AMWINS®

How Cyber and Crime Insurance Policies Respond to Social Engineering

In today's digital world, the prevalence of social engineering attacks continues to be a risk across industries. From title agents handling multi-million-dollar wire transfers to a small contractor virtually without a network, no sector is immune from the sophisticated tactics of cybercriminals. As these bad actors continually appear to be ten steps ahead of standard controls, traditional insurance policies struggle to keep pace with the evolving threats.

CONTACT

To learn more about how Amwins can help you place coverage for your clients, reach out to your local Amwins broker.

LEGAL DISCLAIMER

Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions.

Please refer to your policy for the actual language.

Courtesy of Amwins Group, Inc.

The rising threat of social engineering

Social engineering, a form of deception used to manipulate individuals into divulging confidential information or inducing fraudulent monetary transfers, has become one of the most frequent causes of financial loss. Other terms for social engineering within the insurance industry include Cyber Crime, eCrime, Funds Transfer Fraud, Cyber Deception and Impersonation Fraud. This type of fraud involves convincing employees to transfer money or sensitive data under false pretenses. Over the past decade, social engineering has evolved from rudimentary email scams to advanced tactics including deep fakes and real-time impersonation.

One of the most alarming developments is the use of AI technology to mimic the voice or appearance of senior executives, tricking employees into authorizing significant financial transactions. For instance, in a **recent high-profile case**, an AI-generated video was used to deceive an employee into transferring $25 million, believing they were interacting with their CEO. This incident underscores the urgent need for robust insurance coverage that addresses these sophisticated scams.

Cyber insurance and social engineering

Cyber insurance has traditionally focused on protecting against data breaches, ransomware attacks and run-of-the-mill social engineering where, for example, an accountant receives a wire transfer request purportedly from the CEO. However, as social engineering attacks have evolved, cyber policies have had to adapt. These policies now need to address various segments of social engineering, including impersonation fraud where attackers mimic insureds to induce third party clients or vendors to illicitly redirect funds.

Coverage options for social engineering or cyber depiction in cyber insurance can vary significantly. Some key considerations include:

- **Impersonation fraud/phishing:** This coverage extends to scenarios where attackers impersonate the insured or their clients to fraudulently obtain funds without an initial system breach. Not all carriers offer this coverage, and when offered limits can be lower when compared to other types of cyber risks.
- **Other property losses:** Unlike traditional coverage that focuses on monetary loss, some policies now include provisions for losses involving physical property or inventory. This broader approach helps address cases where goods are shipped as the result of fraudulent requests.
- **Authentication Provisions:** *see Crime section below*

Crime insurance and social engineering

Crime insurance, particularly within professional lines, has also adapted to the rise of social engineering. Traditionally focused on more straightforward crimes such as theft and fraud, crime policies are now adapting to the nuances of modern scams.

Key aspects to consider in crime insurance include:

Coverage for social engineering: Crime insurance policies need to clearly define coverage for social engineering losses, which may involve fraudulently induced transfers or other deceptive practices.

Client funds: One significant gap in crime insurance is coverage for client funds. Some insurers are beginning to offer endorsements that extend coverage to include client funds lost due to social engineering, but this is not universally available. For instance, a wholesale broker may place a $350,000 property policy for a retail partner. After a bad actor monitors the retail broker's email, they impersonate the wholesaler and direct the retailer to send payment to a fraudulent account. The crime insurer then reimburses the lost funds up to the sublimit for client funds once the fraud is discovered.

Callback and authentication provisions: In crime policies, as with cyber insurance, it's important to be cautious of provisions related to callback and authentication procedures. These will often limit coverage for social engineering losses. When possible, it's best to avoid or restrict these provisions, as policies that include authentication provisions will require insureds to demonstrate additional measures to ensure the policy will respond adequately to the incident.

Preparing for unseen risks

A recurring theme among businesses, especially those not traditionally exposed to cyber risks, is underestimating the need for social engineering coverage. Contractors, for example, have historically been considered low risk in terms of cyber exposure. However, this perspective is rapidly changing as social engineering incidents among non-IT contractors are becoming more frequent. The rise in claims among these sectors is forcing brokers to rethink how they assess risk.

In some cases, businesses might transfer money to an account they believe is legitimate for weeks or even months, only to realize much later that they've been scammed. This kind of exposure is particularly high in industries such as attorney, real estate and title firms where the volume of high-dollar wire transfers can add up quickly, resulting in claims well beyond typical coverage limits.

For these sectors, social engineering insurance is not just a "nice-to-have"—it's essential. However, many carriers don't even offer this coverage for certain industries, making it crucial for brokers to find the right markets that cater to these high-risk classes.

Takeaway

As social engineering attacks continue to evolve, companies must ensure that their insurance policies provide comprehensive protection against these sophisticated threats. Both cyber and crime insurance should address the nuances of modern fraud, including deep fake technology and impersonation scams. Businesses should carefully review their insurance policies, consider endorsements for client funds and other property losses.

When discussing social engineering policies with clients, it's important to emphasize the value of internal controls and training that some cyber policies can offer. These can include modules on best practices to help mitigate not only social engineering risks but also broader cyber and crime exposures. Many businesses underestimate their vulnerability until it's too late and these cyber-attacks have only gotten more sophisticated. Even with comprehensive controls in place, human error remains a critical vulnerability that scammers exploit. This occurs to companies of any size – including both Google and Meta. In 2019, **scammers used phishing emails** to steal over $100 million from these giant firms.

Having the right insurance coverage is not just a matter of compliance, but a crucial component of a company's risk management strategy. By understanding the complexities of social engineering and selecting appropriate insurance coverage, retailers can help their clients be better protected against the financial and reputational damage caused by these sophisticated threats. Partnering with a specialist wholesale broker can help you navigate evolving cyber risks and coverage solutions.

We help you win

With a web of evolving threats, the best defense is a good offense. Amwins has cyber and crime insurance expertise, proprietary enhancements, industry-leading data and analytics capabilities and access to international capacity to help ensure your clients are well protected.

Amwins has also established preferred pricing agreements with industry-leading cyber security service providers that can help insureds improve their risk profile while better protecting their businesses against a broad range of cyber threats, including social engineering. Contact your Amwins broker today.

Insights provided by:

- Matt Athey, VP, Amwins Brokerage
- Charles Grodecki, EVP. Amwins Brokerage