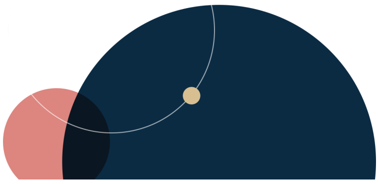
Steptoe

STEPWISE: RISK OUTLOOK | OCTOBER 17, 2024

North Korean IT Worker Infiltration Threats Expose Risks for Organizational Cyber Resilience and Sanctions Enforcement

Author
William Simpson

Cybersecurity, Digital Threats, Disruptive Technology, Malware, North Korea, Russia



Overview

Today's Deep Dive is 1,197 words and an 8-minute read.

On September 23, Google’s Mandiant unit released a report which revealed that a fake information technology (IT) worker scheme run by the Democratic People’s Republic of Korea (DPRK), or North Korea, is generating substantial revenue for the regime. The report found that one American facilitator assisting the IT workers was able to compromise over 60 identities of American individuals, affecting over 300 companies, and generating at least $6.8

million of illicit revenue between 2020 and 2023. This followed an August 8 US Department of Justice (DoJ) press release announcing the arrest of a Nashville local for allegedly helping the DPRK funnel money from US businesses through fraudulently hired remote IT workers, building on previous DoJ actions earlier in May and in October of last year.

The infiltration of North Korean IT workers is a key element in the regime's evolving cyber sabotage strategy, which increasingly targets businesses, government agencies, and other organizations handling critical data. As North Korea's cyber sabotage efforts become more sophisticated, these tactics will not only facilitate financial theft but also raise the risk of espionage and data breaches. Protecting against such insider threats is crucial as Pyongyang continues to leverage its cyber capabilities to bypass international sanctions.

Insider Threats: A Growing Concern for Businesses and Organizations

North Korean IT worker infiltration represents an increasingly sophisticated type of insider threat, particularly targeting sectors handling sensitive information, such as technology, defense, and financial services. While some sources claim that these operations can be traced back to the 2010s, they have expanded significantly since 2020, capitalizing on the proliferation of remote work following the COVID-19 pandemic. These workers are primarily operating from China and Russia, with smaller numbers in Africa and Southeast Asia, enabling them to evade detection while earning substantial revenue and siphoning data from their employers.

The FAMOUS CHOLLIMA case study from the CrowdStrike 2024 Threat Hunting Report highlights the scale of this threat. Between April and May, the cybersecurity firm identified DPRK agents applying to or actively working at over 100 different companies, the majority being US-based technology entities. Often, the infiltrators did minimal legitimate work but used their positions to install remote monitoring tools and exfiltrate sensitive data. The damage caused by these insider threats is multifaceted, compromising corporate data, threatening intellectual property, and providing the DPRK with the financial resources needed to support its weapons of mass destruction programs.

By infiltrating prominent US and other foreign companies, these North Korean operatives introduce substantial organizational security risks. Threat intelligence analysts have found these individuals to leverage advanced remote access tools, including AnyDesk, RustDesk, TinyPilot, and Google Chrome Remote Desktop, to maintain persistent access to corporate networks, often without detection for extended periods of time. The KnowBe4 case in June, where a North Korean operative was discovered planting malware shortly after being hired at the cybersecurity firm, provides a clear example of the potential damage these malicious insiders can cause.

North Korea’s Broader Cyber Strategy

North Korea has consistently employed cyber operations to circumvent international sanctions and fund its weapons programs. The regime’s cyber units, including the Lazarus Group, have historically focused on hacking financial institutions and cryptocurrency exchanges. However, the use of IT worker infiltration is a relatively nascent, yet growing, approach that enables the DPRK to expand the scope of its cyber sabotage capabilities, generate illicit revenue, and gain access to corporate secrets and valuable intellectual property.

Pyongyang’s advances in technology, particularly in artificial intelligence (AI), have aided its ability to develop increasingly sophisticated cyber sabotage capabilities. Experts note that North Korea has been strategically investing in AI development across multiple sectors, despite sanctions limiting its potential to acquire advanced technology components. During infiltration campaigns, North Korean operatives have used AI tools to craft highly convincing personas and evade detection during the hiring process. This has been exemplified by these individuals' utilization of the technology to generate fake profile pictures in a convincing manner, enhance phishing and social engineering attacks, and automate offensive cyber operations, including malware deployment and network reconnaissance.

North Korea's growing alignment with Russia, which has also been implicated in high-profile cyber sabotage campaigns against the US and its allies, presents additional risks concerning Pyongyang's ability to access advanced technologies. Since Russia's invasion of Ukraine in 2022, ties between Moscow and Pyongyang have flourished, culminating in the establishment of a comprehensive strategic partnership following the signing of a bilateral treaty in June. The treaty formalizes long-term cooperation in key areas such as military, economic, and technological collaboration, and Western observers raise concerns that this could extend to joint cyber operations or the sharing of cyber capabilities.

Assessing the Risks for Organizational Cyber Resilience and Sanctions Enforcement

The infiltration of North Korean IT workers into foreign companies, particularly based in the US and other Western nations, presents significant challenges that intersect both organizational cyber resilience and sanctions enforcement. From a cybersecurity perspective, besides acting as malicious insiders, these operatives also introduce long-term, covert risks by embedding themselves in company networks through the roles in which they are hired.

While public and private sector efforts to crack down on the scheme have yielded some results, uncertainty remains over Pyongyang's ability to further refine its tactics, outpacing organizations' abilities to detect and mitigate threats. Should the DPRK continue to successfully infiltrate organizations with its deceptive IT worker scheme, entities will encounter the risk of data exfiltration through internal breaches, which can yield long-term financial, reputational and operational damage. The potential for operational disruptions presents a particularly alarming risk on the horizon, as North Korean operatives, upon infiltrating a network, could lay the groundwork for more destructive cyber sabotage efforts aimed at undermining business continuity or even targeting national infrastructure.

Pyongyang's ability to evade US and international sanctions through its IT worker infiltration campaign remains a significant concern for regulatory authorities. The illicit revenue that the regime has already been able to generate through these infiltrations demonstrates the limitations of existing sanctions frameworks, which struggle to monitor and restrict these types of indirect economic activities conducted through cyberspace.

With the risks outlined, this evolving threat landscape also presents an opportunity for organizational growth in cybersecurity maturity. Companies that recognize the potential for such insider threats and implement advanced detection capabilities may not only mitigate risk but also gain a competitive advantage by enhancing their overall security posture and long-term defense aptitudes. Additionally, cross-industry and public-private collaboration, such as information sharing, can work to enhance both organizational cyber resilience and regulatory authorities' ability to close sanction loopholes. On October 16, the governments of the US and key allies, including Canada, Germany, Japan, and South Korea, announced the establishment of a Multilateral Sanctions Monitoring Team, which could potentially move the needle on multilateral efforts to outpace Pyongyang's ability to evade international sanctions.

Continued challenges exist, particularly in balancing the growth of remote work and freelance employment with the need for enhanced cybersecurity measures. The global labor market is reliant on remote work, particularly for IT positions, and this will continue to provide avenues for malicious actors to exploit vulnerabilities in hiring processes. Mitigating these threats will require sophisticated detection methods and a proactive approach to identifying patterns of insider behavior that may signal infiltration.

Practices

AI, Data & Digital

Internet, Telecom & Media

Economic Sanctions

National Security & Cross-Border Transactions