the mean and standard deviation is as follows:

The Formula for calculating **mean** is as follows:

Where:

X = Nominal/Assigned Values

F = frequency

N = Number of respondents

The formula for **standard deviation** is as follows:

Where:

σ = Standard Deviation

√ = Square root

∑ = Summation

X = Number of respondents for scale response

N = Number of respondents

## 3.9 Decision Rule

The following decision rules will be adopted for this research, any mean score of 3.5 to 5.0 will be accepted as having an influence on the problem at hand, while mean score between 1.0 to 3.49 will be regarded as unacceptable and not having any effect on the problem at hand.

Whereas for standard deviation, any calculated standard deviation that falls within the range of 2.5 to 3.8 will be accepted as normal distribution.

## CHAPTER FOUR

## PRESENTATION, ANALYSIS AND INTERPRETATION

## 4.1 Summary of Questionnaire Distributed

A total number of seventy (70) questionnaires were distributed to the respondents, (The Secretaries in Federal Polytechnic, Mubi). Seventy (70) were returned, representing 100% returned.

## 4.2 Answering Research Questions

Questions formulated for this research was answered using simple mean statistical tool and standard deviation of analyzing data because of the descriptive nature of the research. However, from the decision rule it could be recast that any mean that falls within 3.5 and above is accepted while any mean that falls below 3.5 could be regarded as rejected.

**RESEARCH QUESTION ONE: WHAT ARE THE TYPES OF COMPUTER SECURITY DEVICES USED IN SECRETARIAL WORK**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S/N** | **STATEMENT** | SA  5 | | A  4 | UD  3 | D  2 | SD  1 | N | ∑F |  | σ | Remarks |
| **1** | Secure Password Management Tools (S.P.M.T) are computer security tools used by secretaries in aiding to manage multiple accounts. | | 49 | 19 | 2 | 0 | 0 | 70 | 327 | 4.7 | 0.016 | Agreed |
| **2** | Data Backup Solutions are used by secretaries to handle critical business documents, reports, and schedules such as external hard drives or cloud storage. | | 50 | 19 | 0 | 1 | 0 | 70 | 328 | 4.7 | 0.016 | Agreed |
| **3** | Secretaries receive and send a high volume of emails; they are often targeted by malware attacks. Email security filters automatically detect and block malicious emails for example Proof point Email Protection. | | 44 | 24 | 2 | 0 | 0 | 70 | 322 | 4.6 | 0.015 | Agreed |
| **4** | Encryption and cybersecurity software is a security device used by secretaries to work with sensitive corporate data like financial records, contracts and confidential emails. | | 43 | 23 | 2 | 2 | 0 | 70 | 317 | 4.6 | 0.016 | Agreed |
| **5** | Universal Serial Bus (U.S.B) Blocker Data Protection Devices are security device used by secretaries to secure files transferred via USB, an example is a USB Port Lock (with key) which is a small insert plugged into the USB port and requires a special key to remove. | | 40 | 25 | 3 | 2 | 0 | 70 | 313 | 4.5 | 0.015 | Agreed |

**Source: Field survey (2025) Av Mean = () = () = 4.6 and Av S.D = (**σ**) = = 0.0156**

Variable one from the above table stated that the respondents agreed with a mean score of 4.7 which indicates that Secure Password Management Tools (S.P.M.T) are computer security device used by secretaries in aiding to manage multiple accounts. Variable two with a mean score of 4.7 indicates that Data Backup Solutions are used by secretaries to handle critical business documents, reports, and schedules such as external hard drives or cloud storage. Variable three with a mean score of 4.6 shows that email security filter tools is a security device used by secretaries to securely handle large volume of emails. Variable four with a mean score of 4.6 shows that the respondents agreed that encryption and cybersecurity software is a security tool used by secretaries to work with sensitive corporate data like financial records, contracts and confidential emails. Finally variable five with a mean score of 4.6 shows that Universal Serial Bus (U.S.B) Blocker Data Protection Devices are security device used by secretaries to secure files transferred via USB.

Based on the evaluations made by the respondents, this researcher agrees that the above mentioned are the types of computer security devices used by the secretary in carrying out office duties.

**RESEARCH QUESTION TWO: WHAT ARE THE IMPORTANCE OF COMPUTER SECURITY DEVICES ON THE JOB PERFORMANCE OF THE SECRETARY**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S/N** | **STATEMENT** | SA  5 | A  4 | UD  3 | D  2 | SD  1 | N | ∑F |  | σ | Remarks |
| **1** | Computer Security devices/tools such as encryption software and biometric authentication prevent unauthorized access to confidential files, ensuring that sensitive information remains protected. | 40 | 28 | 2 | 0 | 0 | 70 | 318 | 4.6 | 0.016 | Agreed |
| **2** | Firewalls, antivirus software, and network access control systems help prevent malware attacks, hacking attempts, and phishing scams. | 50 | 19 | 0 | 1 | 0 | 70 | 328 | 4.7 | 0.016 | Agreed |
| **3** | A secure computing environment minimizes disruptions caused by security breaches or system failures. | 40 | 28 | 2 | 0 | 0 | 70 | 318 | 4.6 | 0.016 | Agreed |
| **4** | Computer security devices improve accuracy and reduces errors, unauthorized access or data tampering can lead to errors, security measures such as access control ensure that only authorized personnel can modify or access critical information, leading to greater accuracy in secretarial tasks. | 35 | 31 | 2 | 2 | 0 | 70 | 309 | 4.5 | 0.015 | Agreed |
| **5** | Working with secured systems allows the secretary to perform duties without fear of security breaches or data theft. | 40 | 25 | 3 | 2 | 0 | 70 | 313 | 4.5 | 0.015 | Agreed |

**Source: Field survey (2025) Av Mean = () = () = 4.6 and Av S.D = (**σ**) = = 0.0156**

Variable one from the above table stated that the respondents agreed with a mean score of 4.6 which indicates that computer security devices/tools such as encryption software and biometric authentication prevent unauthorized access to confidential files, ensuring that sensitive information remains protected. Variable two with a mean score of 4.7 indicates that firewalls, antivirus software, and network access control systems help prevent malware attacks, hacking attempts, and phishing scams.

Variable three with a mean score of 4.6 shows that a secure computing environment minimizes disruptions caused by security breaches or system failures. Variable four with a mean score of 4.5 shows that computer security devices improve accuracy and reduces errors, unauthorized access or data tampering can lead to errors, security measures such as access control ensure that only authorized personnel can modify or access critical information, leading to greater accuracy in secretarial tasks. Finally variable five with a mean score of 4.5 shows that working with secured systems allows the secretary to perform duties without fear of security breaches or data theft.

Based on the evaluations made by the respondents, the researcher agrees that the above mentioned are some of the importance of computer security devices on the job performance of the secretary, the researcher is in agreement with respondents with the average mean of 4.5.

**RESEARCH QUESTION THREE: WHAT ARE** **THE CHALLENGES FACED BY SECRETARIES WHEN USING COMPUTER SECURITY DEVICES**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S/N** | | **STATEMENT** | SA  5 | A  4 | UD  3 | D  2 | SD  1 | N | ∑F |  | σ | Remarks |
| **1** | Modern security systems such as encrypted multi-factor authentication tools can be complex to operate. Secretaries, who may not have a technical background, might find these devices confusing to navigate. | | 39 | 29 | 2 | 0 | 0 | 70 | 317 | 4.6 | 0.069 | Agreed |
| **2** | Many secretaries receive limited or no formal training on how to use advanced security devices. As a result, they may struggle with troubleshooting problems, understanding error messages, or following security protocols correctly. | | 50 | 19 | 0 | 1 | 0 | 70 | 328 | 4.7 | 0.071 | Agreed |
| **3** | Some security tools may not work easily across all devices or software used in the office. For instance, a fingerprint scanner might not be supported on certain laptops or older operating systems, leading to workarounds, thereby reducing security effectiveness. | | 51 | 17 | 2 | 0 | 0 | 70 | 329 | 4.7 | 0.071 | Agreed |
| **4** | There is often a trade-off between maintaining strong security and ensuring ease of access. Overly strict security measures may hinder the secretary’s ability to perform their duties efficiently. | | 47 | 19 | 2 | 2 | 0 | 70 | 321 | 4.6 | 0.069 | Agreed |
| **5** | Security technologies evolve rapidly, with frequent software and firmware updates to patch vulnerabilities. | | 46 | 19 | 3 | 2 | 0 | 70 | 319 | 4.6 | 0.069 | Agreed |

**Source: Field survey (2025) Av Mean = () = () = 4.6 and Av S.D = (**σ**) = = 0.0698**

Variable one from the above table stated that the respondents agreed with a mean score of 4.6 which indicates that modern security systems such as encrypted multi-factor authentication tools can be complex to operate. Secretaries, who may not have a technical background, might find these devices confusing to navigate. Variable two with a mean score of 4.7 indicates that many secretaries receive limited or no formal training on how to use advanced security devices. As a result, they may struggle with troubleshooting problems, understanding error messages, or following security protocols correctly.

Variable three with a mean score of 4.7 shows that some security tools may not work easily across all devices or software used in the office. For instance, a fingerprint scanner might not be supported on certain laptops or older operating systems, leading to workarounds, thereby reducing security effectiveness. Variable four with a mean score of 4.6 shows that there is often a trade-off between maintaining strong security and ensuring ease of access. Overly strict security measures may hinder the secretary’s ability to perform their duties efficiently. Finally variable five with a mean score of 4.6 shows that security technologies evolve rapidly, with frequent software and firmware updates to patch vulnerabilities.

Based on the evaluations made by the respondents, this researcher agrees that the above mentioned are the challenges faced by secretaries when using computer security devices. Based on the above findings, the researcher is in agreement with respondents with the average mean of 4.6.

**RESEARCH QUESTION FOUR: HOW WOULD THE IDENTIFIED PROBLEMS BE SOLVED?**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S/N** | | **STATEMENT** | SA  5 | A  4 | UD  3 | D  2 | SD  1 | N | ∑F |  | σ | Remarks |
| **1** | Choose security gadgets that are simple to use and straightforward, requiring few steps to operate. | | 40 | 28 | 2 | 0 | 0 | 70 | 318 | 4.6 | 0.016 | Agreed |
| **2** | Provide frequent, position-specific technical training that focuses on the tools secretaries really use. Quick reference sheets, practical exercises, and on-demand learning materials. | | 39 | 30 | 0 | 1 | 0 | 70 | 317 | 4.6 | 0.016 | Agreed |
| **3** | Conduct compatibility testing before deploying new security technologies. Provide secretaries with standardized equipment known to work with security systems. | | 48 | 20 | 2 | 0 | 0 | 70 | 326 | 4.7 | 0.016 | Agreed |
| **4** | Use role-based access control to ensure security policies are tailored to each employee’s responsibilities. For secretaries, this means granting enough access for their tasks while still enforcing necessary restrictions. | | 40 | 26 | 2 | 2 | 0 | 70 | 314 | 4.5 | 0.015 | Agreed |
| **5** | Ensure all updates to security systems are well-communicated through clear and concise meetings. Provide summaries of changes and their impacts on daily tasks. | | 40 | 25 | 3 | 2 | 0 | 70 | 313 | 4.5 | 0.015 | Agreed |

**Source: Field survey (2025) Av Mean = () = () = 4.6 and Av S.D = (σ) = = 0.0156**

Variable one from the above table stated that the respondents agreed with a mean score of 4.6 choosing security gadgets that are simple to use and straightforward and requires fewer steps to operate is a solution to one of the challenges faced when using computer security devices. Variable two with a mean score of 4.6 agrees that providing frequent, position-specific technical training that focuses on the tools secretaries really use is a good solution. Variable three with a mean score of 4.7 shows that organizations should conduct compatibility testing before deploying new security technologies. Variable four with a mean score of 4.5 shows that using role-based access control to ensure security policies are tailored to each employee’s responsibilities is a good way to implement the use of computer security devices. Finally variable five with a mean score of 4.5 shows that organizations should ensure all updates to security systems are well-communicated through clear and concise meetings.

Based on the evaluations made by the respondents, the researcher is in agreement with the respondents.

## 4.3 Summary of Findings

This project work focused on the **“Impact of Computer Security Devices on the Job Performance of Modern Secretaries in Federal Polytechnic Mubi.”** The study aimed to examine the types of computer security devices commonly used by secretaries, the importance of these tools on their job performance, the challenges faced while using them, and recommendations for improving data security practices. The study revealed that modern secretaries make use of various computer security devices such as Secure Password Management Tools (S.P.M.T), Data Backup Solutions, Email Security Filters, and Encryption Software to manage critical data and ensure secure communication. These tools aid in the protection of sensitive information like financial records, reports, and schedules.

Findings also showed that the use of computer security devices has significantly improved the job performance of secretaries by minimizing risks of data breaches, unauthorized access, and system disruptions. Tools like biometric authentication, firewalls, and antivirus software create a secure work environment, allowing secretaries to perform their duties efficiently.

The study also uncovered several challenges: these include weak access controls, lack of encryption for communications, and non-compliance with security regulations, which expose sensitive data to potential misuse or cyberattacks. The absence of proper training and up-to-date security practices also contributes to these vulnerabilities.

Based on the data collected and analyzed, it was concluded that implementing stricter access controls, adopting encryption across communication channels, and aligning security practices with evolving laws will enhance data protection and improve the performance and confidence of modern secretaries in their day-to-day operations

.

## CHAPTER FIVE

## SUMMARY, CONCLUSION AND RECOMMEDATIONS

## 5.1 Summary

This research work is centered on the *“***Impact of Computer Security Devices on the Job Performance of Modern Secretaries in Federal Polytechnic Mubi***.”* Some of the objectives of the study were: to identify the types of computer security devices and tools that are available to secretaries; to determine the importance of these security devices on the job performance of secretaries; to identify the challenges associated with using computer security tools; and to determine ways of solving the identified problem.

The literature review was conducted using both primary and secondary sources of data. The entire population of seventy (70) Secretaries at the Federal Polytechnic, Mubi, was used. The survey method was adopted as the most appropriate approach to gather direct opinions from respondents regarding their work environment. Data collected were analyzed using simple mean and standard deviation statistical tools. To enhance comprehension, data were presented in tables.

The major findings of the research were also presented, followed by well-thought-out recommendations intended to improve both the implementation and effectiveness of computer security devices in enhancing the job performance of modern secretaries.

## 5.2 Conclusion

This research was able to arrive at a conclusion that the organization will achieve high efficiency of work, and the performance of the modern secretary will improve dramatically, if the proper computer security devices are put in place.

There is a need for modern secretaries to possess adequate knowledge and technical know-how in operating and applying various computer security devices, such as encryption tools, secure password managers, and data backup systems, to ensure confidentiality, integrity, and availability of information.

Lack of proper security tools or poor implementation exposes the organization to risks such as data breaches, unauthorized access, and system failures, all of which affect the productivity of the secretary and the entire organization, there is a strong need for continuous training, seminars, and workshops to keep secretaries updated with current cybersecurity practices, tools, and legal requirements. This will help build a more secured, efficient, and productive office environment.

## 5.3 Recommendations

Based on the research findings and the conclusion above, the researcher made the following recommendations:

1. **Implement Role-Based Access Control Measures:** Organizations should introduce strict access controls by assigning unique login credentials to each secretary and ensuring role-based permissions. This will prevent unauthorized access and safeguard confidential information.
2. **Ensure Regular Cybersecurity Training:** Secretaries should be regularly trained on the proper use of computer security devices such as encryption software, email filters, and password managers. This training should also include awareness of common cyber threats like phishing and data breaches.
3. **Adopt End-to-End Encryption for Communication:** Offices should implement end-to-end encryption tools for emails, instant messaging platforms, and file transfers. This ensures that sensitive company information remains secured from interception by unauthorized individuals.
4. **Establish a Data Backup and Recovery Plan:** The management should invest in reliable data backup solutions to help secretaries protect essential documents, schedules, and reports. Regular backups should be automated and tested to ensure data recovery during system failure or cyber incidents.
5. **Update Security Policies and Align with Legal Standards:** Organizations must review and revise their IT security policies frequently to reflect evolving cybersecurity threats and comply with current data protection regulations. Secretaries should be briefed on these policies to ensure adherence.
6. **Provide Efficient Technical Support:** A dedicated IT support system should be available to assist secretaries in resolving security-related technical issues swiftly. This reduces work disruptions and enhances productivity.

## 5.4 Areas for Further Studies

Since this research did not cover all aspects in relation to the impact of computer security devices on the job performance of modern secretaries in Federal Polytechnic Mubi, further research could be carried out on any of the following:

1. Effectiveness of Biometric Security Systems in Preventing Unauthorized Access in Administrative Offices
2. Impact of Cybersecurity Training on Data Protection Practices among Secretarial Staff in Tertiary Institutions
3. Assessment of Encrypted Communication Tools in Safeguarding Confidential Information in Public Sector Organizations
4. Challenges of Implementing Advanced Security Protocols in Resource-Constrained Educational Institutions

**REFERENCES**

Anderson, J., & Clark, M. (2022). Cybersecurity principles and practices: A modern approach. New York, NY: TechShield Publishing.

Anderson, P. (2020). Digital Security in the Workplace: Safeguarding Administrative Efficiency. Oxford University Press.

Brown, T. (2020). The dynamics of change: Understanding impact in organizations. New York, NY: Business Press.

Carter, L., & Reynolds, M. (2011). The evolving role of the secretary in modern business operations. Chicago, IL: Administrative Insights.

Carter, R., & Lewis, J. (2019). Cybersecurity and Organizational Productivity: A Study of Digital Risk Management. Harvard Business Review.

Daniels, P. (2015). Office management and the role of the secretary: A comprehensive guide. London, UK: Professional Press.

Foster, L. (2006). Measuring workplace success: Understanding job performance and productivity. London, UK: Workforce Insights.

Harrison, P., & Bennett, T. (2022). Employee effectiveness: Strategies for enhancing job performance. New York, NY: Business Excellence Press.

Johnson, M., & White, K. (2019). The Role of Firewalls and Encryption in Data Security. Cambridge Scholars Publishing.

Johnson, R., and Williams, M. (2022). Measuring the effects: A comprehensive guide to impact assessment. London, UK: Academic Insights.

Lewis, T. (2021). Understanding digital devices: Applications and impact in modern technology. London, UK: TechSphere Publishing.

Martinez, R. (2016). *Cybersecurity risks in office administration: Identifying and addressing key challenges*. New York, NY: SecureTech Press.

Miller, S. (2018). Technology and Secretarial Efficiency: Addressing the Digital Threats. McGraw-Hill.

Miller, S., and Davis, P. (2021). Evaluating influence and transformation in modern systems. Chicago, IL: Research & Policy Publications.

Mitchell, R. (2019). *Office security essentials: Protecting sensitive information and resources*. New York, NY: SecureTech Publications.

Mitchell, R., & Carter, S. (2022). Smart devices and digital transformation: The evolution of technology. New York, NY: FutureTech Press.

Nelson, R., & Wright, D. (2020). Workplace dynamics: Examining the factors that drive job performance. Chicago, IL: Organizational Development Publications.

Patel, R. (2021). Foundations of computer security: Threats, defenses, and best practices. London, UK: CyberSafe Press.

Richardson, P., & Evans, M. (2020). The role of devices in the digital age: Connectivity, automation, and intelligence. Chicago, IL: InnovateTech Publications.

Roberts, D. (2020). Legal and Ethical Implications of Cybersecurity in Institutional Management. Routledge.

Thompson, L. (2021). The Impact of Cyber Threats on Workplace Administration. Springer.

Thompson, L., & Roberts, D. (2020). Risk management in cybersecurity: Strategies for digital protection. Chicago, IL: SecureTech Publications.

Watson, J., & Hughes, R. (2018). Secretarial excellence: Skills and strategies for administrative professionals. New York, NY: Business Support Publications.

Williams, G. (2021). Data Integrity and Security in the Modern Office: Challenges and Solutions. Wiley.