Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Social Engineering Fraud

Social engineering fraud, also known as imposter/impersonation fraud, has become endemic throughout North America and Europe. It involves a criminal who purports to be a vendor, client, company executive or other legitimate party and provides seemingly credible information to support that representation. Perpetrators of social engineering fraud are becoming more sophisticated and the resulting costs to corporations are soaring. According to the FBI, from October 2013 to August 2015, more than 8,000 victims across the United States were defrauded of almost $800 million, with the average loss at $130,000.

Social Engineering Fraud Examples

Client/Vendor Impersonation Fraud by Business Email Compromise (BEC)

An employee receives a phone call from an individual who he believes to be a genuine supplier. The fake supplier advises that his bank details have changed and payment is to be made to a new account. Going through procedure, the employee advises that the request must be received in writing via email or on company letterhead. The employee later receives an email from what appears to be the legitimate supplier complete with the supplier's signature at the foot of the email. The employee proceeds to change the bank details and a payment is issued. Sometime later, the genuine supplier requests payment, indicating that the original payment was never received. Further investigation will identify that the earlier request was fraudulent.

Fake Officer Fraud

A mid-level finance employee is the only person remaining in the office on a Friday evening when she receives a phone call from an individual who identifies himself as the company's CEO. He explains that a major acquisition is about to take place, but it must close tonight and he can't get in touch with anyone else on the finance team to process the payments. The employee explains that she only has authority to transfer funds of up to $50,000 and that no one else is in the office to countersign the transfer. The CEO grows increasingly irate with the employee for refusing to transfer the funds because she does not have the authority. He repeatedly tells her that he's granting her the authority. Eventually the CEO persuades her to circumvent the established procedure by issuing multiple $50,000 transfers totaling $500,000.

Lawyer Impersonation

An employee receives a phone call from someone posing as an attorney and claiming to be handling confidential or time-sensitive information. These scammers typically initiate contact at the end of the business day or work week to coincide with the close of business of international financial institutions. They then pressure the victim to act quickly, or even secretly, in transferring funds.

Coverage Issues

The above examples represent common social engineering techniques that have resulted in transfer of funds by unsuspecting victims. Unfortunately, too often insureds have come to realize that their insurance policies (cyber/crime) may not be responsive to these types of sophisticated social engineering scams. Many insureds assume that theft of funds through social engineering fraud would be covered under a cyber liability policy or a crime insurance policy's computer/funds transfer fraud extension; however, insurers have generally denied coverage under both policies The following are common coverage hurdles in traditional cyber liability and crime policies, as well as the solutions that may be available to address those exposures:

Cyber Liability

A cyber liability policy is comprised of several insuring agreements. The privacy liability insuring agreement provides liability coverage should there be a disclosure of personally identifiable information (PII), commonly referred to as a data breach. In addition, the breach response insuring clause will cover costs associated with a data breach when PII is stolen or disclosed without authorization. While it is possible that unintentional, unauthorized disclosure of PII may result from a social engineering scam, the actual theft of funds is not a covered loss under most cyber insurance policies.

Crime: Computer Fraud

Under this insuring agreement, the insurer pays the insured for a direct loss of money sustained by the insured resulting from computer fraud committed by a third party. Computer fraud is generally defined as the unlawful taking of money resulting from a computer violation. Many carriers have cited the "indirect loss" exclusion (or alternatively, failure to trigger the insuring agreement's direct loss requirement) to deny coverage for social engineering losses, stating that it was not the third party's action that directly resulted in loss, but rather an intervening party (i.e., employee executing the requested action). Other exclusions have also been cited by insurers, including: (1) losses arising directly or indirectly from theft of confidential information; and (2) losses resulting directly or indirectly from the surrendering of money in any exchange or purchase, whether or not fraudulent, with any other party not in collusion with an employee.

Crime: Funds Transfer Fraud

Under this insuring agreement, the insurer pays the insured for loss of money sustained by the insured resulting directly from fraudulently transferred funds committed by a third party. This would apply to any fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions, other than forgery, *purportedly* issued by the insured to a financial institution, directing such institution to transfer, pay or deliver money from the insured's account *without the insured's knowledge or consent.* Social engineering losses have been denied under this insuring agreement because the funds were transferred with the insured's knowledge or consent, albeit based on fraudulent information. Insurers have also raised the same exclusions previously referenced in the computer fraud context to bar coverage under funds transfer fraud.

Specific Coverage is Available for Purchase

Specific coverage for transfer of funds arising from social engineering fraud is now offered by a number of crime insurers, including Chubb, Travelers, AIG, Hartford and Zurich, among others. In many instances, a supplemental application or additional information regarding controls and procedures will be required. Depending on the exposure and information supplied, coverage limits can range from very small ($10,000) to meaningful limits ($1 million or more). Currently, very few cyber insurance carriers are willing to extend coverage for social engineering fraud that results in theft of funds. However, a handful of Lloyd's of London syndicates have introduced an extension endorsement to their cyber policies that provides first party recovery of transferred funds as a result of social engineering fraud. The language is similar to what is used for crime policies. Limits available under these extensions generally do not exceed $100,000.

Is Crime or Cyber the Correct Policy to Insure this Risk?

Coverage solutions have been introduced on both crime and cyber policies to address theft of funds that result from social engineering. Several questions must be considered when making a decision as to which policy to utilize to insure for this exposure:

1. Which policy is better suited to meet an insured's needs for transfer of funds coverage?
2. Does the policy language impose any conditions precedent to coverage? If so, do those align with your controls?
3. Which policy will afford a limit that is adequate for your risk?
4. Have you considered the "other insurance clause," if you happen to have coverage under more than one policy for theft of funds resulting from social engineering?