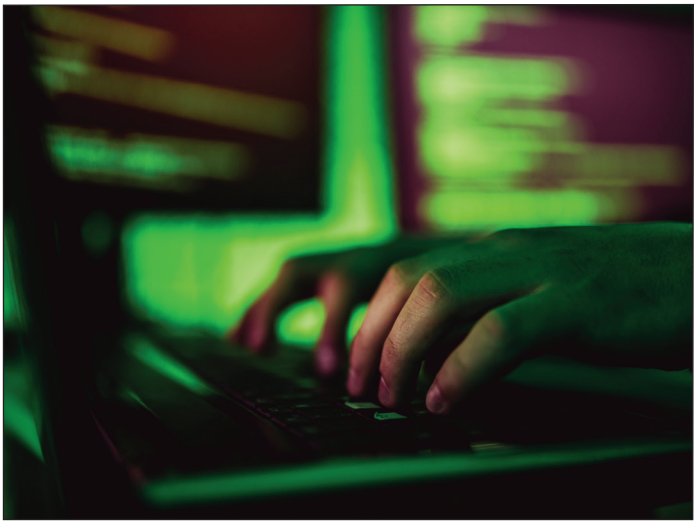
RISK & INSURANCE
Affiliated with THE INSTITUTES
Sponsored Content by Nationwide

3 Things Risk Managers and Brokers Need to Review Before Securing Their Crime & Fidelity Policy

There are several areas to review before picking the right crime and fidelity policy, from growing risk trends to the language provided in the form.

By: Nationwide | June 2022



When an employee steals from their company, what should the employer do?

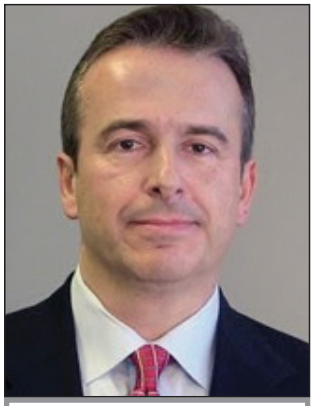
What even the most proficient risk professionals might not know is that employee theft can affect businesses of any type and size. The U.S. Department of Commerce reports companies lose $50 billion each year to employee theft, and such activity causes one in three bankruptcies. And that's not to mention the new ways employees are accessing funds and other items.

"Traditionally, the biggest Crime & Fidelity exposure has been embezzlement by employees. This has been employee dishonesty. For example, employees setting up fraudulent accounts and having the company pay them to accounts that were not valid, or overpay," said James Kardaras, Senior Director of Crime & Fidelity at Nationwide. "But now, electronic crime [criminal activity involving the use of computers or electronic means, to illegally transfer funds or steal, change or erase electronically stored data] is sharply on the rise."

Given these expanding criminal trends, risk professionals should be securing the protection of a comprehensive Crime &Fidelity policy. But what exactly should they be looking for in their coverage and in their underwriter? Before investing in a Crime & Fidelity policy, it is essential that insureds consider the following.

1) Know the Trends: How Are Crimes Being Conducted?

Current advances in technology allow bad actors to exploit a very dangerous tool: the Internet. Enabled on virtually every computer and smart phone, the Internet provides criminals with round-the-clock access to



James Kardaras, Senior Director of Crime & Fidelity, Nationwide

electronic data, resulting in rapidly increasing losses to insureds.

"When you have people outside the institution able to remotely access computers at a bank, for example, and divert funds, little by little, from the employee to other accounts outside the institution, you have this very real, very new risk that no one even thought about years ago," said Kardaras.

Social engineering is a noteworthy growing trend, as more bad actors are succeeding in their criminal enterprises using this approach. "Social engineering fraud, otherwise known as fraudulently induced funds transfers, occurs when a criminal assumes someone else's identity induces an individual within the institution to transfer or wire funds to an unauthorized account controlled by the embezzler," Kardaras explained.

"Criminals can assume your identity using information readily available on social media, whether on LinkedIn, Twitter, Facebook or Instagram, because the more public information about you that's out there, the more easily your identity can be stolen," he said. "People purport to be an employee and they're not. People purport to be a vendor and they're not. People purport to be a customer or a client and they're not."

Sophisticated criminals continue to up the ante even further. Using "deepfake" technology, criminals have the technology to send a fake but flawless video messages from a company's president or CFO giving authorization to transfer funds.

2) Know Your Needs: What to Look for in a Crime & Fidelity Policy

Up-to-date forms are a must. "Some computer crime policies date back to the '90s as a base form. But a lot has changed since then, both with the technology and the tools criminals use to defraud insureds," Kardaras explained. A comprehensive Crime & Fidelity policy should include modernized language that provides the insured protection for emergent risks.

Risk managers and their brokers should seek to procure a policy that provides coverage for the different types of employee theft – from electronic crimes to social engineering fraud.

In addition, because such criminal activities often extend into ransomware and demands for cryptocurrency payment, risk managers and brokers should seek a Crime & Fidelity policy that addresses those threats in coordination with coverage that may be provided for same under the insured's cyber policy.

Additionally, criminal hackers commonly try to extort their victim when demanding ransom. "Insureds should therefore be cognizant of whether the Crime & Fidelity policy they are seeking to purchase provides coverage for extortion or alternatively contains an exclusion that would expressly preclude it."

3) Know the Strategies: How to Prepare Your Business

Risk professionals, when going to market for a Crime & Fidelity partner, should be proactive and already have certain controls in place to demonstrate they are a favorable risk to underwrite. Kardaras advised that when an insured knows their own exposures and can relay that to the carrier, the application and underwriting processes become that much smoother.

"The carrier needs to evaluate a full application, because they are covering internal exposures," Kardaras explained. "Insurers can't simply amass information about the company from public information; rather the company must set out the scope of the risk via the carrier's full application."

A full application likely poses the following types of critical questions: What internal risk controls are currently in place with regard to money, securities and other property? What authority do employees have to handle funds and up to what threshold? At what level is dual authorization required to release payment of funds?

With regard to larger firms, maintaining an internal audit department is key to being viewed as a favorable risk.

"If a large, sophisticated insured doesn't have an internal audit department, to me, that would be a non-starter for providing coverage," Kardaras said. On the other hand, "smaller firms that may not have the staff for an internal audit team," he added, "should be able to provide the carrier with a complete picture of how, and to what extent, fund requests from employees, vendors and customers are authenticated by the insured."

A final piece of the risk-ready puzzle can come down to how a potential insured trains its employees. Much like in the cybersecurity space, companies can train their employees to spot potential or attempted electronic crimes.

"Nationwide employs a questionnaire as a tool to help businesses become more aware of how well-trained their employees are," said Kardaras. "Phishing education and testing employees once a year on cyber readiness is an important element of mitigating their exposure. Our questionnaire asks about that training and evaluates the staff's preparedness for potential cyber crimes and attacks."

Partnering with the Right Kind of Experts

Once risk professionals become familiar with the Crime & Fidelity landscape, it's time to find the right coverage partner. That partner should be well-versed in the space, while also constantly and consistently evaluating the emerging trends to bring the best solutions to clients each day.

The Crime and Fidelity team at Nationwide prides itself on those very things.

The Crime & Fidelity business at Nationwide was developed to complement its established D&O liability, professional liability and cyber liability policies. Nationwide brought in Kardaras seeking to capitalize on his extensive and varied Crime & Fidelity background on both the brokering and underwriting sides. Kardaras has successfully employed this vast knowledge and experience, providing Nationwide clients with the Crime & Fidelity protection essential as criminal activity continues to rapidly grow and evolve.

"Nationwide's Crime & Fidelity team works closely with brokers and risk managers to provide real time information and terminology," Kardaras explains. "Our Crime & Fidelity team works in tandem with our cyber, D&O and Financial Institutions colleagues and we are well-versed on the potential overlapping risks and coverage solutions. We endeavor to be flexible and solution-oriented in our coverage. For example, if we straddle the border between cyber liability and computer crime, Nationwide will find a solution that provides our insureds with protection tailored to their needs."

To learn more, visit: https://www.nationwide.com/business/insurance/commercial-crime/.

About Nationwide
AM Best Rated A+ XV | S&P A+ | Fortune 100 Company
Products underwritten by Nationwide Mutual Insurance Company and Affiliated Companies. Not all Nationwide affiliated companies are mutual companies, and not all Nationwide members are insured by a mutual company. Home Office: One Nationwide Plaza, Columbus, OH. Nationwide, the Nationwide N and Eagle, and other marks displayed on this page are service marks of Nationwide Mutual Insurance Company, unless otherwise disclosed. © 2022 Nationwide Mutual Insurance Company.

&BrandStudio

This article was produced by the R&I Brand Studio, a unit of the advertising department of Risk & Insurance, in collaboration with Nationwide. The editorial staff of Risk & Insurance had no role in its preparation.