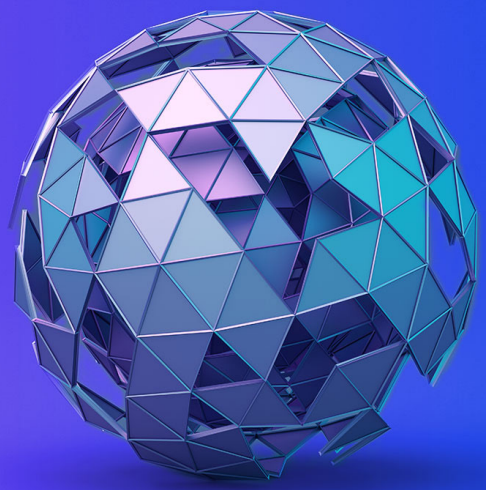
From cyber to fraud:

The evolving landscape of digital crime



Is it a cyber incident or a fraud investigation? The lines between cybercrime and fraud are increasingly blurring. For example, imagine this: Someone might break into your house (cybercrime) by pretending to be the delivery person (fraud). Bad actors are commonly leveraging digital identity-based attacks such as account takeovers, application programming interface (API) abuse, and social engineering as an entry point into a company's system. These types of incidents are generally not sophisticated, the risk likely won't ever fully be mitigated, and they simply act as the gateway for other malicious activities. It's what happens next, what a bad actor may use that pretense for, that defines what type of incident you're dealing with, the severity, and what your company's response should look like.

In traditional cyber events, persistence is often a key factor, as attackers may attempt to maintain access to compromised systems for extended periods to maximize their gains. Attackers may then aim for extortion, demanding a ransom in exchange for returning stolen data or preventing further damage. Destruction can also be a goal, as attackers might seek to disrupt operations or damage a company's reputation.

The reality is, from an attacker's point of view, these types of traditional attacks are starting to be more risky and less fruitful. Why? To start, there have been many recent global law enforcement actions disrupting and deterring bad actors in engaging in these kinds of malicious activity. Secondly, companies' investments in cybersecurity technology and talent are starting to pay off, raising the bar of difficulty for success. And lastly, when attacks are successful, the impact is less impactful as often companies have backups or are not interested in engaging with a bad actors.

In contrast, there has been a shift towards more sophisticated and hand-crafted schemes, moving away from commodity playbooks such as ransomware-as-a-service

Let's examine a few examples of these modern fraud-first types of incidents:

Click fraud

Beyond automating fake clicks on online advertisements, hackers have refined their techniques to target specific industries and campaigns. For instance, they might focus on political advertisements during election cycles to manipulate public opinion or on e-platforms to inflate product prices or create inflated royalty payments.

Process fraud

Organized crime groups have become increasingly adept at exploiting controls in complex business ecosystems. They might, for example, create fake invoices and divert funds to fraudulent accounts or manipulate supply chain or account payables processes. This may also involve sophisticated social engineering such as the use of deep fake video and/or audio.

Market manipulation

Hackers have not only manipulated cryptocurrency markets but also targeted confidential insider information, specifically around merger and acquisition activity, for financial gain.

API abuse

Attackers have become more sophisticated in their use of API vulnerabilities. They might exploit APIs to gain unauthorized access to sensitive data, such as customer information or financial records, which can be used for identity theft, fraud, or other malicious purposes.

What does this mean for you?

While cybersecurity expertise remains essential, it's no longer sufficient to address the multifaceted nature of modern digital fraud alone. This landscape demands a more comprehensive and integrated approach to risk management and is one reason we have started to see instances of the CISO reporting structure flow into the general counsel's office.

Organizations must foster strong collaboration between cybersecurity, legal, compliance, and business functions regardless of the incident type categorization. This interdisciplinary approach ensures a cohesive response to incidents, leverages regulatory frameworks, and addresses the broader business implications of fraud.