# Chapter 11
# Cybersecurity Governance on Social Engineering Awareness

**Vasaki Ponnusamy**
*Universiti Tunku Abdul Rahman, Malaysia*

**Leslie Mark Pannir Selvam**
*Universiti Tunku Abdul Rahman, Malaysia*

**Khalid Rafique**
*Azad Jammu and Kashmir Information Technology Board, Pakistan*

## ABSTRACT

*Raising awareness on social engineering is becoming more essential. When we are connected to the internet, we are at the risk of becoming victims of numerous attacks. It is very difficult to protect ourselves from all of these threats, but the least we could do is not jeopardize our own safety. In order to achieve this, the need to have substantial knowledge on social engineering techniques and how to safeguard one from being victimized are mandatory. This research presents the overview of social engineering attacks. This plays a crucial role in supporting victims of cyber assaults.*

## INTRODUCTION

Security threats, when users surf the internet is growing exponentially. Vulnerabilities that are present in the internet can be exploited by skilled hackers or performing well-crafted social engineering techniques. Breach in cyber security has had massive repercussions in the past in terms of business, liability, reputation staining, customer confidence and productivity (Bradshaw, 2015). Such catastrophic consequences have led to governments and corporations to invest in many resources to build a secured cyberspace thus protecting themselves as well as their users. In terms of social engineering, these resources in training has to be poured unto the employees of the organization especially key personnel as they may poses some vital information of an organization. Leaking of such information can be detrimental for the particular organization in question. Therefore, people with such sensitive information, has to be well versed of

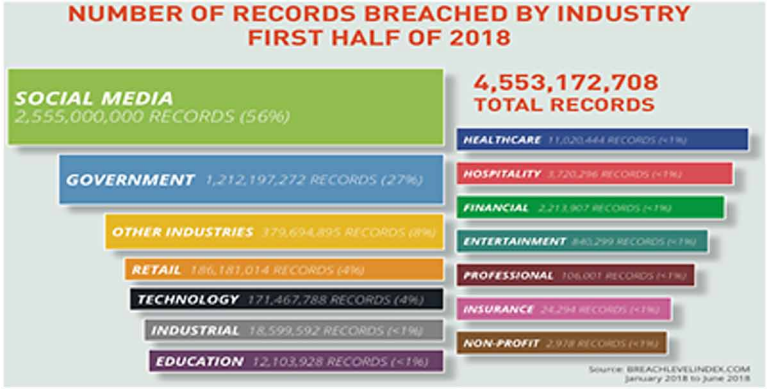
DOI: 10.4018/978-1-7998-1851-9.ch011

the risks they may be of being victims of social engineering as well as other cyber threats. Understanding these risks and knowing how to protect themselves from such scenarios may save an organization secrets. Orhan Sari and Karyda (2017) found that in the first half of 2018, over more than 4.5 billion of records have been breached. Based on Figure 1, most of the breaches (about 56%) occurs in the social media platforms due to the overwhelming usage and also the sophistication of social media attacks. So Orhan Sari and Karyda (2017) stated that these data breaches mostly happen due to human factor and lack of security practices. In addition to that, employees should possess a distinct and clear mind set in order to be able to distinguish potential threats from legitimate contents and their source of originality (Karyda, 2017). Immature perception of employees may lead to massive breaches within the organization (Karlsson et al.,2013). It has to be said that despite stern efforts up to this point, it is quite eminent that knowledge on cyber security still lacks competence. That is the reason why basic security breaches using simple social engineering techniques are still happening to this very date. Adequate knowledge regarding this problem would have seen some improvements of late. However, evidence collected up to this point suggests otherwise. All these factors reflect on how important it is to foster cybersecurity governance in organizations and on social engineering threats.

## Problem Statement

Ever since the emergence of social engineering, about 272 criminal cases using social engineering attacks are reported from January to September 2017 in Malaysia (Yuen, 2017). People are becoming aware of social engineering attacks but the actual technique of social engineering attacks to get confidential data are still unknown. As seen in Figure 2, social engineering is the second common attack after malware attacks. The attackers exploit human vulnerabilities to take advantage from the victims. The major problem why people are easily falling into the trap of social engineering is due to lack of education on the various types of social engineering attacks as well as the techniques the attackers are using. Social engineering comes in diverse form of reaching the target victims and also purposes. The easier the people's emotion get manipulated, the higher the chances of falling into social engineering attacks. Majority of the social engineering victims are the elderly because the elderly community is less familiar with the technology knowledge. Another problem of social engineering that exists in the society is the oversharing of per-

*Figure 1. Number of records breached by industry first half of 2018*
*source: Karyda (2017)*



Identifying Factors of Integration for an Interoperable Government Portal: A Study in Indian Context
Rakhi P. Tripathi, M. P. Guptaand Jaijit Bhattacharya (2011). *International Journal of Electronic Government Research (pp. 64-88).*
www.irma-international.org/article/identifying-factors-integration-interoperable-government/50293