Published on *The National Law Review* https://natlawreview.com

FBI Warns of Hidden Threats in Remote Hiring: Are North Korean Hackers Your Newest Employees?

Article By:

Benjamin W. Perry

Tracey A. Kinslow

Zachary V. Zagger

The Federal Bureau of Investigation (FBI) recently warned employers of increasing security risks from North Korean workers infiltrating U.S. companies by obtaining remote jobs to steal proprietary information and extort money to fund activities of the North Korean government. Companies that rely on remote hires face a tricky balancing act between rigorous job applicant vetting procedures and ensuring that new processes are compliant with state and federal laws governing automated decisionmaking and background checks or consumer reports.

Quick Hits

- The FBI issued guidance regarding the growing threat from North Korean IT workers infiltrating U.S. companies to steal sensitive data and extort money, urging employers to enhance their cybersecurity measures and monitoring practices.
- The FBI advised U.S. companies to improve their remote hiring procedures by implementing stringent identity verification techniques and educating HR staff on the risks posed by potential malicious actors, including the use of AI to disguise identities.

Imagine discovering your company's proprietary data posted publicly online, leaked not through a sophisticated hack but through a seemingly legitimate remote employee hired through routine practices. This scenario reflects real threats highlighted in a series of recent FBI alerts: North Korean operatives posing as remote employees at U.S. companies to steal confidential data and disrupt business operations.

On January 23, 2025, the FBI issued another alert updating previous guidance to warn employers of "increasingly malicious activity" from the Democratic People's Republic of Korea, or North Korea, including "data extortion." The FBI said North Korean information technology (IT) workers have been "leveraging unlawful access to company networks to exfiltrate proprietary and sensitive data, facilitate cyber-criminal activities, and conduct revenue-generating activity on behalf of the regime."

Specifically, the FBI warned that “[a]fter being discovered on company networks, North Korean IT workers” have extorted companies, holding their stolen proprietary data and code for ransom and have, in some cases, released such information publicly. Some workers have opened user accounts on code repositories, representing what the FBI described as “a large-scale risk of theft of company code.” Additionally, the FBI warned such workers “could attempt to harvest sensitive company credentials and session cookies to initiate work sessions from non-company devices and for further compromise opportunities.”

The alert came the same day the U.S. Department of Justice (DOJ) announced indictments against two North Korean nationals and two U.S. nationals alleging they engaged in a “fraudulent scheme” to obtain remote work and generate revenue for the North Korean government, including to fund its weapons programs.

“FBI investigation has uncovered a years-long plot to install North Korean IT workers as remote employees to generate revenue for the DPRK regime and evade sanctions,” Assistant Director Bryan Vorndran of the FBI’s Cyber Division said in a statement. “The indictments … should highlight to all American companies the risk posed by the North Korean government.”

Data Monitoring

The FBI recommended that companies take steps to improve their data monitoring, including:

- “Practice the Principle of Least Privilege” on company networks.
- “Monitor and investigate unusual network traffic,” including remote connections and remote desktops.
- “Monitor network logs and browser session activity to identify data exfiltration.”
- “Monitor endpoints for the use of software that allows for multiple audio/video calls to take place concurrently.”

Remote Hiring Processes

The FBI further recommended that employers strengthen their remote hiring processes to identify and screen potential bad actors. The recommendations come amid reports that North Korean IT workers have used strategies to defraud companies in hiring, including stealing the identities of U.S. individuals, hiring U.S. individuals to stand in for the North Korean IT workers, or using artificial intelligence (AI) or other technologies to disguise their identities. These techniques include “using artificial intelligence and face-swapping technology during video job interviews to obfuscate their true identities.”

The FBI recommended employers:

- implement processes to verify identities during interviews, onboarding, and subsequent employment of remote workers;
- educate human resources (HR) staff and other hiring managers on the threats of North Korean IT workers;
- review job applicants’ email accounts and phone numbers for duplicate contact information among different applicants;
- verify third-party staffing firms and those firms’ hiring practices;
- ask “soft” interview questions about specific details of applicants’ locations and backgrounds;

- watch for typos and unusual nomenclature in resumes; and
- complete the hiring and onboarding process in person as much as possible.

Legal Considerations

New vendors have entered the marketplace offering tools purportedly seeking to solve such remote hiring problems; however, companies may want to consider the legal pitfalls—and associated liability—that these processes may entail. These considerations include, but are not limited to:

- **Fair Credit Reporting Act (FCRA) Implications:** If a third-party vendor evaluates candidates based on personal data (e.g., scraping public records or credit history), it may be considered a "consumer report." The Consumer Financial Protection Bureau (CFPB) issued guidance in September 2024 taking that position as well, and to date, that guidance does not appear to have been rolled back.
- **Antidiscrimination Laws:** These processes, especially as they might pertain to increased scrutiny or outright exclusion of specific demographics or countries, could disproportionately screen out protected groups in violation of Title VII of the Civil Rights Act of 1964 (e.g., causing disparate impact based on race, sex, etc.), even if unintentional. This risk exists regardless of whether the processes involve automated or manual decisionmaking; employers may be held liable for biased outcomes from AI just as if human decisions caused them—using a third-party vendor's tool is not a defense.
- **Privacy Laws:** Depending on the jurisdiction, companies' vetting processes may implicate transparency requirements under data privacy laws, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) in the European Economic Area (EEA), when using third-party sources for candidate screening. Both laws require clear disclosure to applicants about the types of personal information collected, including information obtained from external background check providers, and how this information will be used and shared.
- **Automated Decisionmaking Laws:** In the absence of overarching U.S. federal legislation, states are increasingly filling in the gap with laws regarding automated decisionmaking tools, covering everything from bias audits to notice, opt-out rights, and appeal rights. If a candidate is located in a foreign jurisdiction, such as in the EEA, the use of automated decisionmaking tools could trigger requirements under both the GDPR and the recently enacted EU Artificial Intelligence Act.

It is becoming increasingly clear that multinational employers cannot adopt a one-size-fits-all vetting algorithm. Instead, companies may need to calibrate their hiring tools to comply with the strictest applicable laws or implement region-specific processes. For instance, if a candidate is in the EEA, GDPR and EU AI Act requirements (among others) apply to the candidate's data even if the company is U.S.-based, which may necessitate, at a minimum, turning off purely automated rejection features for EU applicants and maintaining separate workflows and/or consent forms depending on the candidate's jurisdiction.

Next Steps

The FBI's warning about North Korean IT workers infiltrating U.S. companies is the latest involving security risks from foreign governments and foreign actors to companies' confidential data and proprietary information. Earlier this year, the U.S. Department of Homeland Security published new security requirements restricting access to certain transactions by individuals or entities operating in six "countries of concern," including North Korea.

Employers, particularly those hiring remote IT workers, may want to review their hiring practices, identity-verification processes, and data monitoring, considering the FBI’s warnings and recommendations. Understanding and addressing these risks is increasingly vital, especially as remote hiring continues to expand across industries.

National Law Review, Volume XV, Number 79