LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, DECEMBER 10, 2025
Published In Top White Collar Lawyers 2025 Supplement

Mitigating insider risk: Legal leadership in a new era of threats

Jennie Wang VonCannon

The year 2025 saw the rise of the use of artificial intelligence (AI) by nation-states to commit cybercrime against U.S. companies. Such efforts are ushering in a new era of insider threats.

In June 2025, the U.S. Department of Justice (DOJ) announced sweeping law enforcement actions targeting the fraudulent scheme of operatives of the Democratic People's Republic of Korea (DPRK or North Korea) who — aided by U.S.-based facilitators — posed as legitimate remote information technology (IT) workers to get hired by U.S. companies. As alleged by the DOJ, the perpetrators of the so-called "North Korean IT worker scheme" leveraged AI, including deepfake technology, to generate fake resumes, communicate with the U.S. companies, and conduct interviews convincing enough to get hired at the victim U.S. companies. Once on the inside, the DOJ alleges, the remote IT workers committed data extortion and exfiltrated the companies' proprietary and sensitive data.

The North Korean IT worker scheme exposes the modern landscape of today's cybersecurity threats. What is striking is not the efforts by a hostile nation-state to exploit the defenses of U.S. companies. Rather, it is the way the DPRK exploited what has become ordinary business activity since the COVID-19 pandemic, including virtual interviews and hiring remote workers. The victim companies believed they were hiring and sending company laptops to legitimate remote employees, when in reality the remote workers were malicious actors turned insiders. That these insiders worked in IT was particularly damaging from a data perspective because IT personnel often have administrative or other elevated privileges that can be exploited to a company's great detriment. Emerging technologies enabled North Korea to facilitate this scheme at scale.

Given the tactics that the DPRK used to infiltrate U.S. companies, it follows that a company's next major data breach may not come from an external malicious actor — they may already be embedded within the company and be able to breach the company's defenses from within. This type of insider threat showcases the growing sophistication of cyber threats, which necessitate that in-house legal teams take a leadership role in preventing, detecting, and responding to such threats.

The first step in any insider threat program is to identify the critical assets of the company — the "crown jewels" whose theft or compromise would cause significant legal, financial, reputational, and/or operational harm. These can include intellectual property or trade secrets, financial records or customer information. While it may be tempting to label "all of it" as critical, it is important to resist that urge because if all of the company's data is critical, then none of it is. Instead, consider classifying data in decreasing order of importance. This way the insider threat program can be tailored to the resources available at any given time. Some data or assets are protected by law or contracts (i.e., HIPAA or client confidentiality agreements) such that their exfiltration automatically exposes the company to liability. These classes of assets will be ranked higher on the criticality scale.

Jennie Wang VonCannon, *AIGP, CIPP/US, is a partner at Crowell & Moring LLP.*

Once "crown jewel" assets are identified, classify and label them to enable targeted protection and monitoring. To do this effectively, companies should create an inventory of all data, systems, and resources — and then map the personnel who have access to them. Since data is dynamic, track how information moves through your organization, including where it is stored and how it is transmitted both internally and externally. And keep these inventories and maps up to date as the data and business evolve.

Engage stakeholders across the company in this data protection exercise. Individuals from legal, IT, human resources, and the business units who "own" the critical assets should weigh in to avoid blind spots. A successful insider threat program also needs executive-level support to set a tone of compliance, particularly since the next step is to draft clear written policies governing the insider threat program, including the following:

Data access: limit access to sensitive information on a need-to-know basis or according to individuals' roles within the company;

Auditing and detection of data access violations: depending on the company's culture a level of transparency about how employees' data access will be logged and reviewed may be advisable;

Acceptable use: be clear about what users can and cannot do with their company computers and other technology;

Reporting suspicious behavior: because cyber attacks and data issues can be detected by many different types of people outside of the IT department, including third-party vendors, a clear method for reporting that information increases the company's visibility into vulnerabilities;

Consequences for violations of these policies; and

Departing employee protocols, including terminating their access rights.

Of course, training personnel on the policies is crucial both to provide notice and to obtain compliance with them. Finally, continuously assessing risk and monitoring the effectiveness of the policies is necessary to ensure protection of the critical assets.

Companies can fight fire with fire by leveraging technology to strengthen their insider threat programs. Advanced threat detection tools can detect anomalous behavior with respect to data. These include data loss prevention (DLP), user and entity behavior analytics (UEBA), and security information and event management (SIEM) tools.

While AI and other modern technologies may have supercharged malicious actors' ability to infiltrate and steal company data, companies can also use those same technologies to combat these efforts. The most effective insider threat programs will combine robust technological components with a transparent and supportive culture of compliance.