The Importance of the Human–Centric Approach in Combating Cyber Threats

5

Pamela Goh
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Loo Seng Neo
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Xingyu Chen
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

INTRODUCTION

Concerns in the area of cybersecurity have recently been placed under the spotlight, particularly so when 2017 saw a substantial number of cyberattacks and security breaches across the world (Graham, 2017; Leech, 2017). The disruption and costs associated with cyber threats are also increasing exponentially over time, and have rendered such threats as one of the major concerns for many developed countries (Drzik, 2018; World Economic Forum, 2018).

When successful, the consequences of cyberattacks can be profound and manifold. At the individual level, for instance, confidential and sensitive data can be compromised, financial losses can occur, and essential operations can be disrupted (Accenture & Ponemon Institute LLC, 2017; Tham, 2017a). On the wider macro level, the malicious access into computer and network systems can compromise and cause the collapse of "critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population" (Lewis, 2002, p. 1). With the detrimental effects of cyberattacks, it is vital that these cyber threats are managed effectively, for which the present chapter will serve to shed light on the weakest player in the maintenance of cybersecurity – humans.

UNDERSTANDING THE WEAKEST LINK IN CYBERATTACKS: HUMAN BEHAVIOURS

Cyberattacks can be perpetuated via two means: (1) system-centric approach, where perpetrators exploit the technical vulnerabilities of a computer or network system to conduct an attack, and (2) user-centric approach, where negligence or mistakes of the computer users facilitated the execution of cyberattacks (Neupane, Rahman, Saxena, & Hirshfield, 2015). However, successful cyberattacks in reality are often a result of the latter, in which human errors rather than technological shortcomings are the main cause of concern (Kelly, 2017; Tasman-Jones, 2016). According to Symantec, 97 percent of malware attacks in 2016 targeted people and their poor online behaviours, with only the remaining three percent attributed to actual flaws in the network security system itself (Bennett, 2017).

DOI: 10.4018/978-1-5225-9715-5.ch065

Also known as social engineering, perpetrators commonly employ the method of "hacking humans" – rather than the system – by exploiting poor cyber behaviours to gain a backdoor in computer systems and networks (Choo et al., 2016). It encompasses deceiving and psychologically manipulating the victims into divulging confidential information, and/or getting them to perform certain actions that facilitate the execution of cyberattacks. For instance, the social engineering technique of "phishing" works because of the meticulously-crafted email messages that encourage recipients to click on the weblinks or download attachments that are malicious in nature (Lord, 2017; Tham 2017). In 2017, many ransomware attacks targeted at organisations had been caused by successful phishing attempts on unanticipating and careless employees, mainly through their emails or media (Jay, 2018).

Should one exercise caution, such phishing attempts may be avoided as poor human behaviour in the cyberspace forms the core of why many such cyberattacks are successful in the first place (Bennett, 2017; Fallows, 2011; Hadlington, 2017). As what Andy Waterhouse, EMEA Director at RSA Security (cited in Bennett, 2017, p. 12) had commented,

It is not just about silly errors but often a lack of training and understanding of the implications of clicking on a malicious link, going to a risky website or even setting up a service on a public cloud service without looking at the security implications.

The endeavour to combat one's susceptibility to cyberattacks involve a long process of understanding the specific attributions that contribute to this susceptibility, as well as the necessary follow-up actions needed to be done to manage the threats. Approaches to mitigate the cyberattacks therefore goes beyond the protective capabilities of sophisticated technological solutions (Conteh & Schmick, 2016; Goldman, 2013), such as antivirus software and firewalls, and have to include human-centric measures.

UNDERSTANDING HUMAN-CENTRIC MEASURES

Importance of Good Cyber Hygiene to Manage Cyber Threats

Perpetrators are constantly searching for the weakest link in the computer or network system, in order to gain quick and easy but unauthorised access into these areas (Ashiq, 2015). Humans are unfortunately very much the weakest link in cybersecurity, because of their risky behaviours in the cyberspace (Vishwanath, 2016). A 2017 survey conducted by the Cyber Security Agency of Singapore (CSA), for instance, revealed that many people exhibit poor behaviours (e.g., using the same password for both personal and work accounts, not using two-factor authentication, not installing security on mobile phones, not running virus checks for files and devices before opening them) on online platforms that put themselves and their organisations at risk of cyberattacks (CSA, 2017b).

If poor human cyber behaviours are indeed the main cause of successful cyberattacks, then managing these behaviours should reduce one's vulnerability towards cyberattacks. To do so, there is a need to reduce risky online behaviours as well as improve one's cyber hygiene behaviours.