Fusco Orsini & ASSOCIATES INSURANCE SERVICES

Coverage for Social Engineering Attacks (Crime vs. Cyber Insurance)

In the context of cybersecurity, social engineering refers to a cyberattack method in which a cybercriminal preys on key human behaviors (e.g., trust of authority, fear of conflict and promise of rewards) to obtain unwarranted access to victims' technology, funds or data. These attacks can be deployed through various tactics, such as digital impersonation, deceitful messages or malware. Social engineering attacks have become a significant threat for all levels of businesses across industry lines; after all, anyone can be targeted in these incidents—including entry-level workers, managers and CEOs.

To combat social engineering exposures, some businesses have sought risk transfer in the form of insurance. However, they may encounter challenges when trying to find coverage for social engineering attacks within traditional crime or cyber insurance policies. As such, it's important for businesses to have a clear understanding of coverage options for these incidents.

This article provides more information on social engineering attacks, outlines coverage considerations for such incidents and offers additional mitigation measures for businesses to implement.

Social Engineering Explained

In a social engineering attack, a cybercriminal utilizes a number of manipulative tactics to lure their target into performing actions that they normally wouldn't—namely, sharing confidential details (e.g., login credentials or company data) and granting access to funds or technology. Some common social engineering attack methods include:

- **Phishing**—This technique involves cybercriminals leveraging fraudulent emails to trick recipients into providing sensitive information, clicking malicious links or opening harmful attachments. In order to make their emails appear genuine, cybercriminals will often impersonate trusted sources (e.g., a co-worker or well-known organization) and feign a sense of urgency to rush victims into acting. In addition to traditional phishing, cybercriminals may also attempt to manipulate victims over text messages or phone calls (known as smishing and vishing, respectively). Further, cybercriminals may specifically target CEOs with more personalized emails in order to obtain high-value data or financial resources (known as whaling).
- **Baiting**—Through this strategy, cybercriminals make false promises to victims to persuade them into sharing information or downloading malware. These false promises may appear in the form of fraudulent pop-up advertisements or deceitful online promotions. For example, a cybercriminal may use a false advertisement for a free movie download to trick their target into installing a virus on their device.
- **Business email compromise (BEC)**—Such a technique refers to a cybercriminal posing as a business executive for financial gain. Cybercriminals generally deploy BEC scams via email by creating fake accounts for business leaders and using deceiving messages to trick other employees into transferring money, divulging financial data or changing banking details.

Regardless of attack technique, a cybercriminal typically utilizes social engineering to commit fraud against another party, such as the target's financial institution(s), employer or company stakeholders. Specifically, a cybercriminal may launch a social engineering attack in an attempt to get their target to wire funds, permit access to workplace networks and intellectual property, divulge sensitive information regarding their employer's customers or send fraudulent invoices to vendors.

The consequences of social engineering incidents can be substantial. According to recent research from the FBI, these attacks cost impacted businesses an average of $130,000 in lost funds and compromised data. With this in mind, it's vital for businesses to secure proper coverage to protect against potential losses from social engineering attacks.

Coverage for Social Engineering Attacks

While some businesses have looked to their traditional crime and cyber insurance policies to cover losses stemming from social engineering attacks, these policies may not offer adequate protection for such incidents. Generally, the level of coverage that these policies can provide for social engineering attacks (if any) will vary based on the specific policy wording.

In particular, standard crime insurance policies usually cover losses resulting from "direct theft" of money, securities and other property by an employee or contractor within a business, such as a dishonest employee intentionally hacking workplace technology and wiring company funds into their personal bank account. Yet, social engineering attacks that involve honest employees being tricked by cybercriminals into transferring company funds to external accounts would likely not qualify as direct theft, thus excluding these incidents from coverage. Furthermore, some crime insurance policies exclude losses stemming from cyber incidents altogether.

In the scope of cyber insurance, traditional policies generally offer coverage for losses stemming from targeted system breaches and technology failures. However, social engineering incidents often don't involve these elements, as employees are tricked into openly participating in the attacks. Consequently, some cyber insurance policies may also exclude these incidents from coverage.

Nevertheless, it's important to note that some court cases have ruled in favor of policyholders utilizing traditional insurance policies to protect against social engineering losses. For example, in the 2022 case of *Ernst and Haas Management Company Inc.* (the policyholder) *v. Hiscox Inc.* (the insurance carrier), the 9th U.S. Circuit Court of Appeals ruled the policyholder was entitled to coverage under a standard crime insurance policy for losses resulting from a social engineering incident, qualifying the incident as direct theft.

Despite the results of this particular case, businesses should still consider purchasing additional, specialized coverage to ensure sufficient protection for social engineering losses. Primarily, social engineering insurance can be leveraged as an endorsement on either a traditional crime insurance policy or a standard cyber insurance policy, with specific coverage capabilities depending on the nature of the attack and type of fraud involved. However, some carriers may prefer to provide this endorsement solely on crime insurance policies, seeing as these policies can be better positioned to protect against first-party losses (including those resulting from social engineering incidents) than their cyber counterparts.

In addition, businesses should consider utilizing the same carrier for both their crime and cyber insurance policies. This practice can make it easier to identify potential gaps or overlaps between the two forms of coverage, especially as it pertains to protection for social engineering losses. Further, having the same carrier for both policies can help foster open communication between underwriters, establish suitable policy limits and streamline the claims process. Altogether, using the same carrier for crime and cyber insurance can help businesses maintain effective coverage tailored to their unique risks and exposures.

Additional Mitigation Techniques

Apart from securing proper coverage for losses resulting from social engineering attacks, it's also critical for businesses to take steps to prevent these incidents and minimize their impact. Here are some mitigation techniques that businesses can implement:

- **Conduct employee training.** First, businesses should educate employees on social engineering and how it could affect them. Additionally, employees should be required to participate in routine cybersecurity training on social engineering attack detection and prevention. This training should instruct employees to:
  - Watch for social engineering tactics in emails, texts and calls (e.g., lack of personalization, generic phrasing and urgent requests).
  - Refrain from interacting with emails, texts or calls from unknown or suspicious senders.
  - Avoid clicking links or downloading applications provided within emails or texts.
  - Never share sensitive information online, via text or over the phone.
  - Utilize trusted contact methods (e.g., calling a company's official phone number) to verify the validity of any suspicious requests.
  - Report any suspicious emails, texts or calls to the appropriate parties, such as a supervisor or the IT department.
- **Implement access controls.** Another method for limiting social engineering exposures is to use access controls. By allowing employees access to only the information they need to complete their job duties, businesses can reduce the risk of cybercriminals compromising excess data or securing unsolicited funds amid social engineering incidents. To further protect their information, businesses should consider leveraging encryption services and establishing secure locations for backing up critical data.
- **Utilize proper security software.** Lastly, businesses should make sure all workplace technology is equipped with adequate security software. In some cases, this software can halt cybercriminals in their tracks, stopping fraudulent messages from reaching recipients' devices and rendering harmful links or malicious applications ineffective. In particular, workplace technology should possess antivirus programs, spam detection systems, email filters, firewalls, message blocking tools and multifactor authentication capabilities. This security software should be updated as needed to ensure effectiveness.

Conclusion

In summary, social engineering attacks are a notable cyberthreat for businesses of all sizes and sectors, making proper prevention and protection measures increasingly vital. By understanding social engineering tactics, securing adequate coverage and implementing effective mitigation techniques, businesses can successfully safeguard themselves against these incidents. For additional insurance guidance and solutions, contact us today.