CRC Group
Wholesale & Specialty

State of the Market

Social Engineering: Avoid Coverage Confusion on Cyber Crimes

CRC Group | CRC | CRC Swett | SCU

Social Engineering:

Avoid Coverage Confusion on Cyber Crimes

Social engineering – obtaining money or confidential information from unsuspecting, and thus cooperative victims – has become a prevalent and growing problem. Perpetrators play on people's emotions and rely on the human tendency to offer assistance when asked or in response to authority figures. Their methods have become increasingly sophisticated, convincing people to bypass security controls or divulge information.

Research by security technology firms suggests that social engineering has become the preferred method of hacking.[1] These kinds of cons have been around for thousands of years, but the Internet, pervasive use of e-mail, and social media offer present-day scammers far greater opportunities to defraud businesses and individuals.

While the risk is obvious, insurance coverage for social engineering is not. Insurers are responding to the growing threat to businesses, and some are offering specific coverage for social engineering. A challenge, however, is that coverage forms differ widely and respond differently to social engineering exposures, which could leave businesses with significant gaps in their insurance programs.

Further complicating matters are misconceptions over whether social engineering is covered under standard crime policies or cyber insurance. In fact, most crime forms today do not cover social engineering that results in a victim voluntarily parting with money. Over the past few years, underwriters have tightened policy wordings.

Coverage Misconceptions

One of the complexities for retail agents and brokers and their insureds is that two different coverage forms may apply to computer-enabled financial losses – crime policies and cyber policies.

Standard crime insurance policies contain two applicable provisions – a computer fraud clause that applies to the theft of money, securities or property by using a computer to make an fraudulent transfer from the policyholder to another person or location, and a funds transfer fraud provision that applies to theft of money and securities via fraudulent instruction to a financial institution to transfer funds. On the other hand, cyber insurance responds to losses arising from the theft of data. Social engineering muddies the waters because it often results in the voluntary transfer of funds or data.

Courts that have ruled on coverage disputes involving cyber crimes have distinguished between unauthorized funds transfers and transfers that are made voluntarily even though they are prompted by fraud. In general, voluntarily parting with funds, as occurs in social engineering, has been deemed outside the scope of insuring agreements in traditional crime policies and therefore not covered.[2]

Insurance companies that underwrite social engineering risks treat this peril differently. Some offer endorsements for social engineering for additional premium, while others include the coverage. Still others provide full limits for social engineering losses, while other underwriters impose sublimits. Some insurers condition coverage on attempts to authenticate requests for funds transfers, such as "callbacks" or verification using an alternate means of contact (for example, e-mail if the request comes via telephone). Crime policies presuppose the existence of internal controls to mitigate loss; crime insurance is not designed to substitute for a lack of such controls. Cyber liability policies are designed to respond to losses arising from the theft of data, such as employee or customer records. An employee who bypasses controls, believing a fraudulent request to be genuine, may unknowingly create a loss that standard crime and cyber policies will not cover.

To avoid coverage gaps and to ensure that crime and cyber exposures are properly insured, retail agents and brokers should consult a wholesale partner with extensive experience and close relationships with leading underwriters. Social engineering risk is continuing to grow, and navigating the dynamic insurance marketplace requires a knowledgeable guide.

Examples of Social Engineering

An early example of social engineering is the legend of the Trojan Horse, which was built by the Greeks and offered as a gift honoring the Goddess of War to the City of Troy during the Trojan War in the 12th Century B.C. Hiding inside the horse were Greek soldiers, who opened the city gates and let in the Greek army, which attacked Troy. Today, the term Trojan Horse is applied to deceptive software that appears benign but is designed to cause damage or steal information.

Below are a few examples you may have read about in the news:

- Ubiquiti Networks of San Jose, California, reported that it had been duped out of more than $40 million by criminals using employee impersonation and an outside entity to request fraudulent wire transfers. Ubiquiti's fourth-quarter filing indicated it may not have insurance coverage for the loss.[3]

- Ameriforge Group of Houston, Texas, sued its cyber insurer after the insurer denied a claim to recover $480,000 lost in a fraudulent funds transfer. The funds were requested by someone impersonating Ameriforge's CEO, communicating in e-mail that the money was owed to a third party conducting due diligence on a foreign acquisition. The insurer denied the claim because it said the policy required the forgery of a financial instrument.[4]

- The chief financial officer at Certified Transmission in Omaha, Nebraska, was nearly conned into making a fraudulent $98,000 payment after hackers spoofed his CEO's e-mail account. The attempted fraud, which failed because the CFO went to see his boss about the request, used a false domain that at a glance looked like his company's.[5]

A couple of recent examples our brokers have encountered:

- A corporate accounting department staffer, receiving a call from an overseas vendor inquiring about late payment, discovered that an unknown person had posed as the vendor, providing new instructions for wiring funds. The vendor learned that its own systems had been hacked, enabling the thief to send false but authentic-looking invoices. The loss totaled more than $300,000.

- A private company experienced executive impersonation in a scam that tricked the controller into arranging a large wire transfer to satisfy an overdue invoice. The scammer had hacked the company's e-mail and sent the request from the e-mail account of the CFO, who was out of town. Although the controller questioned the payment, a follow-up email was sent assuring the controller that authority had come "from the highest levels" of the organization. The fraud was not discovered until the CFO returned and the controller discussed the transfer, which the CFO did not authorize. Investigators suspect that hackers monitor executive movements and track e-mails to make fraudulent requests appear legitimate.

Social Engineering Lingo

Executive/Supplier Impersonation. Also known as business e-mail compromise, this sophisticated fraud targets businesses that work with foreign suppliers or regularly make wire transfer payments. The scam uses social engineering to hack legitimate e-mails or convince victims to make fraudulent wire transfers. The Federal Bureau of Investigation says that losses from this type of scam have increased 1,300% since January 2015, exceeding $3 billion.[6]

Pretexting. This type of scam uses impersonation, such as a bank executive or tax collector, to convince a target to share personal information, such as account numbers or passwords. Pretexting attacks require perpetrators to conduct research on potential victims.

Phishing. This form of attack is similar to pretexting but generally conducted on a wider scale. It uses e-mail or malicious websites to gather personal information by posing to be a trusted organization, such as a retail store, credit card company or charity. Variants of this tactic are called vishing, in which phishing is conducted over the phone, and smishing, which involves text messaging.

Spear Phishing. These attacks appear to be from a person or business known to the target. They typically entice the target to click on links or open attachments, which activate malicious software.

Endnotes

1. In a survey by European security technology firm Balabit, more than 70% of IT experts said social engineering using employees inside target organizations was a greater risk than automated hacking attempts. Gaining insider access through social engineering has become popular because it is easier and faster than using malicious code to break through cyber security defenses, the study found.

2. The U.S. District Court for the Southern District of Indiana ruled in favor of the insurer in a 2006 coverage dispute involving a standard crime policy and a social engineering loss at a foreign subsidiary.

3. Ubiquiti Networks announced it was the victim of a business e-mail compromise scam in 2015. Its costs related to this loss were estimated to exceed $46.7 million.

4. Ameriforge sought coverage under its $3 million cyber insurance policy, which had a $100,000 deductible. Its insurer denied the claim, saying the fraudulent transfer of funds was not due to the forgery of a financial instrument.

5. Certified Transmission avoided the social engineering scam because its CFO questioned certain aspects of the e-mail communication. The dollar amount of the requested transfer, however, did not raise his suspicions because that was not an unusual transaction for the company.

6. According to the FBI, business e-mail compromise scams have been reported by victims in all 50 U.S. states and in 100 countries, ranging from small businesses to large corporations.

For more information, contact your CRC, CRC Swett or SCU broker.
To find a conveniently located broker visit us on the web at:
crcins.com, crcswett.com or scui.com.