MARSH

SOCIAL ENGINEERING FRAUD – RECOMMENDATIONS AND SOLUTIONS

Social engineering fraud is widespread, increasing at an alarming rate, and the fraudsters are persistent and relentless in the pursuit of their crimes. For those unprepared organisations that fall victim to an attack, the financial consequences can be devastating.

WHAT IS SOCIAL ENGINEERING?

"Social engineering fraud" refers to a variety of techniques used by fraudsters to deceive and manipulate victims into voluntarily performing actions which result in them giving out confidential information or transferring funds.

Techniques vary and can include: emails which purport to be sent from employees, vendors, clients, customers, or other organisations; phone calls, text messages, or even leaving a malware-infected USB stick lying around an office.

Fraudsters aim to piece together information from various sources such as social media and intercepted correspondence in order to appear convincing and trustworthy while perpetrating the fraud. The often complex nature of these schemes makes it extremely difficult to identify the fraud before it is too late. Victims range from small businesses to large organisations, across many industries and geographies. The fraudsters are not selective, and will often adopt a scatter-gun approach to see what response they can get from a fraudulent communication.

HOW ARE BUSINESSES BEING TARGETED?

TOP-3 CYBER THREATS IN 2016[1]

52%	Social engineering
40%	Insider threats
39%	Advanced persistent threat

A diverse range of companies around the globe lost more than US$3.1 billion[2] in the period between October 2013 and May 2016 as a result of social engineering fraud.

[1] Source: Varonis

[2] Source: FBI

EXAMPLES OF ATTACKS[3]

June 2014	April 2015	June 2015
Fraudsters used well-targeted emails to convince Scoular Co's controller to send a series of wire transfers totalling US$17.2 million to a bank in China.	Scrap processor Mega Metals Inc. wired US$100,000 to a German vendor to pay for titanium shavings, but the vendor did not receive payment.	An outside entity used fraudulent requests targeting Ubiquiti Networks' finance department.
Emails claiming to be from the CEO said that Scoular was buying a company in China and instructed a controller to get wire instructions from an employee of its accounting firm.	The hacker falsified wire-transfer instructions to collect money.	An attacker used a "CEO scam", causing an employee to transfer US$46.7 million held by a company subsidiary incorporated in Hong Kong.
Scoular lost US$17 million due to this "spearphishing" attack.	**Mega Metals Inc. was tricked into losing US$100,000.**	**Ubiquiti Networks was the victim of a US$17 million social engineering attack.**

DO TRADITIONAL CRIME POLICIES ADEQUATELY ADDRESS THE EXPOSURES?

Whether or not traditional crime insurance policies (for a commercial institution or a financial institution) provide cover for this type of loss is not always clear. The policy wording may not be broad enough to encompass all of the ways a fraudster could persuade a company to transfer funds.

In order to address social engineering exposures, some insurers offer coverage by way of a specific extension. These are often not fit for purpose, as they may not address all of the ways that a fraud can be perpetrated. They may include a requirement for a specific verification process to be completed in relation to communications the company may receive, which may not be in line with the company's processes and procedures.

Social engineering coverage is more frequently being offered on a sub-limited basis, particularly within the US, and for financial institutions. Many insurers also require the completion of supplemental applications or questionnaires regarding internal business systems and controls, which can be both arduous and time-consuming for insurance buyers.

Coverage available for social engineering can vary from company to company. Coverage for commercial institutions is often broader, as is cover for those businesses that can demonstrate that they have robust systems and controls in place to prevent attacks by fraudsters.

RECOMMENDATIONS AND SOLUTIONS

1. Review systems and controls

Having robust IT security, policies and procedures plays an important part in preventing and managing social engineering frauds, and can include:

- A multi-level authentication and verification process.
- Appropriate access controls.
- Employee fraud awareness training.

When a fraud loss does occur, responding effectively is critical. This ensures that the situation is appropriately managed and that the impact to the business is mitigated.

Marsh Risk Consulting (MRC) Financial Advisory and Claims Services (FACS) provide pre- and post-loss services to assist clients, ranging from fraud risk management through to post-discovery fraud investigation services.

[3] Sources: WSJ, CSO Online, Advisen Ltd.

2. Crime Insurance

Even if your business has the most robust systems and controls in place aimed at preventing social engineering fraud, it is still extremely difficult to prevent attacks. This is because fraudsters are often extremely successful in circumventing internal procedures by demonstrating a sophisticated knowledge of them. They specifically use social engineering techniques to target employees within a business and use them obtain the information they require. The consequences of which can be financially devastating.

Appropriate crime insurance can protect you from the financial consequences of social engineering fraud. It should reflect the different techniques used by fraudsters to perpetrate their fraud, and, in the event of a loss, provide cover for the costs of verifying and preparing appropriate documentation to prove it.

Key coverage/terms should include:

- An "all-risks" definition of fraud/crime to encompass social engineering loss.
- No requirement for prior verification of sender of correspondence.
- Cover for the cost of assessing and quantifying a loss.
- No "voluntary transfer" exclusion.
- No continuing condition precedents or systems of checks for coverage to apply.

SUMMARY

Irrespective of how "honest" employees are, or how sophisticated the systems and controls of a company may be, fraudsters who use social engineering as a means to defraud companies are extremely persistent. Prevention plays a key part in avoiding social engineering attacks on your business.

Commercial institutions are just as at risk as financial institutions when it comes to attacks by fraudsters. Insurance can be an important line of defence in protecting the assets of your business in the event a fraud. The cover you select should be fit for purpose and respond to a wide range of techniques that fraudsters use when carrying out social engineering attacks.

Businesses that demonstrate robust controls and procedures are more likely to obtain favourable terms from insurers. Marsh continues to develop tailored insurance products and select the best coverage available in the market to meet our clients' needs and exposures.

For further details on the impact of social engineering fraud and our crime insurance capabilities, please contact:

ELENI PETROS
FINPRO UK
+44 (0)20 7357 1507
eleni.petros@marsh.com

HOLLIE MORTLOCK
FINPRO UK
+44 (0)20 7357 3097
hollie.mortlock@marsh.com

GRAPHICS NO. 16-1196