**Paper Title**

*Mohd Syahrul Hashim1,Mohd Syahrul Hashim2*

*1Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia*

*2 Faculty of Computer Science, Universiti Malaya*

1syahrul@utm.my;2Hanis@um.edu.my

**Abstract** – *There is a need for research on front-line employees in management control systems*

# *Keywords: information management, information security, etc…*

**1. Introduction**

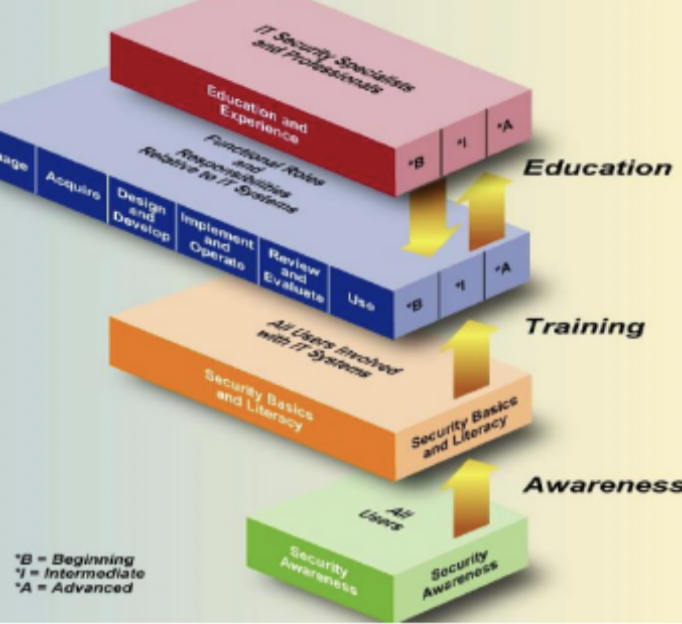
As we live in a technologically advanced era, a broad range of threats,including identity theft, phishing, and data leakage, are constantly evolving (Ramalingam and Raja, 2014). Attackers use stealthy and sophisticated tactics to gain access to sensitive information by exploiting victims confidence. They also use techniques that expose the victim’s or organization’s vulnerabilities. The study found out that the most significant factor that is affecting an organization’s information assets and information security is the gap between expertise and security practice. Sensitive and confidential information such as employees’ data and top-secret documents, including the organization’s information assets, are valuable and need to be protected from any cybercriminal attack. These information assets are generally more vulnerable to data breaches and other possible cyber threats (Richard et al., 2019).

This paper is organized as follows

…

**2. Information Security**

Today, it is common for businesses and individuals to use computers and the world to use the Internet to communicate with each other. However, the issue of information security is growing in importance. For the average person, information security is dealing with machines without fear of getting a virus, reading e-free e- mails, doing business without the worry of credit card numbers being compromised, or using Instant Message apps without fear of anyone be monitoring their communication. The information protection protects information, programs, and hardware that store and distributes information, as defined in the previous description (Perrig et al., 2004).



**Figure 1 : Awareness, Training and Education (NIST, 2003)**

**3. Methodology**

**Table 1 : Related Work**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Number** | **Name** | **Findings** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**4. Conclusion**

**Acknowledgement**

**References**

Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, *47*(6), 53-57.

Pathan, Al-Sakib Khan, Hyung-Woo Lee, and Choong Seon Hong. "Security in wireless sensor networks: issues and challenges." In *2006 8th International Conference Advanced Communication Technology*, vol. 2, pp. 6-pp. IEEE, 2006.

Giruka, V. C., Singhal, M., Royalty, J., & Varanasi, S. (2008). Security in wireless sensor networks. *Wireless communications and mobile computing*, *8*(1), 1-24.

.