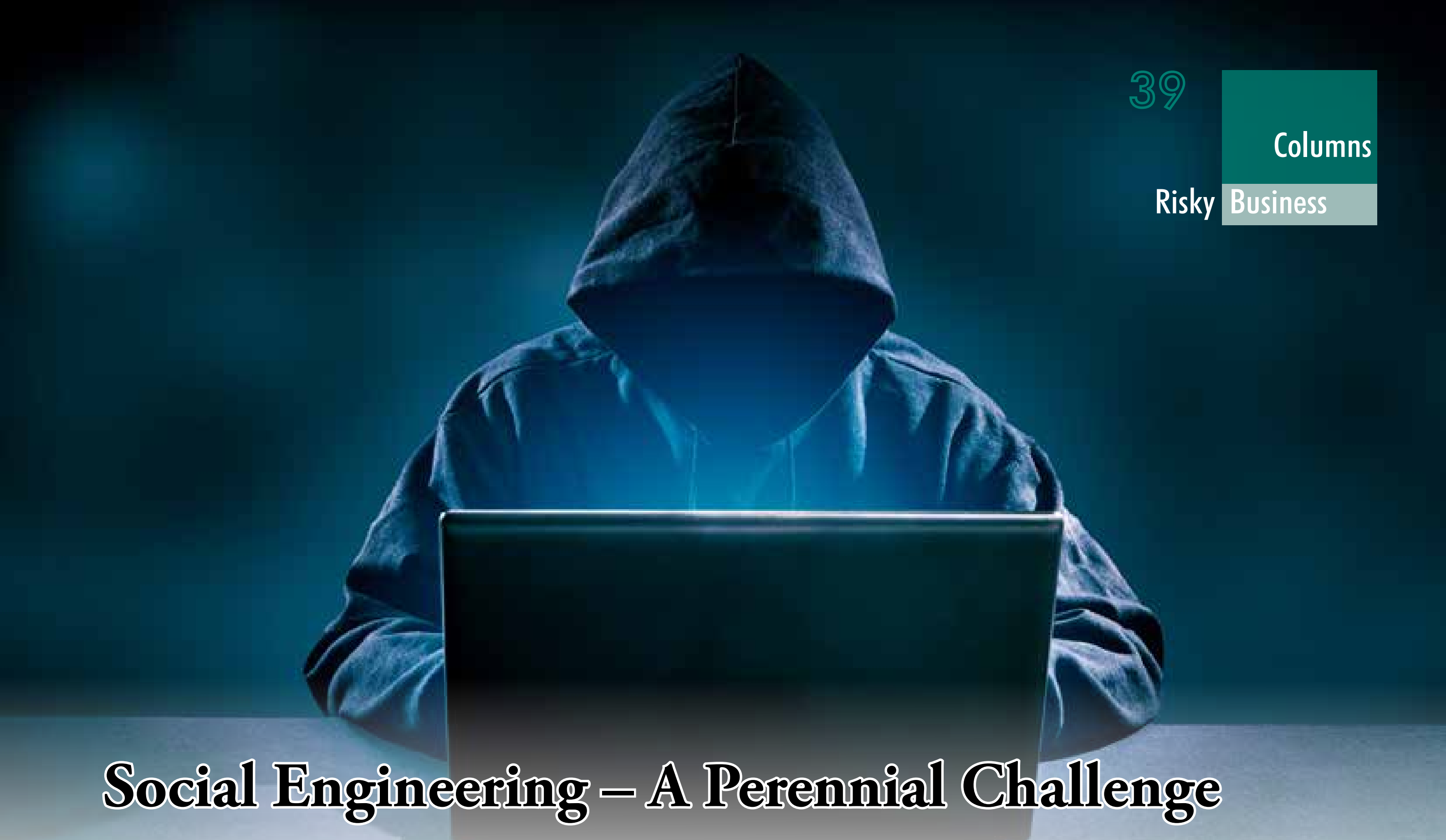


Social Engineering – A Perennial Challenge

Imagine receiving an e-mail from an online retailer you always visit, informing you of a flash sale in the next five minutes. Not wanting to miss out on this opportunity you click the link.

Within the next few seconds, your Internet browser brings you to a familiar retail website, prompting for your credentials. Almost like a reflex, you key in your e-mail and password. The next pop-up that greets you, is a set of familiar blue fonts saying "This password was recently changed".

For the next 30 seconds, you proceed to hammer the keyboard with all known username-password combinations that you can remember, mumbling "One of these must be right …" Before you know it, the flash sale is over and you have just missed one of the greatest deals of your life.

On the other side of the planet, a hacker grins as he has just received the keys to your online kingdom, along with thousands of other victims.

You have just been phished.

What Exactly is Social Engineering?

Social engineering, in a cyber-security context, refers to manipulative acts performed by hackers to get people to give up confidential information, or perform actions that may compromise their computer system.

It is one form of cyber-attack that is often used to gain an initial entry point into an organisation. Social engineering is highly effective as it exploits human vulnerabilities which, unlike computer vulnerabilities, are difficult to pinpoint and fix.

Phishing is one of the most commonly known techniques of social engineering. Phishing scams are conducted via the Internet, and often involve spoofed e-mails and re-created websites that look like the original.

Like the scenario mentioned at the start of this article, one of Singapore's largest banks was also the target of such a phishing scam in 2014. A phishing website built to resemble the bank's original website was detected by the bank. At first glance, it was impossible to tell them apart.

In 2011, a renowned security company which creates two-factor authentication devices fell victim to phishing e-mails. The attacker sent e-mails to employees with a malicious attachment named "2011 Recruitment plan.xls". The attachment contained a zero-day exploit – one that takes advantage of software vulnerabilities that have yet to be disclosed publicly and have no ready security fix or patch – which allowed the hackers to break into the company.

In Singapore, KPMG has investigated several cases whereby phishing e-mails are the root cause behind data breaches for companies. Victims include multinationals, law firms and banks. The malicious payload of these phishing e-mails are obfuscated and exhibit a consistent trend of being able to bypass traditional signature-based anti-virus scanning solutions.

Social engineering may also be performed in person, such as by piggybacking an employee through restricted doorways without a valid pass. One famous example is the story of Kevin Mitnick,[1] who masqueraded as a Pacific Bell (AT&T) employee, entered the telecommunication company's premises, and obtained sensitive information in the process.

However, physical social engineering techniques are high risk manoeuvres. With the proliferation of high definition security cameras and video analytic technologies, physical social engineering techniques could easily compromise a hacker and are rarely practised.

A relatively "safer" approach is vishing – the act of social engineering conducted through the phone. This is generally considered safer for the hackers due to the low risk of being traced, identified and caught. Recent cases in Singapore include the high profile "DHL scam calls" whereby social engineers masqueraded as DHL and overseas customs officers to extort money from unknowing victims. It was reported by the *Straits Times*[2] that over SG$12 million was lost to the scam.

Another similar social engineering campaign also took place in 2016. Social engineers changed their phone's caller ID to that of the Singapore Police Force's "999". Leveraging on the "false authority", the scammers went on to obtain personal and banking information from victims.[3] This method of putting up a false pretence is a social engineering technique known as pretexting.

Who's at Risk?

Cyber defence is an asymmetrical threat. The low barrier of entry needed to create a malicious software (malware), makes cyber-attacks exceptionally attractive for criminals and rogue nations alike. The situation is further exacerbated by the anonymised nature of the Internet.

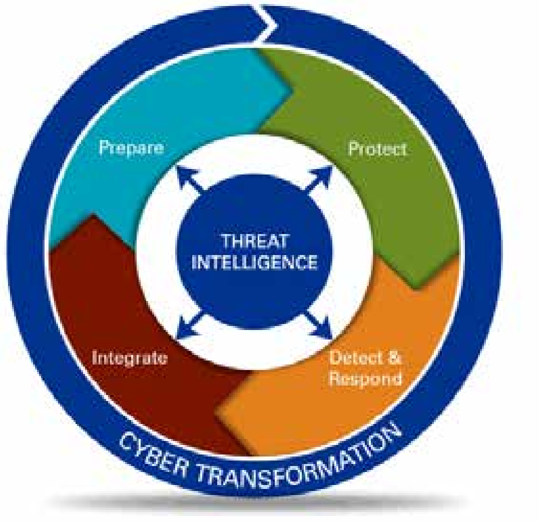
Social engineering is often used as a delivery mechanism for such malwares. Anyone, including your employees, may be socially engineered to become an insider threat that compromises an otherwise secure organisation.

The cost to protect, detect, response and recover from such attacks are increasing. According to the 2016 Cost of Data Breach Study conducted by Ponemon Institute, the average total cost of a data breach for companies surveyed had increased from US$3.79 million to US$4 million.[4] This is several times the price to purchase a zero-day exploit from the black market.[5]

According to Cisco's article on *The Industrialization of Hacking*,[6] organisations are beginning to accept that being hacked is not a matter of if, but when. KPMG's cyber security framework also reflects this thinking. It is intelligence-driven at its core, highlighting the need to remain at the forefront of the threat landscape.

When faced with a cyber-threat, several courses of actions are available. The 2006 *Information Operations* publication[7] developed for the US Armed Forces defined the objectives of cyber operations as activities to disrupt, deny, degrade, destroy or deceive an adversary in cyberspace.

Apart from these reactive intelligence driven actions, proactive detective measures should also be put in place to ensure that future threats of similar nature are mitigated. These activities constitute a successful threat intelligence programme that should form the cornerstone of any organisation's cyber security decision-making process.



Safeguarding Your Firm

A holistic security solution encompasses the people, process and technology aspects of an organisation. It should cover the areas of threat prevention, detection and response.

People

People refers to company employees or contractors who have access to internal systems within an organisation. Employees should be aware that the information they put on the Internet could potentially be used against them or their organisation.

Training programmes and exercises could be conducted to enhance the resiliency of employees against social engineering. Mock phishing exercises could be conducted to measure the "click-through" rate of employees.

Education is a very effective measure that covers all three tenets of prevention, detection and response. However, for it to be successful, it is essential that managers take ownership of dealing with the challenge of social engineering. They have to show a genuine interest and be willing to study how best to engage with the workforce to educate staff and build awareness of the threat of such attacks. This is often about changing the corporate culture such that employees are alert to the risk and are proactive in raising concerns with supervisors.

Process

Procedural changes could make the difference between a successful exploit and a failed one.

Procedures enforcement such as requiring all sensitive transactions to be verified with an out-of-band verification (e-mails verified with a phone call and vice versa), is one example of a low cost, high payoff mitigation measure.

No information should be provided through the phone, be it directly or indirectly. Employees should be trained to respond professionally through the phone, especially when coaxed for information under pressure. This could be in the form of a third-party asking leading questions, performing elicitation, pretexting or other manipulative communication techniques.

Technology

There are numerous ways in which technology-enabled defences can be put in place against social engineering attacks such as phishing.

An intelligence driven approach should be considered. For example, denial and disruption activities such as blocking or quarantining spam e-mails at the gateway can prevent any accidental user from falling victim to phishing e-mails.

This, however, should not be the only course of action. Such e-mails are often lucrative sources of intelligence. Apart from spam filter, e-mail sandboxes could be deployed to identify suspicious attachments. Such e-mails should be sent to a dedicated cyber threat hunting team for further analysis. Indicators of compromise could be generated from these e-mails to search for existing dormant threats within an organisation and further strengthen existing cyber defence implementations.

Humans, the Weakest Link

The human factor is and remains the weakest link in relation to security.

Creating a safer cyberspace is one of the pillars of the Singapore Cyber Security Strategy. A safer cyberspace is the collective responsibility of the Government, businesses, individuals and the community.

The world of cyber security is dominated by specialist suppliers that sell technical products, such as products that enable rapid detection of intruders. These tools are essential for basic security but are not the basis of a holistic, robust cyber security strategy. Investment in the best tools will only deliver a return when people understand their responsibilities to keep their network safe.

A well-informed employee can turn into a critical asset. An organisation with a cohesive, secure culture is the key to mitigating social engineering.

► **Eddie Toh**
Forensic Partner
KPMG in Singapore

► **Chua Zong Fu**
Associate Director, Forensic
KPMG in Singapore

The views and opinions are those of the authors and do not necessarily represent the views of KPMG in Singapore.

Notes

[1] Source: Ghost in the Wires: My Adventures as the World's Most Wanted Hacker, K. Mitnick, & S. Wozniak, 2012

[2] Source: <http://www.straitstimes.com/singapore/courts-crime/155-people-lost-over-12m-in-dhl-phone-scam>

[3] Source: <http://www.straitstimes.com/singapore/do-not-return-calls-from-numbers-starting-with-999-police-on-latest-phone-scam>

[4] Source: 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute LLC, 2016

[5] Source: <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#15e8e9bd6033>

[6] Source: <https://newsroom.cisco.com/feature-content?articleId=1572627>

[7] Source: Joint Publication JP 3-13 Information Operations, United States Government US Army, 2006