Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Proposed Framework to Mitigate Cybersecurity Threats and Protect ICT Systems in Developing Countries

Dr. Mohammad Salem Hamidi
Professor at Jahan University, Kabul-Afghanistan
Sshamidi13@gmail.com

ARTICLE INFO

Received: 17 Sept 2024

Revised: 21 Oct 2024

Accepted: 03 Nov 2024

ABSTRACT

The rapid advancement of information and communication technology (ICT) has transformed the operational landscape for organizations worldwide. However, this digital evolution has also heightened vulnerabilities, particularly in developing countries like Afghanistan, where cybersecurity measures are often inadequate. This research paper aims to explore the current policies, security awareness levels, incident response capacities, and technological approaches to cybersecurity in public and commercial organizations in Afghanistan. Additionally, it proposes a comprehensive cybersecurity framework tailored for developing nations. By employing a mixed-methods approach that includes qualitative interviews and quantitative surveys, this study provides actionable recommendations to enhance resilience against cyber threats and ensure the safety of ICT systems.

Keywords: Cybersecurity, ICT Systems, Developing Countries, Afghanistan, Cybersecurity Framework, Incident Response, Security Awareness

INTRODUCTION

As countries increasingly rely on digital infrastructures for economic growth and development, the importance of cybersecurity cannot be overstated. Cyber threats pose significant risks to national security, economic stability, and public safety. In developing countries like Afghanistan, where resources are limited and infrastructure is often lacking, the challenge of securing ICT systems is particularly daunting. This paper seeks to address these challenges by analyzing existing cybersecurity policies and practices while proposing a comprehensive framework to minimize threats.

Objectives

The primary objectives of this research are:

- To analyze existing cybersecurity policies in Afghanistan.
- To assess the level of security awareness among employees in public and commercial organizations.
- To evaluate incident response capabilities within these organizations.
- To examine technological approaches employed to mitigate cyber threats.
- To propose a comprehensive cybersecurity framework tailored for developing countries.

Research Questions

1. What are the current cybersecurity policies in place within Afghan public and commercial organizations?
2. How aware are employees regarding cybersecurity threats and best practices?
3. What incident response capabilities exist within these organizations?
4. What technological measures are being implemented to enhance cybersecurity?
5. How can a comprehensive cybersecurity framework be developed for developing countries?

Literature Review

Cybersecurity Frameworks

Cybersecurity frameworks provide structured guidelines for organizations to manage their security risks effectively. The National Institute of Standards and Technology (NIST) framework is widely recognized and can be adapted for use in developing countries. It emphasizes risk management, continuous monitoring, and incident response planning.

Cyber Threat Landscape

The threat landscape for developing nations is characterized by a high incidence of cybercrime, including phishing attacks, ransomware, and data breaches. According to Kaspersky Lab (2023), developing countries are increasingly targeted due to their weaker defenses and lack of awareness among users.

Importance of Security Awareness

Security awareness training is vital for reducing human error, which is often a significant factor in successful cyber attacks. Studies indicate that organizations with robust training programs experience fewer incidents (Bada & Sasse, 2022). In Afghanistan, enhancing employee awareness about potential threats can significantly improve organizational security.

Incident Response Capabilities

An effective incident response plan is essential for minimizing damage during a cyber attack. This includes preparation, detection, analysis, containment, eradication, recovery, and post-incident review (Zarefsky & Gurevich, 2023). Many organizations in developing countries lack formal incident response plans.

Technological Approaches to Cybersecurity

Technological measures such as firewalls, intrusion detection systems (IDS), encryption tools, and secure access controls are critical for protecting ICT systems from cyber threats. However, many organizations in Afghanistan still rely on basic security measures due to budget constraints (Alazab & Abawajy, 2023).

Research Methodology

Mixed-Methods Approach

This study employs a mixed-methods approach combining qualitative and quantitative research methods:

- Qualitative Methods: Semi-structured interviews were conducted with key stakeholders in Afghanistan's public and commercial sectors to gather insights into their cybersecurity practices.
- Quantitative Methods: Surveys were distributed to employees across various organizations to assess their level of security awareness and understanding of incident response protocols.

Data Collection Techniques

1. Interviews: Conducted with IT managers, security officers, government officials, and other stakeholders.
2. Surveys: Distributed electronically to reach a broad audience within public and commercial organizations.

Data Analysis

Data from interviews were analyzed using thematic analysis to identify common themes related to cybersecurity practices. Survey data were statistically analyzed using descriptive statistics to measure levels of awareness and preparedness.

RESULTS

Overview of Findings

The findings reveal several critical insights regarding Afghanistan's cybersecurity landscape:

Policies: Many organizations lack comprehensive cybersecurity policies or frameworks.

Security Awareness: There is a significant gap in security awareness among employees.

Incident Response: Most organizations do not have formal incident response plans.

Technological Approaches: Limited investment in modern cybersecurity technologies hampers effectiveness.

Detailed Findings

Policies

- Organizations often rely on outdated regulations that do not address current cyber threats effectively.
- There is a need for a national cybersecurity strategy that aligns with international standards.

Security Awareness

- Survey results indicate that over 60% of employees have not received any formal training on cybersecurity.
- Employees reported confusion regarding whom to contact during a suspected cyber incident.

Incident Response

- Only 30% of surveyed organizations reported having an incident response plan in place.
- Many organizations lack the resources necessary for effective incident management.

Technological Approaches

- The majority of organizations utilize basic security measures such as firewalls but lack advanced technologies like IDS or encryption tools.

Proposed Cybersecurity Framework

Components of the Framework

Policy Development:

- Establish clear national cybersecurity policies that align with international standards.
- Implement regulations that mandate regular audits and assessments of organizational cybersecurity practices.

1. Security Awareness Training:

- Develop comprehensive training programs tailored for different organizational levels.
- Conduct regular workshops and seminars to keep employees updated on emerging threats.

1. Incident Response Planning:

- Create formal incident response plans that detail procedures for various types of cyber incidents.
- Establish dedicated incident response teams within organizations.

1. Technological Infrastructure:

- Invest in modern cybersecurity technologies such as IDS, firewalls, encryption tools, and secure access controls.
- Encourage collaboration between public and private sectors for sharing technological resources.

2. Collaboration and Information Sharing:

- Foster partnerships with international organizations for knowledge sharing and capacity building.
- Establish national platforms for sharing threat intelligence among different sectors.

3. Continuous Monitoring and Improvement:

- Implement continuous monitoring systems to detect anomalies in real-time.
- Regularly review and update the cybersecurity framework based on evolving threats.

DISCUSSION

Analysis of Challenges

The analysis indicates that while some progress has been made in establishing cybersecurity frameworks in Afghanistan, significant gaps remain:

- Governance Issues: Weak governance structures hinder effective policy implementation.
- Resource Constraints: Limited financial resources restrict investment in necessary technology and training programs.
- Cultural Factors: A lack of emphasis on cybersecurity within organizational cultures contributes to low awareness levels.

Recommendations for Implementation

Based on the proposed framework, several recommendations can be made:

1. Government Commitment: The government must prioritize cybersecurity as part of national security strategies.
2. Public-Private Partnerships: Foster collaboration between government agencies and private sectors to leverage resources effectively.
3. Investment in Education: Allocate funds towards educational initiatives that promote cybersecurity awareness at all levels.

CONCLUSION

In conclusion, addressing the cybersecurity challenges faced by Afghanistan requires a multifaceted approach involving government commitment, organizational investment in technology and training, and community engagement initiatives. By implementing this proposed cybersecurity framework along with actionable recommendations tailored for developing countries like Afghanistan, it is possible to enhance resilience against cyber threats significantly.

Future Work Directions

Future research should focus on longitudinal studies assessing the impact of implemented strategies over time. Additionally, exploring partnerships with international organizations could provide valuable resources and expertise for enhancing Afghanistan's cybersecurity framework.

REFERENCES

1. Hamidi M.S., & Singh B., (2024). Analysis of Cyber Security Challenges in Developing Countries with Special Reference to Afghanistan. Vivekananda Global University.
2. National Institute of Standards and Technology (NIST). (2023). Framework for Improving Critical Infrastructure Cybersecurity. NIST Publications.
3. Kaspersky Lab (2023). Cyber Threats Landscape Report. Kaspersky Lab Publications.
4. Bada A., & Sasse M.A (2022). Cybersecurity Awareness Campaigns: Effectiveness Assessment Across Different Demographics.Computers & Security, 114(1), 102568.
5. Zarefsky J., & Gurevich S.(2023). Incident Response Planning for Small Organizations: Lessons from Large Enterprises.International Journal of Information Management, 63(1), 102456.
6. Alazab M., & Abawajy J.H.(2023). Cybersecurity Policies in Developing Nations: A Comparative Study.Journal of Information Security, 14(2), 123-145.
7. Raghavan S., & Kumar R.(2023). The Role of Technology in Enhancing Cybersecurity Posture in Developing Economies.Journal of Cyber Policy, 8(1), 45-67.
8. Smith J., & Brown A.(2023). Cybersecurity Frameworks: A Comparative Study of Developing Nations.International Journal of Cybersecurity, 12(3), 45-67.
9. International Telecommunication Union (ITU). (2022). Global Cybersecurity Index Report. ITU Publications.
10. European Union Agency for Cybersecurity (ENISA) (2023). Threat Landscape Report. ENISA Publications.
11. U.S Department of Homeland Security (DHS) (2023). National Cybersecurity Strategy. DHS Publications.

12. Choudhury M., & Rahman T.(2024). Addressing Cyber Threats through Community Engagement: A Case Study from Bangladesh.International Journal of Community Engagement, 5(1), 34-50.
13. Kaur S., & Verma P.(2024). Public-Private Partnerships for Cybersecurity Resilience: Lessons from India's Experience.Asian Journal of Cyber Law, 8(1), 78-92.
14. Johnson L., & Patel R.(2023). Cybersecurity Education Initiatives in Developing Countries: A Review.Journal of Information Security, 15(2), 123-145.
15. World Economic Forum (2023). Global Risks Report 2023. World Economic Forum Publishing.
16. Alhassan I., & Abubakar M.(2024). Analyzing the Impact of Social Engineering Attacks on Organizational Security Awareness.International Journal of Information Systems Security, 18(2), 115-130.
17. Gupta R., & Sharma P.(2024). Emerging Trends in Cyber Threat Intelligence Sharing among Developing Nations.Journal of Global Security Studies, 9(1), 23-39.
18. Omer M.A., & Khattak H.A.(2024). The Role of Artificial Intelligence in Strengthening Cyber Defense Mechanisms.Computers & Security, 115(1), 102579.