PUBLICATION

How Remote Hiring Practices Could Lead to Infiltration of Your Organization: North Korea Operatives are Exploiting Remote Hiring and What Employers Can Do to Stop It

Authors: Matthew George White, Jennifer K. McCarty

December 18, 2024

In today's fast-paced digital world, businesses often seek to access a global pool of skilled professionals by turning to remote talent to fill gaps in their IT needs. Although this practice has many advantages, it also carries hidden risks that could spell disaster for unwary employers. *What if that promising resume came with a side of international espionage?* One of the most alarming threats in this realm is the growing trend of operatives from North Korea – officially the Democratic People's Republic of Korea (DPRK) – posing as remote IT workers. This phenomenon isn't just the stuff of spy novels – it's a real, documented threat with severe implications for companies of all sizes. These operatives have been implicated in schemes to fund the DPRK regime through paychecks and other illicit activities, leaving their unwitting employers exposed to legal, financial, and reputational risks.

In this alert, we will break down the scope of the threat, where it's been observed, how to avoid becoming a victim, and what steps to take if you discover you've unwittingly hired a shadow operative.

The Threat: How DPRK Operatives Hide in Plain Sight

The North Korean government, under crippling international sanctions, has turned to cybercrime and IT outsourcing as unconventional revenue streams. One of its more insidious tactics involves operatives disguised as legitimate IT professionals securing remote work positions with businesses worldwide. These operatives often present stellar resumes, appear to have significant technical expertise, and offer competitive rates (often along with stolen or fabricated identification documents). Once hired, they funnel their earnings back to North Korea to fund illicit activities, including the country's nuclear weapons program. Unfortunately, at the same time, many are also stealing sensitive data from their employer.

Equally concerning, their access to a company's IT systems can be leveraged for espionage, data theft, or introducing malware or "backdoors" into their employer's systems. Your organizational risk isn't just a matter of unwittingly breaking international sanctions – it's about protecting your company's customers, finances, and sensitive data.

Where Has This Been Observed?

Various federal agencies, including the U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation (FBI) have issued warnings about this scheme, *see, e.g.,* Guidance and PSA. According to reports, these DPRK operatives have been found working for companies across Europe, North America, and Asia, and in sectors such as software development, database management, and mobile application design. They often operate under aliases, using falsified or stolen identities to hide their true identities. These operatives often target small and medium-sized enterprises (SMEs), which may lack the resources to conduct thorough due diligence on remote hires; however, dozens of Fortune 100 companies have also fallen victim to this scheme.

How They Operate

1. **Forged Identities:** DPRK operatives typically impersonate IT freelancers from regions such as South Asia, Eastern Europe, or even the United States. They craft convincing profiles complete with glowing reviews and legitimate-looking certifications.

2. **Collaborative Networks:** Many operatives work in teams to obscure their origins further, sometimes even recruiting U.S. Citizens to assist in their operations. In fact, in May 2024 the Justice Department unsealed charges regarding the prosecutions of an Arizona woman, a Ukrainian man, and three unidentified foreign nationals who allegedly participated in schemes to place overseas IT workers – posing as U.S. citizens and residents – in remote positions at U.S. companies. *See* Justice Department Press Release.

3. **Payment Laundering:** These freelancers often request payment through methods that make tracking the funds nearly impossible, ensuring the money is funneled back to North Korea.

4. **Cyber Attacks:** Beyond siphoning funds, these operatives have been implicated in introducing malware into their employers' systems, facilitating ransomware attacks, or conducting espionage on behalf of the regime.

How to Avoid Becoming a Victim

While the threat is real and it is significant, it is not insurmountable. By implementing additional hiring and cybersecurity practices when considering a remote worker, you can reduce your risk of hiring a North Korean operative. Baker Donelson has assisted several clients, of all sizes, who were unwitting victims of these schemes, and we have identified the following best practices:

1. Conduct Thorough Background Checks

- Verify the identity and credentials of all remote hires. Use professional background check services that can validate international education and work history claims.
- Be cautious of resumes with inconsistent timelines or unverifiable references.
- Check References. Contact previous employers or clients directly to validate the worker's experience.

2. Implement Vendor Risk Management Protocols

- Treat freelance IT workers as you would any third-party vendor. Require nondisclosure agreements (NDAs) and carefully vet their security practices.
- Limit access to sensitive systems or data. We understand this can be difficult for software developers to segregate systems from one another as an added layer. Remember: least privileged access is *always* a best practice.

3. Monitor for Red Flags

- Operatives often resist video calls or in-person meetings, citing poor internet connections or time zone differences. Consider using identify verification centers for verifications of remote employees.
- Be wary of payment requests to accounts in high-risk jurisdictions or through cryptocurrency. Rather, insist on payment through traceable methods that comply with anti-money laundering (AML) regulations.

4. Leverage Technology to Detect Fraud

- Use geolocation tools to verify the freelancer's location.

- Deploy software that flags suspicious activity, such as unauthorized file access or unusual login times based upon where the individual claims to be located and/or where the access is initiated.
- Regularly use port checking capabilities to determine if the platform is being accessed remotely via desktop sharing software or a VPN or VPS, particularly if usage of remote desktop sharing software or VPN services to access accounts is not standard practice.
- Deploy robust endpoint detection and response (EDR) tools to monitor and control access.

5. Train Your Team

- Educate your HR and IT teams about this threat. Awareness is the first step in prevention. Add this scenario to your cyber incident response plan and test for it.
- Teach interviewers to recognize red flags in job applications and communication patterns.
- Regularly update employees on emerging threats and best practices for cybersecurity.

What to Do if You've Been Victimized

Discovering that you've unwittingly hired a DPRK operative can be a harrowing experience, but swift action can mitigate damage. Here's what to do first:

1. Terminate Access Immediately

- Revoke the individual's access to all systems, platforms, and data.
- Freeze any pending payments to the individual.

2. Engage Experienced Counsel

- Engage legal counsel specializing in cybersecurity to navigate reporting requirements, regulatory compliance, and potential liability.
- Cybersecurity attorneys can also help coordinate your response with law enforcement and ensure you meet obligations under breach notification laws.
- Employment attorneys can also help to ensure compliance with applicable employment laws.

3. Report the Incident

- Notify the relevant authorities, such as the FBI or the Treasury's Office of Foreign Assets Control (OFAC). Legal counsel should assist with this.

4. Assess and Contain the Damage

- Engage cybersecurity professionals, through counsel to maximize the attorney-client privilege, to analyze the extent of any potential breach. Activate your incident response plan, as appropriate.
- Under counsel's guidance, conduct a thorough audit to determine whether sensitive information was accessed or exfiltrated.
- Identify and close any vulnerabilities that allowed the operative to infiltrate your systems.

5. Cooperate With Investigators

- Authorities may require access to logs, emails, and other data to build a case. Cooperation may help mitigate potential penalties for your company.

6. Review and Revise Policies

- Update hiring practices and cybersecurity protocols based on lessons learned from the incident.
- Implement ongoing monitoring to prevent recurrence.

The Cost of Complacency

The financial, reputational, and legal risks of hiring a DPRK operative cannot be overstated. Beyond potential sanctions, your company's data and intellectual property are at stake. A single day on the job and breach of systems can lead to costly litigation, loss of client trust, and regulatory fines.

Consider this a wake-up call: Remote hiring requires increased vigilance. The savings from hiring foreign remote workers can evaporate in an instant if you fall victim to one of these schemes. Employers must therefore balance the benefits of global hiring with the due diligence necessary to safeguard their operations.

Conclusion

In our ever-connected global economy, the line between opportunity and risk has never been thinner. While the international talent pool offers incredible advantages, it also comes with pitfalls that require vigilance. The threat of hiring North Korean IT operatives is a stark reminder that not all that glitters is gold.

By staying informed and proactive, you can protect your company from becoming an unwitting accomplice to international cybercrime. And if you've already been targeted, swift action and professional guidance can help you recover and fortify your defenses. Remember, in the realm of cybersecurity, an ounce of prevention is worth far more than a pound of cure. For more information, or if you need assistance with any of these issues, please contact the authors: Matt White, CIPP/US, CIPP/E, CIPT, CIPM, PCIP, Jenni McCarty, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity or Labor & Employment teams.