CYBER CRIME THROUGH SOCIAL ENGINEERING

AXIS

Organizations of all sizes, across all regions, and in all business sectors face an evolving risk from cyber criminals.[1]

As businesses have become increasingly dependent upon technology, criminals have shifted from theft of physical assets to the theft of electronic information. The growing use of technology-enabled processes exposes businesses to cybercrime — from direct theft of data (leading to the potential loss of financial assets) to the theft of personal data (that can be used to assemble an attack on financial assets). Cybercrime can threaten processes from point of sale purchases by debit/credit cards in the retail environment, to ATM transactions in the banking environment, to e-commerce or on-line sales, and to electronic business communications.

Recent studies illustrate the wide-ranging threat of electronic crime.

> *"In 2017, more than three of four (78%) respondents to the U.S. State of Cybercrime Survey detected security events in the preceding twelve months,"*

and more than one third (36%) reported that the number of security incidents had increased over the previous year. The average number of incidents is also significant, with increasing monetary loss.

While cyber criminals employ several measures to breach information security defenses and seize sensitive business information, technical security measures implemented in response to increased regulation (as a result of Sarbanes-Oxley, Gramm-Leach-Bliley, and the Health Insurance Portability and Accountability Act) make direct pure technological attacks more difficult and costly. As a result, cyber criminals have shifted their focus away from such pure technological attacks and instead have increasingly attacked employees through the use of "social engineering" — a collection of techniques used to manipulate people into performing actions or divulging confidential information.

Social engineering is not a new concept. A social engineer is nothing more than a con man who uses technology to swindle people and manipulate them into disclosing passwords or bank information or granting access to their computer. Understanding how these social engineers work and the schemes they employ is key to implementing successful internal controls which minimize the risk of loss.

Social engineers prey on innate human emotions

The success of social engineering schemes does not always rely upon sophisticated software or hacking technology. Social engineers exploit human emotions (such as fear, curiosity, the natural desire to help, the tendency to trust, and laziness) to bypass the most iron-clad security measures. Social engineering schemes, therefore, remain one of the most foolproof and commonly used methods to breach secure systems.

In the cyber world, the weakest link in the security chain is the employee who accepts a person or scenario at face value. Social engineers target this vulnerability. A few common examples illustrate how social engineers prey on human emotion.

Messages from Trustworthy Sources:

> *"Social engineers cleverly manipulate the natural human tendency to trust and accept representations at face value."*

Human nature is to trust others until they prove that they are not trustworthy. If someone tells us that they are a certain person, we usually accept that statement.

Seizing upon this trait, cyber criminals commonly hack email accounts to gain access to the owner's contact list. Once access to an email account has been obtained, the cyber criminal can send messages to all the owner's contacts. These messages prey on trust and curiosity. For example, the social engineer may send a:

- link that you "just have to check out." Because the link comes from a friend and humans are curious, the recipient clicks on the link and the system becomes infected with malware the criminal can use to take over the machine and collect information.
- download (disguised as pictures, music, movie, document, etc.) embedded with malicious software. Once downloaded (which the recipient is likely to do since he/she thinks it is from a friend), the system is infected. Now, the criminal has access to the system.

Phishing Schemes:

Phishers seize on fear and gullibility to obtain private information. Phishers send e-mails, instant messages, or text messages that appear to derive from a legitimate or popular company, bank, school, or institution. These messages explain there is a problem that requires you to “verify” information by clicking on the displayed link and providing information in their form. The link location may look legitimate (containing the correct logos and content copied from a legitimate website). The spoofed site closely resembles a legitimate site and tricks the user into entering his credentials, thereby enabling the social engineer to implant malicious programs or executables or spy on the user’s computer activity.

Baiting scenarios:

Social engineers also use greed to manipulate human operators. Often found on Peer-to-Peer sites offering a download of a hot new movie or music, social engineers dangle something people want and wait for people to take the bait. Once people take the bait, the cyber criminal uses malicious software to corrupt secure systems and steal confidential information or banking information.

Impersonating Superiors:

Impersonation is one of the most common social engineering techniques. Impersonation can occur over the phone or on-line. For example, a social engineer may obtain the name of someone in the organization who has the authority to grant access to confidential information. Using that information, they call the target and claim that a senior official authorized the disclosure of information or transmission of funds. Similarly, a social engineer may impersonate a network administrator or help desk member and ask an employee for his/her username and password (so they can troubleshoot a network problem and/or trace a problem).

These schemes prey upon the desire to be helpful and fear of being reprimanded. Many employees receive a negative reaction from superiors if they do not act promptly and/or take too long to complete a project. Fearing reprimand, many employees want to be helpful and follow directions — which can lead to giving away too much information.

Traditional insurance may not cover social engineering

Many businesses mistakenly believe that traditional commercial crime policies cover all cyber-related losses. Although traditional commercial crime policies contain a computer fraud and funds transfer fraud insuring agreement, courts interpreting such policies have generally distinguished between incidents (1) where a thief hacks the insured's computer systems and, without any action by the insured, uses the computer to steal the insured's property (either directly by transferring funds using the insured's computer system or by convincing the insured's bank to transfer the insured's funds) and incidents and (2) where the insured voluntarily transfers funds. Depending upon the precise terms and conditions of the coverage provided, courts have generally held that the latter claims — many of which arise from social engineering — are not covered.

Traditional computer fraud insuring agreements generally limit coverage to direct loss resulting from "theft" through the use of any computer system."[2] Many claims involving social engineering do not involve the fraudulent withdrawal of funds from the insured's account, but instead involve an authorized withdrawal induced by fraud.[3] Courts have held that such a loss is outside the scope of coverage typically afforded by the computer fraud insuring agreement because it does not arise "directly" from the use of any computer to fraudulently cause a transfer of property; it arises from an authorized transfer of funds.[4] The mere fact that the insured received a fraudulent email inducing it to take action does not establish the use of any computer to fraudulently cause a transfer of that property." The insured has, upon receipt of an instruction, the choice to take immediate action, conduct an analysis of the instruction, or decline the instruction. That decision-making process breaks any causal nexus and thus, the loss arose from an authorized (and therefore uncovered) transfer of funds.[5]

The decision in *Taylor & Lieberman* illustrates this distinction between covered losses due to a hacking incident and uncovered losses arising from the knowing transfer of funds. In that case, the insured voluntarily transferred funds to a third-party, but claimed that its loss was nonetheless covered under a computer crime policy because it was induced to transfer the funds based upon information conveyed through a computer. The Ninth Circuit Court of Appeals held that receipt of an email is not an "unauthorized entry" into the insured's computer: "T&L also argues that the computer fraud coverage applies because the emails constituted an unauthorized (1) "entry into" its computer system... First, there is no support for T&L's contention that sending an email, without more, constitutes an unauthorized entry into the recipient's computer system."[6]

The Second Circuit Court of Appeals upheld coverage in *Medidata Solutions v. Federal Insurance Company*,[7] but only after the insured proved that it received emails "armed with a computer code" which caused the insured's email system to populate an email the name, email address and photo associated with the insured's president. The district court, however, acknowledged that computer fraud insuring clause requires proof that "perpetrator violate[d] the integrity of a computer system through unauthorized access."[8] The court found that the insured satisfied this standard and established coverage because the insured received spoofed emails that were allegedly "armed" with computer code.[9] The Second Circuit affirmed that decision, based upon its conclusion that "spoofing code was introduced into the email system."[10]

In so holding, *Medidata* distinguished the loss alleged therein from other social engineering schemes. The district court acknowledged the decision in *Taylor*, but distinguished *Taylor* on the basis that it addressed whether the mere receipt of email triggered computer crime coverage and held that *Taylor* stood for the proposition that "the mere sending of emails from the client to the accounting firm did not constitute unauthorized entry into the accounting firm's computer system."[11] That ruling, *Medidata* held, did not apply because "Medidata did not suffer a loss from spoofed emails sent from one of its clients. A thief sent spoofed emails armed with a computer code into the email system that Medidata used."[12]

Social engineering schemes commonly involve an authorized wire transfer input and released by authorized signatories. These facts, the Fifth Circuit explained, break any causal chain between fraudulent emails and the loss: "The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money."[13] Thus, traditional computer crime policies do not cover such losses: "To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would, as stated in Pestmaster II, convert the computer-fraud provision to one for general fraud."[14]

Courts have reached the same result when analyzing such claims under the funds transfer fraud insuring agreement. Subject to the specific terms of the policy, such insuring agreements typically cover fraudulent instructions issued to a financial institution directing such institution to transfer, pay, or deliver money from an account maintained by an insured without the insured's knowledge and consent. Just as the computer crime insuring agreement is designed to cover a hacking incident, the funds transfer fraud insuring agreement is designed to cover the limited instances where an imposter induces a financial institution to allow funds to be withdrawn from the insured's account by posing as the insured and submitting fraudulent instructions. The insuring agreement therefore, will not respond where an employee authorizes a withdrawal.[15] Coverage exists only if the insured demonstrates that the thief issued instructions that purport to have been authorized and the insured can otherwise satisfy the remaining conditions of coverage.[16]

As *Taylor*, *Apache* and *Pestmaster* explain, the computer crime insuring agreement and funds transfer fraud insuring agreement incorporated into standard commercial crime policies are designed to cover certain types of hacking incidents, not loss resulting from the insured's conscious decision to proceed with a business transaction (even if induced by a fictitious or fraudulent computer submission). An insured seeking to cover the risk of loss from social engineering should consider insurance policies tailored to address such risks.

Guarding against social engineering

> *“Social engineering is one of the most difficult crimes to prevent, as it cannot be defended against through hardware or software.”*

In order to build defenses against social engineering attacks, organizations need to design and implement comprehensive security practices:

- **Risk Assessment:** A risk assessment helps management understand risk factors that may adversely affect the company and track existing and upcoming threats. Determining security risks helps enterprises to build defenses against them.
- **Policies and Procedures:** Policies and procedures must be clear and concise. They should be aimed toward mitigating social engineering attacks. Well-defined policies and procedures provide guidelines for employees on how to go about protecting company resources from a potential cyber attack. Strong policies should include proper password management, access control, and handling of sensitive user information.
- **Security Incident Management:** When a social engineering event occurs, a company must have a written, comprehensive protocol for managing such incidents. To manage the incident, the help desk must be trained to track (among other things) the target, their department, and nature of the scheme. Such protocols will enable a company to actively manage the risk of the breach to mitigate potential losses.
- **Training Programs:** Companies should invest in security training programs and update their employees on security threats. Because companies are composed of various departments, training and awareness must be customized to the needs and requirements of each department. Such practices help employees recognize and handle security attacks effectively.

> *“Despite the best vendor background screenings, fraud detection systems, segregation of duties, and education, companies still face an uncertain risk of loss from social engineering schemes.”*

As a result, strong consideration should be given to purchasing coverage tailored to social engineering schemes. Subject to specific terms of coverage within the policy, social engineering coverage expands coverage traditionally afforded under commercial crime policies to address schemes arising from the impersonation of vendors, executives, and clients. Combined with strong internal controls, such coverage enables companies to better protect themselves against the growing risk of a catastrophic loss from social engineers.

Such coverage can be endorsed onto either a commercial crime policy or a cyber insurance policy. Because commercial crime policies are oriented toward covering first-party loss, an insured may prefer to endorse social engineering coverage to that policy while preserving the liability coverage afforded under a cyber policy in the event of a breach which results in substantial liability exposure.

Scott Schmookler, Esq. is a partner in the Chicago office of Gordon Rees Scully Manuskhani, LLP, where he counsels clients on insurance issues relating to commercial crime policies, cyber crime, and data breaches. Scott can be reached at **sschmookler@gordonrees.com** or at (312) 980-6779. To learn more, visit **www.gordonrees.com.**

Lisa A. Block, Esq. is Vice President and Commercial Crime Product Manager for AXIS Insurance's Commercial Management Solutions unit. Based in Princeton, New Jersey, she has nationwide responsibility for commercial crime underwriting and business development. Lisa can be reached at **lisa.block@axiscapital.com** or at (212) 500-7689. To learn more, visit **www.axiscapital.com**.

[1] Recent studies illustrate the wide-ranging threat of electronic crime. 2014 U.S. State of Cybercrime Survey, *available a*t http://www.pwc.com/us/en/increasing-it-effectiveness/publications/2014-us-state-of-cybercrime.jhtml (last visited September 3, 2014).

[2] Taylor & Lieberman v. Fed. Ins. Co., 2017 U.S. App. LEXIS 4205, *3-4 (9th Cir. Mar. 9, 2017); Apache v. Great Am. Ins., 662 F. App'x 252, 258-59 (5th Cir. 2016); Kraft Chem. Co. v. Fed. Ins. Co., 2016 Ill. Cir. LEXIS 1, at *17 (Ill. Cir. Ct. Jan. 5, 2016); Universal Am. Corp. v. Nat'l Union, 959 N.Y.S.2d 849, 853 (Sup. Ct. 2013), aff'd, 972 N.Y.S.2d 241, 242 (App. Div. 2013), aff'd, 37 N.E.3d 78, 81 (N.Y. 2015); Great American Ins. Co. v. AFS/IBEX Fin. Servs., Inc., No. 07-cv-924, 2008 U.S. Dist. LEXIS 55532 at *45 (N.D. Tex., July 21, 2008); 6 Pinnacle Processing Group, Inc. v. Hartford Cas. Ins. Co., 2011 U.S. Dist. LEXIS 128203, 2011 WL 5299557 (W. D. Wash. Nov. 4, 2011).

[3] Pinnacle Processing Group, Inc. v. Hartford Cas. Ins. Co., 2011 U.S. Dist. LEXIS 128203, 2011 WL 5299557 (W. D. Wash. Nov. 4, 2011) (rejecting the insured's contention that computer fraud coverage is implicated simply because a computer was used in the scheme).

[4] Brightpoint, Inc. v. Zurich Am. Ins. Co., No. 1:04-CV-2085, 2006 U.S. Dist. LEXIS 26018 (S.D. Ind. Mar. 10, 2006).

[5] *Id.; see also* Pestmaster Serv. v. Travelers Cas. & Sur. Co. of Am., CV 13-5039-JFW, 2014 U.S. Dist. LEXIS 108416 (C.D. Ca., July 17, 2014).

[6] *Taylor*, 2017 U.S. App. LEXIS 4205 at *3.

[7] 268 F. Supp. 3d 471 (S.D.N.Y. 2017), *aff'd*, 729 Fed. Appx. 117 (2d Cir., July 6, 2018).

[8] *Id.,* 268 F. Supp. 3d at 480.

[9] *Id.*

[10] *Id.* at 118; *see also American Tooling Center, Inc. v. Travelers Casualty and Surety Company of America*, 2018 U.S. App. LEXIS 19208 (6th Cir., July 13, 2018) (finding coverage under policy coverage "use of any computer to fraudulent cause a transfer of Money, Securities or other Property….", on the theory that transmittal of email involved the use of a computer).

[11] *Id.,* 268 F. Supp. 3d at 480.

[12] *Id.*

[13] *Apache,* 662 F. App'x at 254. *Principle v. Ironshore,* 2016 WL 4618761 (N.D. Ga. 2016) cited the district court's decision *Apache v. Great Am. Ins.,* 2015 U.S. Dist. LEXIS 161683 (S.D. Tex. Aug. 7, 2015). The district court's decision in *Apache* was subsequently reversed by the Fifth Circuit (662 F. App'x 252, 258-59 (5th Cir. 2016). *Principle* is currently on appeal.

[14] *Id.* at 268

[15] Black's law dictionary defines a "fraudulent act" as "[c]onduct involving bad faith, dishonesty, a lack of integrity, or moral turpitude." Black's Law Dictionary 687 (8th ed. 1990). This definition requires proof of an intent to deceive: "mere irregularities committed without such intent do not constitute acts of fraud or dishonesty." 13 Couch, Insurance 2d, § 46:55, p 58.

[16] Sb1 Fed. Credit Union v. FinSecure, LLC, NO. 13-6399, 2014 U.S. Dist. LEXIS 49596 (E.D. Pa. Apr. 9, 2014); Morgan Stanley Dean Witter & Co. v. Chubb, 2005 N.J. Super. Unpub. LEXIS 798 (N.J. App. Div. Dec. 2, 2005); Northside Bank v. American Cas. Co. of Reading, No. GD 97-19482, 2001 WL 34090139 (Pa. Commw. Pl. Jan. 10, 2001).