eBook

Human Risk Case Studies

Mitigate Human Risk with Intelligence Driven Solutions

Stay ahead of threats to **protect your people, assets, and reputation** with Nisos' expert insights

“The scale, scope, and pace of risks faced by enterprises today and tomorrow will only continue to accelerate, driving the need for businesses to generate and then translate insight into action at an ever-faster rate. Nisos’ uniquely qualified team excels at building insight across the risk spectrum, working hand-in-hand with businesses to apply insights to drive effective mitigation”

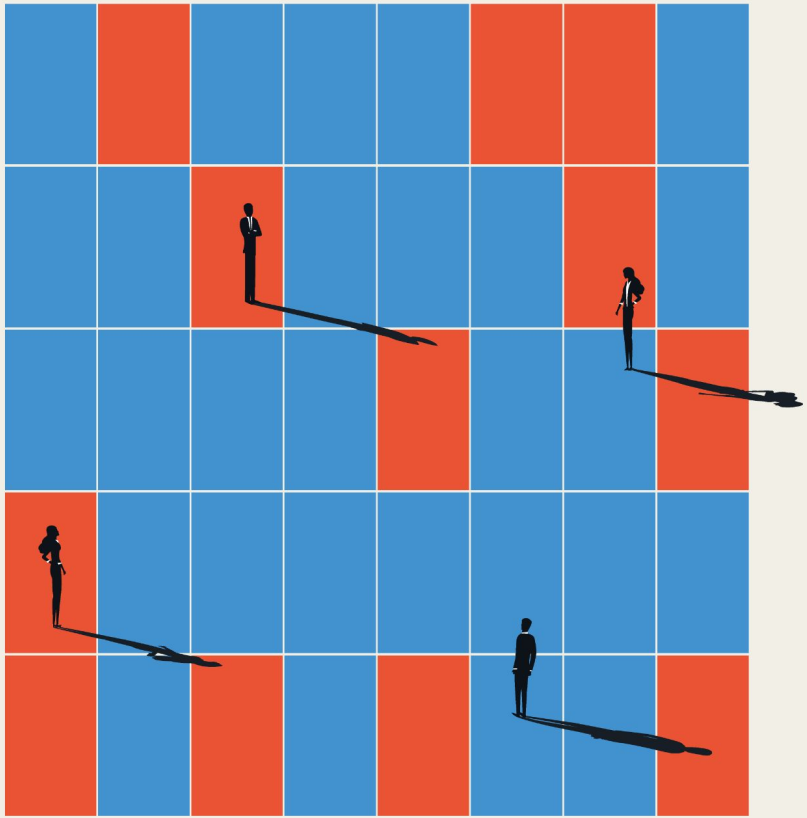
John Moore
Global Risk Management Professional

Case Study

Executive Protection

Mitigating Threats to Executives and Their Families

Nisos **uncovers significant threats targeting an executive and their family** from a financial services enterprise



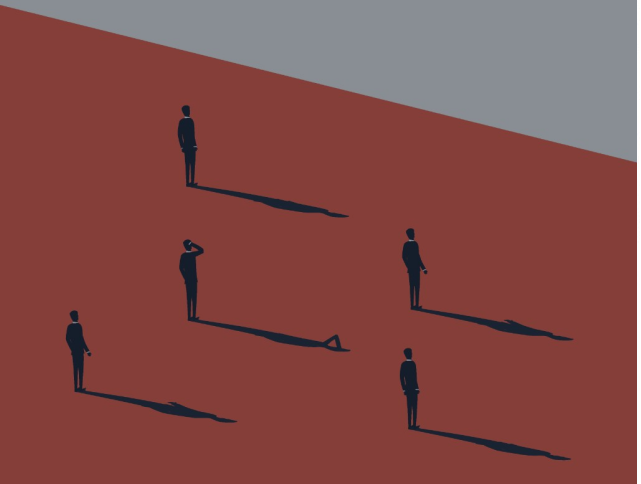
SITUATION

Identity theft and fraud are serious security issues that can plague executives and companies. Due to the wide availability of Personally Identifiable Information (PII) online, proactive measures need to be taken to protect high-profile individuals and their families.

A Client within the financial sector tasked Nisos with identifying vulnerabilities associated with a C-level executive after attempts of fraud and identity theft targeting the executive's family member.

The primary objective was to assess the risks associated with breached information, accounts for sale, physical location data, and their overall digital footprint.

INVESTIGATION



Looking to protect the executive's and the company's sensitive data, the Client tasked Nisos to assess the risks associated with the executive and their family member.

Nisos conducted a comprehensive analysis and found that both the executive and the family member had moderate risk profiles.

This assessment was based on several factors:

- Wide availability of physical addresses and contact information.
- Public images and family information shared on social media profiles.
- Inclusion of PII in breach data.

IMPACT

Assessing the extent of risk to the executive identified that the vulnerabilities for the C-level executive also extended to their spouse and children. This required a holistic approach to ensure the security of the entire family.

The vulnerabilities Nisos uncovered included:

- The executive's family members' social security number (SSN) was **found for sale on a dark web marketplace.**
- Both the executive and the family members' **PII was present on numerous websites** that required no payment or login credentials to access.
- A recent data breach of a financial institution was identified as a potential contributor to the fraud experienced. However, it was noted that the more likely cause was a threat actor **acquiring information through a deceptive phone call.**

Case Study

Insider Threat

Monitoring and Identification of Insider Threats

Nisos identifies potential insider threats in **social media posts during ongoing monitoring**

SITUATION

Insider threats can severely damage companies by exposing sensitive information, disrupting operations, and undermining trust. These risks, whether intentional or accidental, can lead to financial losses, reputational harm, and compromised security.

Nisos alerted an existing Client of elevated risks identified during our ongoing monitoring service. Our team of expert researchers continuously monitored for emerging threats that could compromise the Client's security.

During our investigation, Nisos discovered a post on social media in which an individual claimed to have leaked sensitive internal information about the Client to prominent news outlets.

INVESTIGATION

The discovery of the social media post triggered an in-depth investigation to assess the credibility of the threat and to uncover the identity of the potential insider.

Through a combination of open-source intelligence, proprietary tools, and third-party vendor solutions, Nisos was able to gather crucial details that ultimately helped the Client address the situation and protect their data.

- **Employment History:** The individual likely worked for the Client following their acquisition of another company.
- **Leaking Propensity:** In the same post, the individual also offered to expose sensitive information about another former employer, indicating a tendency to leak employer information.
- **Disparaging Posts:** The individual had posted multiple disparaging posts about the Client and its personnel, which were later deleted.

IMPACT

Nisos identified a major risk to the Client by carefully monitoring insider threats. Nisos' comprehensive approach provided a clear path for the Client to safeguard their sensitive information and address the risk effectively.

- Nisos used open-source information to gather insights about the individual behind the social media account. By analyzing their digital footprint and online behavior, Nisos was able to track the individual's activities and identify connections that provided valuable context for the threat.

- Our team of researchers assessed the individual's behavior, past actions, and potential motives to determine the level of threat posed to the Client. This analysis gave the Client a clear understanding of the severity of the situation and enabled them to shut down the threat.

Case Study

Employment Shield

Investigating Nation-state Employment Fraud

Nisos uncovers North Korean state actors gaining employment at **major tech platform company**

SITUATION

Employment fraud presents significant risks to businesses, leading to financial loss, security breaches, and damaged reputations. Fraudulent employees accessing sensitive information can undermine organizational trust, especially in remote work environments where vetting processes can be more challenging.

North Korean IT workers have been known to pose as non-North Korean nationals to infiltrate businesses, funneling funds to the DPRK's economic and security efforts. In 2022, the U.S. government issued warnings about North Korean IT workers using fake identities to secure jobs and fund illicit activities.

Fearing an insider threat, a Client and their legal counsel engaged Nisos to investigate several former employees who provided false documentation to obtain employment and exhibited suspicious behavior during their time with the company. Nisos was tasked to investigate the former employees to uncover any relationship with criminal or nation-state organizations.

Client counsel engaged Nisos to investigate potential links to criminal or nation-state actors and to provide guidance on responding to a security incident.

A team of Nisos experts analyzed the information provided by the Client, including background logs, email addresses, IP addresses, and social media accounts related to the subjects.

- **Nisos found the subjects used falsified identity documents,** and copied specific language from the resume of another, unrelated individual.
- Several application IDs connected to the subjects' email addresses and IP addresses used at login have **also been used by North Korean threat actors.**
- Despite claiming extensive work histories, **there is only a limited online presence for the subjects**, including a LinkedIn account, two GitHub accounts, and a Slack community.
- Nisos investigators **attributed two individuals** who were likely associated with the person of interest based on social media and US-based address association.

The individuals discovered are part of a growing effort by the DPRK to exploit remote work to fund the DPRK's weapons development programs, as well as steal intellectual property (IP) and other sensitive information on behalf the regime.

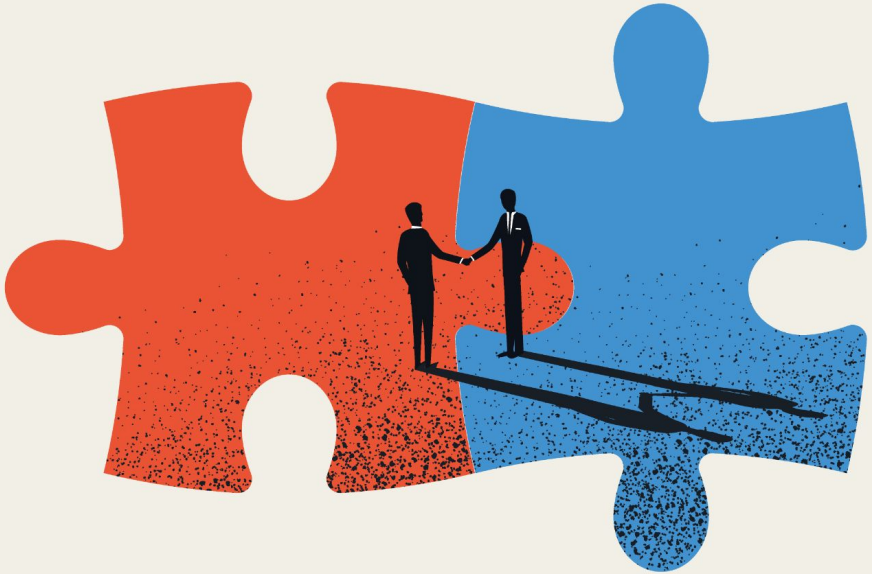
- **Legal and Law Enforcement Action**: The investigation resulted in actionable intelligence that supported law enforcement efforts to pursue legal action against the individuals involved.
- **Enhanced Security Response**: By working alongside legal counsel and law enforcement, Nisos supported the Client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

Case Study

Third-Party Intelligence

Protecting Assets and Identifying Risks

Nisos uncovers content leaks through an OSINT investigation and highlights **the importance of vigilant data protection**



SITUATION

Vetting individuals as part of mergers and acquisitions is a best practice that helps safeguard proprietary information from unintended exposure, ensures good security posture, and reduces the risk of financial loss.

The Client tasked Nisos with investigating a newly acquired company and a third-party individual posting sensitive information about the company on social media. This information posed both a security and a financial risk to the company as it involved intellectual property. The Client sought to mitigate the current threat and prevent future data leaks.

INVESTIGATION

The Nisos open source (OSINT) investigation focused on social media content analysis and verifying the individual's identity based solely upon a social media username provided by the Client.

- **Social Media Content Analysis:**
  - Nisos located the individual's social media profile and reviewed and catalogued all publicly available posts and videos.
  - We identified nearly 20 technical videos and documents containing company sensitive information, including those that predated the acquisition.
- **Identity Verification:**
  - Nisos cross-referenced public record sources to validate the individual's identity and obtain background information including employment and education history, current address, and technical credentials.

IMPACT

Nisos successfully identified the individual and documented key proprietary content on their social media profile underscoring a potential exposure of sensitive information.

- **Protect IP:** The Client was able to remove the sensitive information from the social media platform, and put preventions in place for future data leaks.
- **Due Diligence:** Given the individual was accessing and sharing sensitive data in the public domain before the M&A transaction, the Client recognized the importance of third-party intelligence as part of the due diligence process.
- **Data Leak Alerts:** The Client also engaged Nisos to monitor for sensitive company information exposure to alert them about any instances of proprietary information available in the digital domain including on the deep and dark web.

Let's **Connect**

Nisos is the human risk management company specializing in unmasking threats before they escalate. We are a trusted advisor who operates as an extension of security, intelligence, legal, and human resource teams to protect their people and business. Our intelligence-led solutions help enterprises make critical decisions, manage human risk, and drive real world consequences for digital threats.

For more information, visit **nisos.com.**

For more information:

visit: www.nisos.com
email: info@nisos.com
call: +1-703-382-8400
follow: LinkedIn