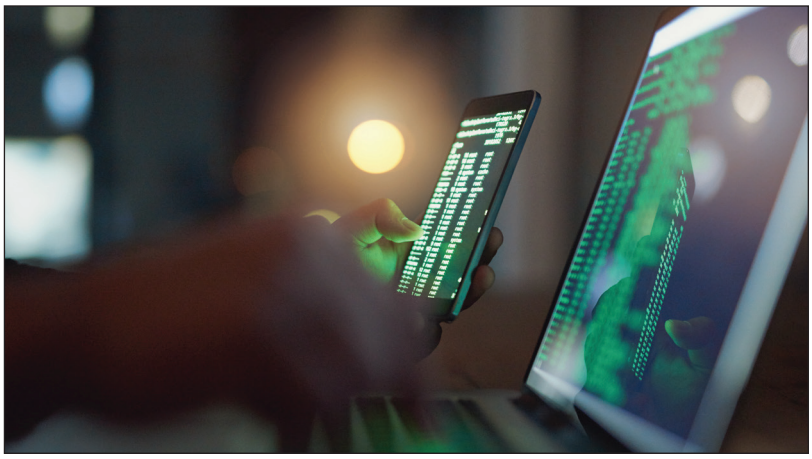
INSIGHTS
RISK & INSURANCE

Cyber Thieves Are Robbing You in New Ways. Will Your Insurance Provide Protection?

Nationwide®

Social engineering, phishing and crypto-currency burglary all represent evolving methods of theft that challenge traditional crime and cyber policies.



Theft is not a new threat. But it is taking on new forms in an increasingly digital world.

Cyber thieves can infiltrate organizations and execute fraud in any number of ways — through a phony email or phone call, a corrupted link, or by targeting vulnerable digital currency, to name just a few.

Businesses are reporting more security breaches and incidents of cyber fraud than ever before. According to Kroll's 2018 Global Fraud and Risk Report, 84 percent of surveyed executives reported that their company experienced at least one instance of fraud in the previous year, while 86 percent also said their company experienced a cyber attack involving data theft.

Both of those percentages represent all-time highs.

As the frequency and nature of these incidents increase and evolve in complexity, creating insurance solutions to help companies recoup their losses resulting from the ever-changing nature of the risk is an industry-wide challenge.

"Crime insurance traditionally would cover the direct loss of funds or property resulting from theft. Cyber liability insurance would take on the indirect consequential loss to a third party," said James Kardaras, Underwriting Director, Crime and Fidelity, Nationwide. "What they have in common is the use of a computer for illicit purposes, but there remain gaps and gray areas where much of cyber-related risk remains uninsured."

James Kardaras
Underwriting Director, Crime and Fidelity

Stand-alone cyber policies and traditional crime and fidelity policies alike traditionally did not protect against losses incurred by an employee willingly transferring funds to a fraudulent account, even if that employee was duped by hackers. The emergence of crypto-currency like bitcoin makes matters more complicated, since regulators and insurers are not sure how to qualify or quantify its value.

Social engineering, phishing, and theft of crypto-currency all represent evolving methods of theft that muddle the traditional definitions of fraud and challenge traditional notions of how crime and cyber policies will respond to such losses.

Sophisticated Social Engineering

Social engineering fraud, also known as business email compromise, is often a focused and well-planned attack. In this case, the thief impersonates either a senior official within the target company, a vendor or a customer, emulating their style of speech from behind a fake email account.

In the phony email, the impersonator directs an employee to send valuable data or to wire a sum of money to an external account.

"Employees want to do well, either by pleasing the boss or pleasing the customer, and if the email conveys a sense of urgency, the employee may be more likely to bypass typical verification protocols to complete the request. By the time the mistake is uncovered, it's usually too late to stop the transaction or even trace where the data or the funds have gone," Kardaras said.

Today, social engineering schemes have evolved to include the fraudulent transfer of tangible property, wherein the perpetrator, posing perhaps as a sales executive attending a conference, asks an employee to send or reroute a shipment of goods to the show site or a nearby hotel. The thieves then intercept the shipment and make off with the goods.

"If an employee willfully completes these requests, a traditional crime and fidelity policy would not recognize this as theft and wouldn't provide coverage," Kardaras said. "Cyber policies would likely not respond either, since there has been no breach of the company's network."

Financial Phishing

Like social engineering, phishing schemes involve scammers posing as trustworthy third parties — typically a bank. But rather than inducing an internal employee to transfer funds or data, phishing emails lure recipients to click on a corrupted link under the guise that they need to update or verify their user information.

These links have served as vehicles to infect companies' networks with malware or ransomware, but increasingly they redirect employees to copycat websites where they enter private information like company account numbers, which are then used to access funds directly.

"Financial phishing, which seeks a more direct and immediate payout, now accounts for more than 50 percent of all phishing attacks," Kardaras said.

Attacks specifically targeting the financial institutions themselves are also becoming more common. Malevolent links sent via a phishing email can help hackers gain access to an employee's systems.

"This technology enables hackers to gain remote access to employees' computer terminals at banks, follow their movements, and track what type and what volume of transfers they conduct each day," Kardaras said. They can then mimic those actions to make fraudulent transfers into their own accounts, but of a volume and size small enough not to raise any red flags."

Crime insurance could potentially respond to protect insureds from these losses, if the risks are identified, underwritten to, and the policy wording is drafted accordingly. One problem is that many victims don't register the fraud until it becomes significant. It is estimated that banks across Europe and the U.S. have lost hundreds of millions through these unauthorized transfers.

Crypto-Currency Theft

The emergence of bitcoin and other virtual currency makes recovering from cyber theft even more complicated. Crime and fidelity policies will typically cover the loss of money, securities or property, but virtual currency does not fall within traditional definitions under these insurance policies.

"If an organization using these virtual currencies suffers a loss of virtual currency, depending on the policy's definitions, it is possible that such a loss would not be covered if it is not included within the policy's definitions of money, securities or property," Kardaras said.

Additionally, the fluctuating value of bitcoin would make it difficult for underwriters to evaluate the risk associated with a bitcoin store, and to determine exactly how much a claim is worth in the event bitcoin is stolen. Nonetheless, it is estimated that more than $1 billion worth of virtual currency has been stolen over the past decade.

As bitcoin grow more legitimate and widespread, so likely will the corresponding risk of crypto-currency theft.

Bridging the Shortfall of Coverage Solutions

Traditional crime and fidelity policies were crafted by the Surety and Fidelity Association of America in the 1990s, and much of their language has not been updated to reflect modern-day risks.

Various carriers have attempted to address and clarify the gray areas in crime and cyber coverage via exclusionary or enhancement endorsements attached to the policy. A cyber policy may typically exclude, for example, losses incurred via fraudulent funds transfer stemming from a social engineering scam. Similarly, traditional crime policies may explicitly exclude any coverage for digital currencies.

These new endorsements and policy wording providing affirmative coverage for these evolving risks seek to seal the gaps and eliminate the confusion emanating from the complex and rapidly-developing cyber exposures.

"For commercial firms, Nationwide may offer protection for fraudulently-induced funds transfers resulting from social engineering scenarios where such losses would not be picked up by traditional policies," Kardaras said.

"For financial institutions, we offer a separate, computer crime policy form updated with language that may protect businesses from email compromise as well as any unauthorized access to company funds resulting from a virus or malware. Protection for crypto currency losses are underwritten on a case-by-case basis."

In recognition of the complexity and challenges that the growing cyber-theft landscape presents, Nationwide's fidelity and cyber liability teams work together to offer insureds complementary coverage.

"We don't work in silos," Kardaras said. "We work hand in hand to offer coverage that meets the spectrum of our customers' needs, from first-party crime to computer fraud and third-party liability and everything in between."

To learn more, visit https://mls.nationwideexcessandsurplus.com/fs/products/commercial-crime/.
