CISO PLAYBOOK

Guide to implementing controls for the North Korean threat

As discussed in the Sophos blog post introducing this CISO playbook, fraudulent workers from North Korea are infiltrating organizations of all sizes across multiple sectors. To help organizations address this threat, we created a control matrix that lists 51 controls for organizations to consider. Most of the recommendations require cross-functional support, so it is critical to involve the appropriate internal stakeholders from your human resources (HR), IT, legal, finance, and cybersecurity teams from inception through execution.

Early-stage awareness and socialization of this threat may generate organizational support to implement the controls mentioned in the control matrix. Use the matrix to guide the conversations, understanding that many of the recommendations may just be enhancements of existing tasks.

Matrix overview

We created two versions of the matrix: a static version and a version containing project management features. Both versions list process and technical controls across eight categories that span employee acquisition through post-hire:

- HR and process controls
- Interview and vetting
- Identity and verification
- Banking, payroll, and finance
- Security and monitoring
- Third-party and staffing
- Training
- Threat hunting

For each control, we have included the following elements:

- Control category
- Control type
- Control name
- Control description
- Primary function
- Participating functions
- Hiring stage
- Frequency
- Implementation notes
- Sophos product mapping (where applicable)

We also included columns for organizations to select the status of each control, assign owners, and add notes.

Detection and prevention

While it is important to prevent fraudulent workers from being hired, cybersecurity teams should consider the possibility that North Korean threat actors may already be embedded in the organization. The 'Security and monitoring' and 'Threat hunting' worksheets in the control matrix list controls that could detect these workers.

Early wins can be instrumental in building momentum. Conducting threat hunts within the organization and sharing the findings with leadership can demonstrate the tangible risk and justify broader cross-functional engagement.

The following articles published by Sophos and other vendors include indicators associated with this threat. While these articles and the control matrix reflect current TTPs, North Korean threat actors will likely evolve their approach as organizations respond to the threat. It is crucial for organizations to stay abreast of the issue and adapt as appropriate.

- **Sophos:** NICKEL TAPESTRY expands fraudulent worker operations
- **Mandiant:** Staying a Step Ahead: Mitigating the DPRK IT Worker Threat
- **ReliaQuest:** Threat Spotlight: Red Flags for Red Star Hackers: Hunting for North Korean Insiders
- **SentinelOne:** DPRK IT Workers | A Network of Active Front Companies and Their Links to China

Matrix overview cont.

The 'project manager-ready' version of the control matrix includes additional worksheets that are pre-populated with data to illustrate the functionality:

- **Project Tracker Sheet:** This unified view lists all the controls across the eight categories.
- **Control Status:** Updating this sheet updates the control status column on the Project Tracker Sheet. Note that changes to the control status column on the individual category worksheets will not be reflected on the Project Tracker Sheet.
- **Project Status:** The preloaded pivot table will update to reflect the control status set on the Control Status worksheet. After changing a status on that sheet, click 'Refresh All' in the Data tab to update the pivot table on this worksheet.
- **Control Owners:** The preloaded pivot table will update as control owners are assigned in the Project Tracker Sheet; the charts will also reflect control status. After changing an owner on the Project Tracker Sheet, click 'Refresh All' in the Data tab to update the pivot table on this worksheet. Note that changes to the owner column on the individual category worksheets will not be reflected on the Project Tracker Sheet.

Executive and stakeholder buy-in

This threat spans technical, legal, financial, and operational dimensions. To effectively address the risk posed by fraudulent North Korean workers, it is essential to obtain support and commitment from the executive team and all stakeholders. Therefore, framing the issue in business terms is critical. Executives, particularly the organization's chief financial officer (CFO), chief human resources officer (CHRO), and general counsel, should be made aware that the consequences of fraudulent hires include salary diversion to sanctioned entities and also potential data theft, extortion, and other insider threat activities. Referencing real-world incidents and official advisories from law enforcement and government agencies can help underscore the urgency and legitimacy of the threat.

The control matrix illustrates the need for collaboration across departments, as only 39% of recommended controls are exclusively for IT and cybersecurity teams. Tailoring messaging to each function is also key: HR should be engaged for enhancing verification and onboarding processes, finance for payroll and sanctions compliance, and legal for employment law and contractual safeguards.

Cross-functional tracking and execution

To support cross-functional execution, organizations should establish a dedicated task force comprising representatives from the cybersecurity, HR, legal, and finance teams. A dedicated program manager can be useful for coordinating efforts, tracking progress, facilitating communication, and ensuring accountability. Each control should have clearly defined ownership, with primary and secondary leads, and escalation paths for unresolved issues. Centralizing documentation will help maintain visibility into control implementation, decisions, and audit trails. In addition to the notes column included in the control matrix, organizations may find it helpful to use HR software or collaboration platforms such as Confluence or SharePoint. Capturing unusual behaviors in a centralized location can also expose suspicious details and patterns that might get overlooked or discounted in isolation.

Routine audits and reviews are essential, especially of third-party vendors. These partners must be educated on the threat landscape and held to the same standards as internal teams. Training should be continuous and role-specific, with HR, IT, and cybersecurity teams regularly updating each other on evolving tactics and tools. Ultimately, defending against fraudulent hires must become a company-wide effort, with education and vigilance extending to every employee.