RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 153 – 2 August 2019

Cyber Security: Beware the Human Factor

By Edwin Hooi

SYNOPSIS

The recent major data security breaches reported in Singapore's public sector over the period of April 2018 to March 2019 may have exposed the "soft underbelly" of Singapore's national security. Whilst a force multiplier, technology should not eclipse the human factor in cyber security.

COMMENTARY

ON 31 MARCH 2019 Prime Minister Lee Hsien Loong convened the Public Sector Data Security Review Committee. Subsequently on 15 July 2019, this was followed up with the Smart Nation and Digital Government Office (SNDGO) announcing the roll out of 13 new cyber security measures as part of a common cyber security framework to be adopted by all government agencies.

While these are important first steps in the cyber security arms race, a significant challenge that will continually be faced by the SNDGO and possibly all cyber security defenders at large, would be the temptation of viewing the cyber security issue through a technology-biased lens. There is also the notion that cyber security is largely a technical matter which can be addressed with the best technology. The report by the Committee of Inquiry ("COI") on the Singhealth data breach highlighted that "vulnerabilities in human assets can be just as dangerous as those in information systems".

Human Error as a Key Factor

On 29 January 2019, six months after the Singhealth data breach, confidential records of 14,200 people who had been diagnosed with HIV were stolen from the Singapore Ministry of Health ('MOH') and leaked online. In what may be considered a "classic" insider attack, the perpetrator had allegedly gained access to the confidential records by exploiting a personal relationship with a Singapore doctor who had authorised access to the MOH's HIV registry.

In March 2019, it was reported that compromised login credentials of Singapore government agency personnel were found to be leaked and put up for sale on the dark web.

Even in the Singhealth data breach whereby the Advanced Persistent Threat ("APT") was using advanced hacking tools, the COI concluded that it was highly likely that a phishing email, considered by experts to constitute a non-malicious or inadvertent form of insider attack, led to the initial breach of the Singhealth network security.

Prima facie, human error or negligence was a key factor in all the said data breaches. The human factor played a dominant role whereby technology alone would not have been able to stop the perpetrators.

The Insider Threat

To be circumspect, some of the most serious data security breaches to-date have occurred outside of Singapore. According to the US Department of Health and Human Services website, there have been 2,667 major health data breaches affecting over 193 million individuals in the US as of March 2019 since 2009. On 30 July 2019, a major US bank, Capital One, suffered one of the largest data breaches to-date which resulted in the personal information of approximately 100 million people being stolen by a former employee of one of its cloud computing contractors.

Arguably the most damaging data breaches would be the exfiltration of highly classified US intelligence information by Chelsea Manning in 2010 and separately by Edward Snowden in 2011. Known as "insider threats", these incidents resulted in the US government scrambling for countermeasures and precipitated the establishment of the National Insider Threat Task Force (NITTF).

An insider threat is defined as the potential for an insider to harm an organisation by leveraging on his or her privileged level of knowledge and/or access. The data breaches by Snowden and Manning are clear examples of what is known as the malicious insider attack. The HIV data breach in MOH could easily qualify as another example of a malicious insider attack.

An "insider threat" may also not necessarily be driven by malicious intent; it may constitute an individual who is complacent or ignorant about security policies and procedures. A lack of training, for example, can lead to ignorance or complacency which in turn can make an organisation vulnerable to security threats. These are known as non-malicious or inadvertent insider threats.

Hence in the case of the Singhealth data breach, the employees who opened the phishing emails and inadvertently paved the way for the initial breach into the Integrated Health Information Systems Private Limited ("IHiS") system, could be considered as non-malicious or inadvertent insider threats.

Importance of Organisational Culture

Organisational culture, in which the human factor also plays a dominant role, was a key consideration in the COI report on the Singhealth data breach. The report highlighted that the delayed treatment of cyber security issues and incidents by the IHiS staff and middle management in their incident response to the data breach was largely attributed to organisational culture.

In Amy Zegart's study of the mass shooting at Fort Hood, Texas in 2008 by an insider which killed 13 and wounded 43, she concluded that organisational weaknesses within the Pentagon played a significant role which led to a series of failures in preventing the shooting.

Zegart asserted that inappropriate organisational culture and processes resulted in a failure to share information and a misallocation of resources which squandered multiple opportunities to detect and thwart the attack. She called these organisational weaknesses "dark matter that lurked invisibly in the background" which were often overlooked as contributing factors in past disasters.

Another organisational weakness was the "hidden hazard of routines" which could lead individuals in organisations to continue doing things in the same ways even though it was no longer effective or appropriate in the face of evolving and new threats.

Case for a Holistic Approach

As long as human participation in key aspects of organisations or systems is needed, the human factor will remain the weakest link in cyber security. With human users, invariably as insiders of the system or organisation, because of their privileged access to their organizations or systems, they will presumably have intimate knowledge of their organisation/system's security features and consequently its vulnerabilities.

In the context of transforming organisational culture to combat organisational weakness and mitigate the insider threat, the public sector and private sector should continue in their efforts to keep employees motivated and loyal, to build security-inclined cultures.

Such cultures are to promote widespread employee buy-in to the need for cyber security hygiene and to incentivise employees to identify and address potential vulnerabilities. Equally important would be finding an appropriate balance between trusting employees and remaining aware of the possibility of security threats by both insiders and outsiders.

Whilst the capabilities of cybersecurity software will continually improve with the advancement of technology, barring the advent of fully autonomous artificial intelligence ("AI") in the likes of "Skynet" from the "Terminator" series of movies, the human factor remains a critical factor.

The effectiveness of software will only be as good as the data input into them. Technology is undoubtedly a critical force multiplier in any security system, but at the end of the day, it is just that – a force multiplier.

Sustained vigilance must take a holistic approach incorporating technical means as well as non-technical factors. Among such factors are insider threat mitigation and fostering a strong healthy organisational culture that is security-inclined. All this will remain necessary to address the perennial weaknesses attributed to the human factor in cyber security.

Edwin Hooi is a certified consultant in Risk and Information Systems Control (CRISC). He has served clients in both private and public sectors in governance, risk management and compliance. An RSIS alumnus, he is a founding executive committee member of the RSIS Alumni Association.