



ASSESSMENT OF INFORMATION SECURITY AWARENESS IN HEALTHCARE BY SOCIAL ENGINEERING EXERCISE

Giunn Wu^{1,2}, Chia-Mei Chen¹, Zheng-Xun Cai¹,
Wang-Chuan Juang^{1,2,3}

1. Dept. of Information Management, National Sun Yat-sen University

2. Division of Information Management, Kaohsiung Veterans General Hospital

3. Quality Management Center, Kaohsiung Veterans General Hospital



INTRODUCTION

- As cyberattacks continue to grow, the healthcare sector has continued to react to cybersecurity concerns that **threaten patient safety and privacy**.
- Many cyber incidents in the healthcare sector have compromised technical defense mechanisms by applying **social engineering (SE)** tactics that exploit human vulnerabilities.

AIM

- Humans** represent the **weakest** link in cybersecurity chains. Research showed that human error is involved in more than **90% of security breaches**.
- This study aims to investigate employees' information security awareness (ISA) to appropriately recognize social engineering attacks in healthcare institutions.

METHOD

A long-term **social engineering exercise** is implemented to observe employees' responses to mock attacks and to evaluate **the effectiveness of such a risk reduction scheme**.

- Send out a mock SE attack **monthly** to all employees.
- The **date and time** of sending mock SE mails to given employees are **selected randomly**.
- The **contents and subjects** of the mock mails are **different** each month.

We conducted such simulated SE attacks continuously **from 2019/01 to 2022/05**.

RESULTS

- This study assesses the workforce's ISA and identifies the vulnerable workforce with a susceptible likelihood of social engineering attacks.
- The analysis implies that **the job type influences the workforce's awareness**. The table below implies that a portion of employees contribute multiple violations over the 40-month exercise. The number of violated **RD employees** is larger than the total staff number as most RD staff are **contract-based research assistants**. Furthermore, they are likely prone to view mock SE emails as their primary duty is to **explore and research diversified information from the web**.
- The **IT and Accounting & Statistics** types have the **least VRs** as their job duties train them to be **precaution and preserve**. Even though IT staff possess higher ISA sense, a **portion (22.5%) of the IT staff** still are **vulnerable to SE attacks**.
- 50% of the staff in the hospital belong to the **Medical Staff** type and 38% are **nurses**. Therefore, the behaviors of **these two job types represent most of the hospital's behaviors**. Overall, the evaluation indicates that an **employee's job type** may affect his/her SE violation rate and that **some job types tend to be SE-prone and some are not**.

Job type	Violations	# of violated employees	# of employees	Violations Rate
Research Design	226	148	108	2.0926
Administration	261	149	272	0.9596
Nursing	1,259	700	1,449	0.8689
Medical Staff	1,545	905	1,891	0.8170
MIS	30	18	80	0.3750
Accounting & Statistics	4	1	19	0.2105
Total	3,325	1,921	3,819	0.8706

CONCLUSIONS

- This study helps healthcare organizations **gain insight into the workforce's ISA** of social engineering attacks and **guides them to adopt appropriate security remedies** to improve the situation.
- The implemented **SE exercise mimics the attack procedure** applied by professional hacker groups. By sending SE emails persistently, the workforce might be tricked by one of the emails. This also explains why **social engineering** tactics are the **most common and effective attack techniques** adopted by threat actors.
- The workforce's ISA is the first line of defense**. A regular and long-term SE exercise is **effective to raise the workforce's ISA but cannot eliminate SE threats**. Organizations could instill a culture of security awareness to better handle evolving cyber threats. Our analysis suggests that **multiple risk mitigation schemes** should be implemented to reduce cyber risk. Furthermore, as cyberattacks keep changing by applying diversified vulnerabilities, **mitigation schemes should be adaptive accordingly**.

REFERENCES

- Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, 8(1), 1-24.
- ENISA. (2018). Cyber Security Culture in organizations. Retrieved from <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations>
- MIMECAST. (2022). The Awareness Training Kit. Retrieved from <https://info.mimecast.com/security-awareness-training-kit-ppc.html>