Aon Risk Solutions
Financial Services Group

Client Alert: Social Engineering Exposures

While social engineering can refer to many things outside of a risk management context, within the insurance world, social engineering has assumed a specific, and notable, meaning. In brief, social engineering refers to the use of identity deception to gain the confidence of an employee to induce him or her to part with an organization's money or securities. We will explore some of the most common forms of social engineering, relevant coverage interpretations, and available coverage solutions.

Where Does The Threat Arise From?

Social engineering attacks can come in many forms, including:

- Phishing scams are attempts by fraudsters to induce individuals into providing personal information such as bank account numbers, passwords, and credit card numbers
- Spear phishing is an electronic communications scam targeted towards a specific individual, organization, or business
- Vishing, or voice phishing is the criminal practice of using social engineering over the telephone to gain access to private personal and financial information
- SMiShing (short for "SMS phishing") is a security attack in which the user is tricked into downloading a Trojan horse, virus, or other malware onto a mobile device
- Mining social media allows a perpetrator to identify executives at a company via social media, with collected information used to gather proprietary information or induce fraudulent transfer

Regardless of the threat source, the fraudster seeks to induce the transfer of money or securities to a fictitious account for the benefit of the perpetrator. The fraudster may imitate a senior executive (i.e., "fake president"), often in a very credible format, and once funds are sent to the fictitious account, they are often unrecoverable.

Commercial crime insurers' responses have varied and evolved significantly in recent years.

While a "theft" has undoubtedly occurred in a social engineering loss, the commercial crime policy likely has not been triggered because the employee did not "steal" the money/securities directly, and the employee certainly did not benefit from it. Historically, crime policies did not explicitly address social engineering, thus resulting in varying outcomes.

Relevant Cases

Although a few courts have found coverage for social engineering losses under crime policies, most courts have found that social engineering losses are not covered under the policy's Computer Fraud, Funds Transfer Fraud, or Forgery coverage agreements. See *American Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am., No. 16-12108, 2017 U.S. Dist. LEXIS 120473 (E.D. Mich. Aug. 1, 2017); Taylor & Lieberman v. Fed. Ins. Co., 681 Fed. Appx. 627 (9th Cir. 2017); and Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252 (5th Cir. 2016).* The decisions that have denied coverage have generally held that duping caused the loss, and that the use of a computer was merely incidental. Only two recent decisions have found coverage, or potential coverage, for social engineering losses. *Medidata Solutions., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471 (S.D.N.Y. 2017) and Principle Solutions Group, LLC v. Ironshore Indem., Inc., 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016).* Both of those cases, however, are currently being appealed by the insurer and may be overturned. None of the cases involved an insured that had been directly hacked.

We're here to empower results

If you have questions about your specific coverage or want more information, please contact your Aon broker.

aon.com

Empower Results®

Coverage Solutions

Social engineering coverage is widely available in the crime insurance marketplace. Underwriters require a social engineering questionnaire to ascertain whether they will offer the coverage, and to determine the limit and deductible that they are comfortable providing.

While domestic (U.S.) underwriters do offer social engineering limits within their respective crime policies, more often than not, they provide a sub limit for this coverage. However, higher limits can be provided within the primary layer if the insured can show appropriate controls.

Strategies for achieving higher limits over a primary sub-limit, including limits equal to (or above) the existing overall crime program limits, include:

- Layered crime policy – In this example, the primary coverage for social engineering would be provided on a sub-limited basis within the Insured's crime policy. The excess crime insurer(s) would then provide coverage for social engineering, also on a sub-limited basis, on each of their respective excess layers. Each excess layer of social engineering coverage would drop down and be follow-form, attaching directly excess of the social engineering sub-limit below.
- A separate stand-alone excess social engineering crime tower is also available to maximize capacity. This approach can be purchased in conjunction with the layered approach mentioned above. Excess insurers will follow form to the primary insurer's social engineering endorsement terms and conditions.
- Consider approaching the London market. Certain Lloyd's of London syndicates offer social engineering coverage within crime programs with no sub-limit applied.

Avoid condition(s) precedent language on any social engineering endorsement, such as "Before acting upon any such Transfer Instruction the Insured shall confirm the validity of such Transfer Instruction according to a prearranged procedure in which the Insured verified the authenticity and accuracy of the Transfer Instruction by means of a call back to a predetermined telephone number or other verification procedure agreed to in writing." If the Insured can demonstrate internal controls, your broker may request this (or any similar) wording to be deleted from the social engineering endorsement.

Conclusion

While virtually unheard of just a few years ago, social engineering is a serious crime exposure. While the exposure has grown, so too have the options to address it.

About Aon's Financial Services Group

Aon's Financial Services Group (FSG) is the premier team of executive liability brokerage professionals, with extensive experience in representing buyers of complex insurance products including directors' and officers' liability, employment practices liability, fiduciary liability, fidelity, and professional liability insurance. FSG's global platform assists clients in addressing their executive liability exposures across their worldwide operations. Aon's Financial Services Group manages more than $2.2 billion in annual premiums, assists with annual claim settlements in excess of $1 billion, and uses its unmatched data to support the diverse business goals of its clients.