Evaluating Cyber Security Practices and Awareness: Insights from DFAR Staff Survey

Abstract

In an era where cyber threats are pervasive, understanding the attitudes and practices of employees toward cyber security is critical. This study investigates the cyber security practices, awareness, and concerns of staff at the Department of Fisheries and Aquatic Resources (DFAR). Based on responses from 118 participants, the study examines demographic influences, IT system usage, security awareness, and perceived challenges. Findings reveal significant gaps in training, emphasize the importance of user-friendly IT systems, and highlight key areas for improvement, including increased public awareness and enhanced legal frameworks. Recommendations are provided to foster a secure digital working environment, ensuring both operational efficiency and data integrity.

1.0 Introduction

The rapid digitization of organizational workflows has made cyber security an integral component of modern governance and business operations. Government institutions like the DFAR, which handle sensitive information, face unique challenges in balancing efficiency with security. As cyber threats become more sophisticated, the human factor—comprising employee awareness, practices, and training—plays a pivotal role in mitigating risks.

This study aims to evaluate the cyber security landscape within DFAR through a comprehensive survey of its employees. By examining their practices, perceptions, and recommendations, this research seeks to identify key areas for intervention and improvement.

2.0 Methods

The study employed a structured questionnaire distributed among 118 employees at DFAR. The survey comprised 25 questions, including multiple-choice and open-ended formats. Topics ranged from demographic information to specific cyber security practices, IT system usage, and perceived challenges. Data were collected over a defined period, ensuring anonymity and voluntary participation.

Data analysis focused on identifying trends, correlations, and areas of concern. Responses were categorized and analyzed quantitatively, supplemented by qualitative insights from open-ended questions.

3.0 Results

3.1. Demographics

The respondent pool included participants across various age groups, with 42% aged 20–34, 38% aged 35–44, and the remainder distributed among older categories. Gender representation was relatively balanced, with 52% male and 48% female participants. Educational qualifications varied, with 48% holding bachelor's degrees, 30% master's degrees, and 12% PhDs. Most respondents were employed in non-executive roles, while 15% held executive positions.

3.2. IT Systems Usage

Employees reported regular use of multiple devices for online activities, with smartphones (85%) and laptops (70%) being the most common. IT integration in daily tasks was high, with 60% indicating that over 50% of their work depended on IT systems. However, only 45% found these systems user-friendly, citing challenges such as complex interfaces and inadequate support.

3.3. Cyber Security Awareness

Password Practices: While 80% of respondents used unique passwords for different accounts, only 50% updated their passwords regularly.

Personal Information Protection: Common measures included enabling two-factor authentication (65%) and avoiding public Wi-Fi for sensitive transactions (70%).

Victimization Rates: Approximately 20% reported being victims of cyber security breaches, primarily through phishing scams or malware attacks.

Training Adequacy: Only 40% felt that IT training at DFAR was sufficient, highlighting a need for more frequent and comprehensive programs.

3.4. Cyber Security Concerns

Top concerns included data breaches (45%), phishing scams (30%), and privacy issues (20%). Respondents emphasized the increasing sophistication of cyber threats and the need for proactive measures.

3.5. Suggestions for Improvement

- Participants proposed several improvements:
- Increasing public awareness through campaigns and workshops (50%).

- Strengthening legal frameworks and enforcement (40%).
- Enhancing IT system user-friendliness and support infrastructure (30%).

4.0 Discussion

The findings reveal a multifaceted challenge in addressing cyber security within DFAR. While IT systems are integral to daily operations, user experiences suggest a need for greater attention to usability and support. Training programs must evolve to address not only technical aspects but also behavioral changes, such as recognizing phishing attempts and practicing secure online behavior. The relatively high proportion of employees victimized by cyber breaches underscores the urgency of strengthening organizational defenses. This includes both technological safeguards and fostering a culture of vigilance among employees.

Policy Implications

- Drawing from international best practices, DFAR could adopt a multi-pronged approach:
- Comprehensive Training Programs: Regular workshops focusing on emerging threats, safe practices, and system updates.
- Public-Private Partnerships: Collaborations with tech companies and universities to stay ahead of cyber threats.
- Enhanced Legal Frameworks: Advocacy for robust cyber laws to deter malicious activities.

5.0 Conclusion

This study highlights critical gaps and opportunities in cyber security practices at DFAR. By addressing these areas through targeted interventions, the organization can build a resilient digital environment, ensuring both efficiency and security. Future research could expand this survey to other government institutions, fostering a broader understanding of cyber security dynamics in the public sector.