Armstrong Teasdale

May 13, 2026 • Advisory • www.atllp.com

NORTH KOREAN OPERATIVES INFILTRATE U.S. COMPANIES

WHAT IS HAPPENING

Over the past several years, reports have shown that North Korean operatives have infiltrated U.S. companies by posing as remote workers using deepfakes, social engineering, and AI tools. These operatives often work through "laptop farms" that host company-issued devices and allow remote access to corporate systems. Their activities can expose companies to sanctions violations, regulatory penalties, frozen assets, trade secret theft, data breaches, and extortion attempts involving stolen information.

HOW TO PREVENT THIS

Companies can reduce risk through coordinated cybersecurity, HR, and sanctions compliance controls, including stronger identity verification, tighter system access restrictions, continuous monitoring, and enhanced vendor and payment screening procedures.

- Require live, on-camera interviews and government-issued identification verification, where permitted by law.
- Independently verify prior employment, education, and professional credentials rather than relying solely on candidate-provided contacts.
- Use E-Verify and ensure third-party staffing agencies follow robust identity verification procedures.
- Apply continuous authentication and least-privilege access controls rather than relying solely on pre-employment screening.
- Restrict access from high-risk jurisdictions and limit the use of personal devices and external storage media.
- Implement and maintain endpoint detection and response tools to continuously monitor suspicious activity.
- Establish clear policies governing access to sensitive information, suspicious activity reporting, and remote work security.
- Send company equipment only to verified addresses or conduct additional verification for alternative delivery requests.
- Screen vendors, contractors, and workers against applicable sanctions lists and monitor for red flags such as VPN use, payment requests to third parties, refusal to appear on camera, or frequent bank account

PEOPLE

Brian E. Kaveney

Stewart G. Mayo, CIPP/US

SERVICES AND INDUSTRIES

Industrial Security and Security Clearance

changes.

- Avoid cryptocurrency payments and do not pay ransoms or extortion demands.
- Maintain relationships with law enforcement and be prepared to report suspicious activity promptly.

WHAT TO DO IF THIS HAPPENS

If it is discovered that an operative has infiltrated a company, immediately revoke system access, secure affected systems, and begin a cybersecurity investigation to determine the scope of access and potential data exposure. Take appropriate employment actions consistent with applicable law, preserve relevant evidence, and, if appropriate, notify law enforcement to mitigate potential sanctions and regulatory risks.