

Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 38 • NUMBER 6 • JUNE 2026

When Trusted Access Becomes a Threat: The *U.S. v. Linwei Ding* Conviction and Escalating Insider Risk

By Artie McConnell, Eric B. Gyasi and Om M. Kakani

On January 29 in San Francisco, former Google engineer Linwei Ding was convicted after trial of economic espionage and trade secrets theft for taking hundreds of Google's confidential documents on AI chip technology and using them to build a startup in China.

The verdict underscores a critical and escalating risk for companies that develop or handle high-value intellectual property: the insider threat.

Insider threats are increasingly sophisticated, avoid traditional perimeter-focused cybersecurity controls by using authorized access, and persist undetected for months, exposing organizations to massive data loss, severe economic and national security risks, and triggering significant regulatory, criminal and reputational consequences.

THE *DING* PROSECUTION: A CASE STUDY IN INSIDER CORPORATE ESPIONAGE

Linwei Ding was employed by Google as a software engineer beginning in 2019 and allegedly began uploading confidential company information to a personal cloud account between May

2022 and May 2023. At trial, federal prosecutors presented evidence that more than 1,000 unique files containing highly sensitive AI-related trade secrets were transferred outside of Google's internal systems. The trial evidence showed that the stolen information related to Google's AI supercomputing infrastructure, including technical details concerning Tensor Processing Units (TPUs), Graphics Processing Unit (GPU) systems, and networking components used to train and deploy large-scale AI models. Additionally, the government proved that, while still employed at Google, Ding secretly affiliated with and later founded China-based technology companies.

The trial highlighted some notable characteristics about the insider threat risk and corporate responses:

- *Insider threats can pose substantial challenges to companies and jeopardize core competitive advantages:* Prosecutors emphasized that the stolen materials allowed Ding to “skip huge parts of the design process” for an AI supercomputer, potentially undermining years of Google's R&D investments.
- *Insider threats are often subtle, gradual and often within the scope of an employee's authorized permissions:*

The authors, attorneys with Baker & Hostetler LLP, may be contacted at amcconnell@bakerlaw.com, egyasi@bakerlaw.com and okakani@bakerlaw.com, respectively.

Unlike external cyber intrusions, the alleged activity involved authorized access using routine credentials, internal systems and approved tools such as cloud storage. This type of conduct can persist for months without triggering traditional security alarms, demonstrating the limit of perimeter-focused cybersecurity strategies and the importance of monitoring how systems are used, not merely restricting access.

- *Trade secret theft is a national security enforcement priority for Department of Justice (DOJ):* The *Ding* case involved economic espionage charges, which require proof of intent to benefit a foreign government. As a result, where sensitive dual-use technologies are involved, failure to detect or respond to insider misconduct may expose companies to parallel investigations, compulsory process and reputational damage tied to broader political issues.
- *Detection and voluntary disclosure:* At trial, prosecutors indicated that Google detected anomalous activity and referred the matter to law enforcement. Notably, DOJ recently announced an indictment in *United States v. Ghandali et al.*, another insider scheme involving Google. As in *Ding*, suspicious activity was spotted and promptly reported to law enforcement, underscoring the critical role early detection and rapid reporting can play in protecting corporate trade secrets and enabling timely investigative action. In both matters, DOJ noted the company's proactive referral. This is the model DOJ has been explicitly encouraging per their revised Corporate Enforcement Policy, especially in national security matters.

AUTHORIZED ACCESS AS A CRITICAL VULNERABILITY

The *Ding* Prosecution Is Not an Isolated Event

The case closely parallels the high-profile conviction of Dr. Xiaorong (Shannon) You in the Eastern District of Tennessee for stealing proprietary BPA-free coating formulations valued at roughly \$120 million. Like *Ding*, You used her authorized access to transfer confidential materials to personal storage accounts and external drives with the intent to

launch a competing coating-technology venture in China with substantial financial assistance from the Chinese government.

Insider Threats Are Not Limited to Nation-State Actors

Different insider risk scenarios require different prevention and detection approaches and constant agility in control management. Defending against a nation-state actor quietly exfiltrating trade secrets may require robust data-loss-prevention controls, long-term behavioral analytics, and strong compartmentalization. In contrast, identifying an internal administrator who is financially motivated and willing to sell network access to a ransomware group may employ different tactics, such as monitoring for privilege misuse, sudden behavioral changes, and anomalous access patterns. Although both situations fall under “insider risk,” the motivations, tactics, and detection signals are fundamentally different—and effective programs recognize and tailor safeguards to each scenario.

The Active Recruitment of Insiders

Rising trends show that insider threats increasingly originate not just from internal dissatisfaction but from an active, coordinated external effort to convert employees into malicious collaborators. Cybercriminal groups are deliberately seeking out disgruntled, recently laid-off, demoted or otherwise dissatisfied workers and are directly contacting them across open platforms like LinkedIn as well as dark-web recruitment forums. These actors offer financial incentives tied to ransomware payouts or stolen-data sales, and often equip recruits with the tools, malware and technical support needed to carry out attacks. In some cases, criminal networks even embed operatives inside companies using falsified identities – meaning the threat landscape now includes both compromised insiders and externally placed infiltrators.

Building a Defensible Insider Threat Program

The *Ding* trial shows how companies that invest now in governance and monitoring are better positioned to detect warning signs early, respond decisively, and demonstrate to regulators and prosecutors that they exercised reasonable and responsible care. Potential controls companies can implement, based

on their analysis of potential insider threat risk, include the following:

- *Implement a formal insider threat program:* Organizations should maintain a documented and cross-functional insider threat program that integrates legal, compliance, HR, IT and security functions.
- *Access controls should be dynamic and contextual, not static:* Regular audits should assess whether employees' system access remains appropriate given their role, tenure and current projects. High-risk personnel – such as engineers working on core IP – warrant enhanced oversight.
- *Modern insider risk programs should evolve to combine technical telemetry with behavioral insights:* Companies need to combine technical measures (e.g., unusual download volumes, off-hours access, cloud uploads) with behavioral signals (e.g., undisclosed outside business activities, travel patterns inconsistent with job duties), which usually reflect a gradual escalation of suspicious activity. In the *Ding* case, prosecutors highlighted extensive data uploads to personal accounts over time – activity that sophisticated monitoring tools can flag.
- *Use data monitoring and anomaly detection:* Insider threats often use common tools present in the network environment. This tactic exploits trusted enterprise software and cloud sync tools, which are regularly not monitored for suspicious use. Without strong behavior analytics, this network activity can slip under the radar.
- *Develop audit trails and real-time alerts:* Companies should maintain persistent logging of file access and transfer actions, to include alerts for high-risk actions like exporting sensitive files or connecting unauthorized devices.
- *Perform risk assessments:* regular risk assessments for sensitive/high-profile projects involving

proprietary and competitive technologies are important for identifying vulnerabilities.

- *Crown jewel systems:* Companies should identify their “crown jewels” and implement systems with stricter access governance to protect them, including by using time-boxed, purpose-based access for these systems.
- *Enforce disclosure and conflict-of-interest obligations:* Cyber governance should anticipate external influence, incentives and conflicts, not just technical misuse. Outside employment, board roles and foreign business affiliations should be disclosed, clearly communicated and meaningfully enforced. Failure to detect or act on conflicts can significantly increase insider risk exposure. Governance programs should connect ethics, conflicts of interest, and cybersecurity controls and information – rather than treat each as a separate compliance silo.
- *Prepare for law enforcement and regulatory inquiries:* Escalation and government relations plans are essential. Early engagement with both in-house and outside counsel can help balance cooperation, employee rights and protection of corporate interests.

CONCLUSION

The *Ding* case serves as a cautionary example of how trusted insiders can allegedly exploit authorized access, and evade traditional perimeter-focused defense efforts, to inflict outsized harm – particularly in industries driven by cutting-edge technology and intellectual property. This case is a reminder that cyber governance is more than preventing outside hackers and is an example of the need to govern trusted access to a company's most valuable intellectual property across the entire cybersecurity loop. As enforcement authorities intensify their focus on national security risks, companies should treat insider threat compliance as a core enterprise risk, not merely a cybersecurity sub-issue.

Copyright © 2026 CCH Incorporated. All Rights Reserved.
Reprinted from *Intellectual Property & Technology Law Journal*, June 2026, Volume 38,
Number 6, pages 19–21, with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, www.WoltersKluwerLR.com



Wolters Kluwer