IT Protection and Security: MIT 264
Alden A. Quiñones
Activity 10 : Security Awareness Program

Scenario:

The Department of Social Welfare and Development Field Office XII currently has no cybersecurity training program for staff. Given the sensitive nature of the data we handle including personal information of beneficiaries .it is critical to introduce a structured cybersecurity training program.

Proposed 4 Core Topics for the Training Program:

1. **Data Privacy and Confidentiality** - Staff must have a deep understanding of the importance of protecting personal information, in compliance with the Data Privacy Act of 2012 (RA 10173). The training will cover the correct ways to collect, handle, store, and share sensitive data. It will also emphasize the rights of data subjects and the legal responsibilities of personnel, ensuring that employees recognize that negligence or mishandling of data can have serious legal and ethical consequences for both individuals and the agency.

2. **Phishing and Social Engineering** - One of the most common threats to any organization is phishing and social engineering attacks. The training will focus on how to recognize suspicious emails, fake websites, fraudulent calls, and text messages designed to deceive employees into giving away confidential information. Real-world examples will be presented, particularly incidents involving government agencies, to make the training relatable.

3. **Safe Internet and Email Use** - Safe practices when browsing the internet and using email are crucial to maintaining organizational security. This training topic will include guidance on creating strong passwords, identifying suspicious links and attachments, and avoiding risky online behavior. Staff will also learn about the importance of using secure networks, VPNs, and regularly updating software to protect against vulnerabilities.

4. **Physical Security Practices** - Cybersecurity is not only digital; physical protection of devices and sensitive materials is equally important. Training under this topic will teach staff how to secure laptops, mobile phones, flash drives, and other equipment, especially when working off-site or during fieldwork. It will also cover best practices in managing physical documents that contain sensitive information, such as proper storage and disposal.

Training Frequency Proposal:

The proposed training program should be mandatory for all newly hired employees within their first month of employment. To ensure that cybersecurity knowledge remains current, refresher training should be conducted every six months. Additionally, immediate briefings must be held if there are major changes in cybersecurity policies or when new threats emerge. Finally, an annual Cybersecurity Awareness Month should be celebrated through interactive activities such as workshops, webinars, and knowledge competitions to strengthen a culture of security across the organization.