A Practical Guide from Nisos®

Human Risk Buyer's Guide for Employment Fraud

A holistic, proactive, and cross-functional approach is the best-practice approach to staying ahead of employment fraud. This buyer's guide will outline how employment fraud has evolved, and the different types of risk enterprises face today, as well as considerations for improving your organization's ability to improve your policies, processes, and approaches to reducing your risk.

TABLE OF CONTENTS

Executive Summary

Employment fraud poses an escalating threat to organizations, driven by fraudulent applicants and employees who capitalize on vulnerabilities in hiring processes, corporate policies, and IT security controls. Using tactics such as falsified credentials, identity theft, or exploiting remote work environments, bad actors are hired and gain unauthorized access to internal systems, leading to potential financial theft, intellectual property breaches, and reputational damage.

Today’s best practices are to adopt a holistic and continuous approach to human risk management. This includes incorporating multi-disciplinary collaboration, leveraging advanced tools, conducting expert-led investigations, and implementing monitoring. By prioritizing proactive fraud prevention and monitoring, businesses can safeguard their operations, minimize losses, and enhance trust in their workforce.

This buyer's guide is designed to help human resources teams, CISOs, corporate security, and legal teams understand the risks and techniques used to commit employment fraud. It provides best practices and actionable solutions to help teams effectively identify, investigate, and prevent these threats from impacting operations, reputation, and employee safety.

The Rising Threat of Employment Fraud

Fraudulent applicants and employees pose a significant threat to organizations, often exploiting weaknesses in hiring processes to secure jobs they're unqualified for or to commit workplace misconduct. The shift to remote work, alongside the increasing use of advanced technologies, has made it easier for job applicants to conceal their true identities. This is especially true when employers no longer meet candidates in person, leaving them vulnerable to fraud.

Many individuals who are intent on committing employment fraud use falsified credentials to gain access to positions. This might include fake degrees, fabricated employment histories, or forged references. In more severe cases, applicants may steal someone else's identity to pass background checks. As remote work becomes more common, traditional in-person verification methods are less frequently employed, giving these bad actors more opportunity to deceive employers.

Once these fraudulent employees are hired, the damage they can cause is significant. They may engage in activities such as embezzlement, data theft, or sharing sensitive company information with competitors or malicious actors. The financial and reputational consequences can be devastating, especially in highly regulated industries. For example, in December 2024, 14 North Korean individuals were indicted by the Department of Justice for fraudulently earning $88 million and stealing corporate information while working for U.S. companies under stolen identities.[1]

[1] https://therecord.media/doj-indicts-14-north-koreans-earning-88-million-at-us-firms

Combating Employment Fraud in the Digital Age

To address the growing issue of employment fraud, companies are turning to more advanced verification tools. AI-driven background checks and credential authentication systems are becoming increasingly common, along with stricter hiring protocols to reduce the risk of onboarding fraudulent candidates.

However, while corporate security teams often handle digital risks, they tend to focus on IT controls and overlook the human aspects of fraud. This includes understanding who the threat actors are, what their motives may be, and how they designed their fraudulent schemes. With the rise of remote work, the proliferation of social media, and the dark web, digital and human risks have now converged. As a result, a collaborative approach is needed, involving not just cybersecurity teams, but also HR, legal, and compliance departments, along with corporate security teams.

Experts estimate that U.S. companies lose 20% of every dollar to workplace fraud [2]

Despite this, many businesses still lack the policies, processes, and cross-functional collaboration required to address the full scope of employment fraud. A proactive, holistic approach is essential to protect organizations in today's rapidly evolving work environment.

[2] https://www.ehstoday.com/archive/article/21909476/study-employers-lose-20-cents-of-every-dollar-to-workplace-fraud

Types of Employment Fraud

Despite its benefits and flexibility, remote work has helped to facilitate the growth of employment fraud complexity and frequency. Businesses are increasingly targeted by sophisticated schemes designed to exploit hiring processes and, as we've pointed out, the consequences can be significant. Before we dive into employment fraud trends, let's cover the most common types of employment fraud used to exploit businesses.

Employment fraud can be categorized into three primary types:

Misrepresentation: (Low Risk)

Employees or contractors lying on their resumes, fabricating reference contacts, and using remote desktop tools to periodically get help from unauthorized third parties (generally friends and family, not paid help).

Polywork: (Moderate Risk)

Employees or contractors conduct all low-level fraud but on an escalated basis, consistently outsourcing their jobs to unauthorized third parties. Polywork also refers to employees working multiple full-time jobs at the same time and with potentially competing / conflicting business interests.

Organized Fraud: (High Risk)

Employees or contractors outsource their jobs through a coordinated criminal or scam network of unauthorized third-party contractors and facilitators. These can include employment fraud with nation-state ties such as the DPRK[3] (Democratic People's Republic of Korea, a.k.a. North Korea) which has recently made headlines and been the subject of Department of Justice[4] (DOJ) and Federal Bureau of Investigation[5] (FBI) advisories.

[3] https://www.nisos.com/research/dprk-it-worker-scam/
[4] https://www.justice.gov/opa/pr/charges-and-seizures-brought-fraud-scheme-aimed-denying-revenue-workers-associated-north
[5] https://www.ic3.gov/PSA/2024/PSA240516

Trends in Employment Fraud

Remote work has redefined the traditional hiring processes. It’s become easier for fraudsters to exploit vulnerabilities in corporate recruiting and hiring processes and practices. Through social media and the virtual nature of remote working, fraudulent applicants have widespread access to the information needed to construct fake identities and hide their true motives. From false claims about credentials, to working multiple jobs without permission, and leaking sensitive information, here are some increasingly common tactics.

- **Remote Work Scams:** With remote work becoming more prevalent, fraudulent employees are taking advantage of the virtual hiring process. By using fake identities or stolen credentials, they apply for positions in companies that lack rigorous verification processes, and gain access to sensitive information once hired.

- **Resume Fabrication and Employment History Falsification:** The rise of freelance platforms and gig work has seen an uptick in applicants falsifying their credentials, qualifications, or past employment to meet job requirements.

- **Identity Theft:** Some fraudsters assume another individual’s identity, using stolen personal information to bypass background checks.

- **Third-Party Fraud Schemes:** There are reports of organized networks creating fraudulent employment schemes that involve multiple layers of deception, including fake recruiters or third-party employment agencies.

Key Steps to Managing the Human Risk of Employment Fraud

In today's digitally enabled workforce, standard background checks are no longer sufficient to assess the business risk of hiring an applicant. Human resources and security teams often lack the tools and expertise to effectively evaluate employees' digital "outside the firewall" activities. These insights help enterprises understand how the employees' behaviors, actions, and sentiments impact risks to operations, IP, or company reputation. There's an opportunity for corporate security teams, CISOs, legal teams, and human resources leaders to consider more comprehensive approaches to identifying employment fraud risks, investigating suspicious behaviors, and preventing future employment fraud incidents.

There are three primary steps to minimizing employment fraud, before, during, and after incidents occur - identifying indicators, investigating risks, and preventing fraud. A holistic approach includes robust screening and monitoring for criminal history, false identification and credentials, incriminating social media, polywork, data leaks, and risky affiliations, as well as deeper cross-functional investigations into suspicious behaviors during employment.

Identify Indicators of Employment Fraud Risk:

Indicators of fraud can occur at various stages of the hiring process.
Businesses can more carefully screen applicants and be on the lookout for telltale signs:

- **Inconsistent or Vague Employment History:** Fraudulent applicants may provide incomplete timelines or vague details about previous employers, including gaps in employment that are not well-explained or employment history that is hard to verify.

- **Suspicious Email Addresses:** Addresses from generic email providers with employer-specific naming conventions, such as firstname.lastname.work@gmail.com.

- **Manipulated Credentials:** Fake degrees, certifications, or affiliations with non-existent educational institutions are common indicators that an application could be fraudulent.

- **Mismatched Identity Information:** Document discrepancies, such as inconsistencies between ID numbers, birth dates, and other personal details across submitted forms could indicate identity theft or fake identities.

- **Unverifiable References:** Fraudsters often provide fake or untraceable references. If the contact information for all references is sparse, non-responsive, or includes unverifiable companies or persons, it's a potential red flag.

- **Suspicious Behavior During Virtual Interviews:** Remote work scams may be accompanied by unusual behaviors during interviews. Applicants may avoid video calls, make excuses for poor video quality, or seem unprepared despite impressive credentials on paper.

Investigate Heightened Risk Profiles:

When candidates show signs of heightened risk, businesses must take a proactive approach to assess potential threats.
Below are key actions to help address and mitigate these risks:

- **Collaborate Across Teams:** HR, security, CISO, and legal should work together to assess the candidate's risk to ensure all angles.
- **Make Informed Hiring Decisions:** Use input from all departments to decide whether the candidate's risk outweighs their potential value. Consider mitigation strategies, like post-employment monitoring, if necessary.
- **Respond Quickly to Fraud Detection:** If fraud is found, act fast to assess the situation and prevent further damage. Investigate any misrepresentation, polywork, data leaks, or fraudulent behavior.
- **Launch a Formal Investigation:** Initiate a formal probe to gather evidence, interview relevant parties, and understand the full scope of the fraud. Work with cross-functional teams to follow proper procedures.
- **Mitigate Damage and Protect Reputation:** Take steps to minimize the impact of the fraud, address vulnerabilities, and protect sensitive data. Communicate with stakeholders as needed to repair any damage to the company’s reputation.

Prevent Employment Fraud in Real Time:

To establish and maintain an understanding of applicant and existing employee risk profiles teams should monitor behaviors inside and outside the firewall. There are several critical steps to prevention:

- **Cross Check Social Media:** Conduct a detailed review of the applicant's online presence for consistency in name, appearance, work history, education, etc. Some fraudulent applicants may have various online personas using the same photo or name across different profiles.
- **Use Comprehensive Background Checks:** Leverage third-party screening services to conduct thorough background checks, including criminal records, employment verification, and educational credentials. Additionally, implement identity verification software, particularly for remote hires.
- **Verify References and Employment History:** Always contact provided references and cross-check their validity. If possible, confirm employment history with official HR departments rather than relying on direct supervisors, who may be harder to verify.
- **Strengthen Identity Verification in Remote Hiring:** As remote work fraud increases, it is crucial to implement more robust identity verification procedures. This could include video-based identity checks or requiring candidates to submit official identification documents and additional proof of identity.
- **Educate Your HR and Hiring Teams:** Train your hiring and recruitment teams on employment fraud detection techniques. Make sure they are familiar with the common trends and indicators of fraud, and ensure they know how to handle suspicious cases properly.
- **Monitor for Fraud Post-Hiring:** Fraud can still occur after an individual is hired. Regularly review employee performance, access to sensitive systems, and any signs of inappropriate activity. Implement monitoring tools that can help detect anomalous behaviors in the workplace, whether digital or physical.

Working Together to Manage Employment Fraud

While the goals for managing employment fraud are clear, the path to reaching them eludes many businesses. Human resources teams play a central role in the hiring process, but lack the specialized tools and expertise required to detect sophisticated fraud schemes. Unfortunately, the siloed nature of HR, IT, and corporate security limits the potential for comprehensive screening and gaining contextual insight about the complete risk profile of each candidate and employee.

Because digital threats and human threats are converging, it is imperative that human resources teams work in unison with legal, IT, and corporate security teams to gain a full view of the potential risks. Corporate security can assist by identifying red flags and patterns of fraudulent behavior, while the IT teams help ensure that robust systems are used for identity verification and secure handline of data and IP. Meanwhile legal teams should provide guidance on compliance, investigations, and policy enforcement. By working together with a multi-layered approach, companies can help reduce the risks of employment fraud.

Nisos Employment Shield Solution

To protect businesses from human risks associated with employment fraud, Nisos offers Employment Shield, an analyst-led solution designed to identify and prevent employment fraud within your organization. We do this by assessing hiring risks, conducting deep investigations on high-risk individuals, and monitoring for fraud. We deliver the who, what, why, and how of human risk. Our services include identity verification, and screening for potentially damaging associations and activities. Nisos helps you mitigate financial losses, legal liabilities, and operational risks, ensuring safer, more informed hiring and employee risk management decisions.

Identify Indicators or Employment Fraud Risk

Our assessments analyze external data sources to reveal criminal history, deepfakes, signs of undisclosed polywork, and other fraud indicators. These assessments serve as next-level pre-employment screening or to help identify employment fraud within your workforce

Investigate Heightened Risk Profiles

When fraud indicators are identified, we conduct deeper investigations to understand the threat actor's identity, network, their tactics, techniques, and procedures (TTPs), and their motives.

Prevent Employment Fraud in Real Time

With open-source monitoring, we actively hunt for employment fraud indicators, providing you with peace of mind for both short- and long-term talent acquisition decisions.

Nisos Employment Shield extends beyond traditional background checks with in-depth analysis of employment fraud risks, including:

- Lawsuits
- Polywork
- Malign influence
- Identity confirmation
- Criminal history
- Negative social media

Case Study: Investigating Nation-State Employment Fraud

Situation

A major tech platform client and its legal counsel engaged Nisos to investigate two former employees who provided false documentation to obtain employment and had behaved suspiciously during their time at the company. The client was concerned with potential links to criminal or nation-state actors.

Why Nisos

Nisos specializes in identifying and mitigating employment fraud risks through tailored intelligence and investigative strategies. Our experts analyzed background logs, email addresses, IP addresses, and social media accounts. We found falsified identity documents, copied resume language, suspiciously limited social media presence, and evidence that the application ID credentials and IP addresses had also been used by North Korean threat actors. Our investigators attributed two individuals who were likely associated and part of a DPRK effort to exploit remote work to fund its weapons programs and steal IP. Nisos helped the client reinforce their security posture against future exploitation, while our actionable intelligence supported law enforcement to pursue legal action against the threat actors.

Impact

- **Legal and Law Enforcement Action:** The investigation resulted in actionable intelligence that supported law enforcement efforts to pursue legal action against the individuals involved.
- **Enhanced Security Response:** By working alongside legal counsel and law enforcement, Nisos supported the client in reinforcing their security posture against future exploitation attempts.
- **Compliance:** By terminating the fraudulent employees, Nisos helped the client to avoid sanctions and regulatory fines

Case Study: Uncovering Employment Fraud Risks

Situation

A client suspected that an employee was using their position in the company to benefit personal business ventures. Nisos was tasked to investigate fraudulent activities, misuse of company resources, and conflicts of interest that could impact business operations or integrity.

Why Nisos

Nisos leverages advanced open source intelligence (OSINT) methodologies with expert investigative methods to uncover hidden risks that could impact our client's organization. Our approach includes data aggregation, social media analysis, business research, and criminal record verification to provide a comprehensive view of potential threats. Nisos helps organizations proactively detect and address employment fraud, safeguarding both assets and long-term integrity by identifying risks before they escalate.

Impact

- **Identification of Potential Risks:** The investigation revealed multiple concerns, including conflicts of interest and misuse of company resources, providing the client with critical insights into possible employment fraud.
- **Uncovering Undisclosed Personal Ventures:** Although no direct evidence of fraud was found, the employee's involvement in competing personal ventures raised significant risks to the client's business interests.
- **Actionable Recommendations:** Based on the findings, Nisos recommended further internal audits and reviews to assess the full extent of misconduct and protect the client's assets.

Case Study: Protecting National Security Through Intelligence Investigations

Situation

Nisos was tasked with identifying an individual who had been behind the posting of a controlled unclassified military document on an online forum which posed a potential risk to the U.S. government. Our investigation aimed to determine if the person responsible had access to controlled unclassified information and potentially classified data, and to assess any associated risks.

Why Nisos

Nisos specializes in investigating and mitigating risks related to employment fraud and unauthorized access to sensitive information. Our expert investigators analyze online activities, affiliations, and other digital footprints to uncover vulnerabilities that could compromise an organization's security or intellectual property. By leveraging advanced investigative techniques, we help organizations identify potential threats early, enabling proactive responses that safeguard both assets and national security. With Nisos, you can trust that your business is protected from evolving risks in an increasingly complex threat landscape.

Impact

- **Access to Sensitive Information:** Our investigation confirmed the individual had access to controlled unclassified information from the Defense Technical Information Center (DTIC), but no evidence was found linking them to classified materials on the Secure Internet Protocol Router Network.

- **Security Risks Identified:** The posting of restricted documents on a public forum highlighted significant potential risks to national security.

- **Actionable Recommendations:** Nisos recommended further investigation to fully assess the individual's access to sensitive information and mitigate any potential security threats.

Working with Nisos: Your Human Risk Management Partner

Nisos' Employment Shield is an analyst-led solution that helps organizations prevent employment fraud by assessing hiring risks, conducting deep investigations on high-risk individuals, and monitoring for potential fraud. Combining advanced technology with human intelligence, Employment Shield uncovers risks such as identity fraud, criminal history, and damaging associations before they impact your business. By mitigating financial, legal, and operational risks, Nisos ensures safer hiring and employee management decisions.

How Nisos helps safeguard key personnel with Employment Shield:

- Identify Indicators of Employment Fraud Risk
- Investigate Heightened Risk Profiles
- Prevent Employment Fraud

Unlike the traditional threat intelligence approach of delivering large datasets that are not customized to your organization and threat surface, Nisos uses our vast multi-source collection capability to uncover human risk threats specific to your business. Nisos' threat assessments provide unparalleled visibility into your digital footprint and risk. Our insights provide actionable intelligence and prioritized threat mitigation recommendations to help you reduce human risk.

About Nisos

Nisos, the Managed Intelligence Company®, is a trusted digital investigations partner specializing in unmasking human risk. We operate as an extension of security, risk, legal, people strategy, and trust and safety teams to protect their people and their business. Our open source intelligence services help enterprise teams mitigate risk, make critical decisions, and impose real world consequences.

For more information, visit: nisos.com email: info@nisos.com | 703-382-8400