AMWINS

Evolving Social Engineering Tactics Raise the Stakes for Cyber Coverage

Chances are your clients have made significant investments in technology-based controls to defend against cybercrime. However, as the saying goes, "A chain is only as strong as its weakest link." The unfortunate reality is that the human link in the security chain is the most vulnerable—and therefore the one most targeted by cybercriminals.

Reports show that **98% of cyberattacks involve "social engineering"** — a tactic where criminals prey on human emotions and habits to deceive people into divulging passwords, account details and other sensitive information that make systems open to attack and put your clients at risk. Managing social engineering risk involves a layered strategy of system controls, employee training and insurance coverage.

CONTACT

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

LEGAL DISCLAIMER

Courtesy of Amwins Group, Inc.

New tactics increase risk

Social engineering predates cybercrime. Fraudsters have long preyed on human fear and vulnerability, using impersonation and other techniques to steal money and property. But in the cyber world, social engineering became both easier and more lucrative. Your clients are no doubt familiar with some of the most common types, such as phishing, and have — or should have — already taken steps to combat it.

Unfortunately, cyber criminals continue to evolve their tactics, and new technology has increased the sophistication of social engineering attempts. **The FBI recently issued a warning** to both businesses and individuals to be aware of the escalating threat posed by cyber criminals utilizing artificial intelligence (AI) tools in attacks.

AI is helping scammers create extremely convincing and targeted messages, including voice and video cloning that impersonates coworkers, supervisors or other trusted individuals, all with the goal of obtaining sensitive information or authorizing fraudulent transactions.

Risk mitigation

Technology controls play a vital role in defending against social engineering attacks. Multifactor authentication (MFA) has become the required standard from underwriters in the cyber insurance marketplace.

Requiring two (or more) authentication methods makes it more difficult for cyber criminals to acquire all the components necessary to access a system. However, preventing cyber criminals from obtaining any authentication component is the best defense.

Training employees is essential in prevention by helping strengthen the "weakest link." The FBI recommends several areas where both the human and technology **components can be improved in an AI world**, including more effective MFA strategies, email handling and overall authentication strategies.

Coverage solutions

Insurance is also a key part of risk mitigation and insureds have several coverage options for social engineering exposure, including a crime, cyber liability, or stand-alone social engineering policy. There are considerations to be aware of when reviewing policy wording.

Crime policies can contain computer fraud or funds transfer fraud insuring agreements. However, social engineering may involve a “voluntary” transfer of information or funds. There can also be issues covering third-party funds held by the insured as well as limitations related to the methods used by the fraudsters.

Cyber liability policies are generally designed to respond to security breaches and related expenses; however, social engineering losses often occur without penetrating the organization’s network. Also, some cyber policies apply sublimits to social engineering coverage.

There is wide variability among cyber and crime forms in the marketplace, so careful examination is required to compare coverages.

Stand-alone social engineering solutions may provide the best solution, offering protection specifically for loss resulting directly from being duped into transferring money or securities in good faith reliance upon a telephone, written or electronic instruction purportedly from a client, vendor, or employee of the insured. Stand-alone insurance solutions can also be extremely helpful for providing additional capacity for social engineering losses.

Partner with a leader in cyber and crime insurance

Amwins has cyber and crime insurance expertise, industry-leading data and analytics capabilities, and access to stand-alone social engineering solutions as well as 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. **Learn about our cyber service partnerships here**.