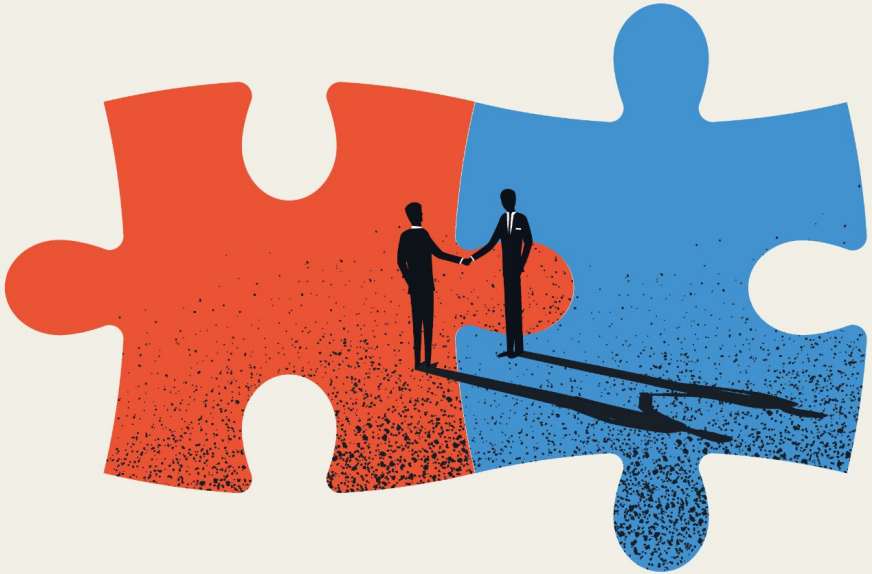
Case Study

Third-Party Intelligence

Protecting Assets and Identifying Risks

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



Proprietary and Confidential Information - Copyright© 2024 - All Rights Reserved - Nisos®

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.

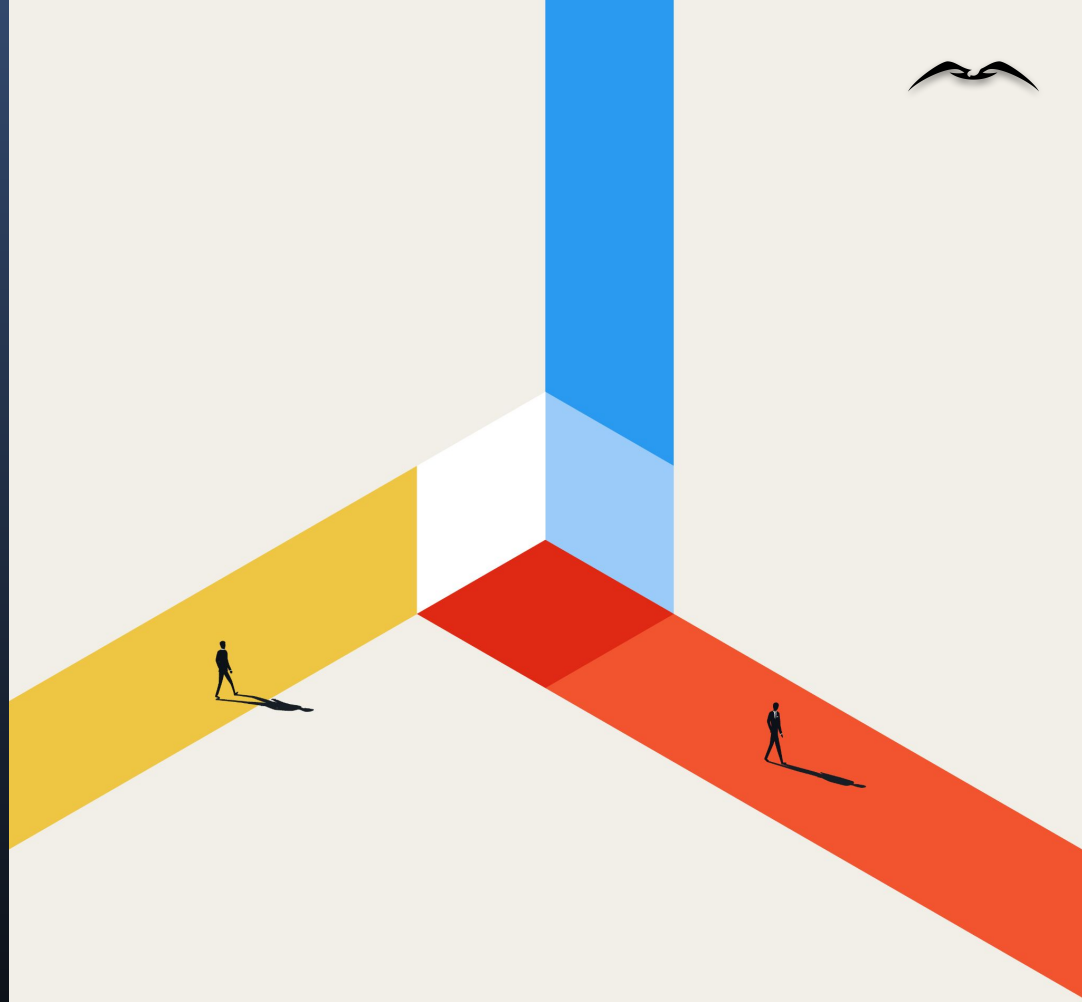
- **Protect IP:** The Client was able to remove the sensitive information from the social media platform, and put preventions in place for future data leaks.
- **Due Diligence:** Given the individual was accessing and sharing sensitive data in the public domain before the M&A transaction, the Client 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.

Case Study

Third-Party Intelligence

Supply Chain and Reputational Verification

Nisos **conducts thorough investigation to confirm reputational trustworthiness** of a global medical distribution company



Proprietary and Confidential Information - Copyright© 2024 - All Rights Reserved - Nisos®

SITUATION

Trust is a cornerstone of successful business operations, especially in interconnected global industries. A company's credibility significantly influences its business relationships and market standing. Undisclosed ties to questionable entities can undermine operations and erode stakeholder confidence. For organizations operating in complex environments, verifying the integrity of third-parties is a critical step toward mitigating risk and safeguarding their reputation.

When a prominent medical equipment distributor sought reassurance about its reputation and affiliations, they turned to Nisos for a thorough investigation.

The objective was to investigate the Client and its associated companies, with a focus on determining any historical ties to criminal, governmental, or otherwise suspicious organizations or persons.

INVESTIGATION

The investigation relied solely on publicly available and third-party information, with no use of software or hardware from within the company.

The investigation utilized open source (OSINT methodologies, drawing from public internet records, the deep web, and third-party databases.

Analysts collected detailed information on the Client's corporate structure, key personnel, affiliated entities, and any potential links to concerning organizations.

IMPACT

Nisos' investigation affirmed the Client's position as a credible and reputable entity in the medical equipment sector. By identifying no risks or suspicious ties, we provided the Client with confidence in their organizational reputation, enabling them to maintain strong partnerships and compliance with international standards.

The investigation revealed:

- The Client's business reputation is good, with no adverse legal findings or disputes.
- No ties to governmental, military, or criminal entities were found.
- Key executives hold roles in related companies with no negative records.
- Affiliated companies show strong alignment through shared boards and objectives.
- Corruption and sanctions databases revealed no allegations or red flags.

Case Study

Third-Party Intelligence

Third-Party Partnership Assessments

Nisos uncovers content leaks and highlights **the importance of vigilant data protection** in third-party relationships

Proprietary and Confidential Information - Copyright© 2024 - All Rights Reserved - Nisos®

SITUATION

Businesses must carefully evaluate the risks associated with their third-party partnerships, as these relationships can expose them to a variety of potential threats. Failing to address these risks can lead to serious financial and reputational damage. Understanding the complexities of third-party risks is a vital step in securing operations and strengthening overall business resilience.

Our Client, a leading organization in the nuclear energy sector, sought to assess potential cyber and geopolitical risks arising from its partnerships with key vendors and customers.

The investigation focused on identifying any breaches, insider threats, or geopolitical risks linked to these third-parties.

The goal was to evaluate the trustworthiness of these third-parties, to ensure the continuity and security of the Client's operations amidst a challenging and high-risk environment.

INVESTIGATION

Nisos investigators conducted a detailed assessment of the Client's key vendors and customers. Leveraging open-source and threat intelligence tools, the investigation aimed to uncover risks tied to insider threats, employee behaviors, and trustworthiness within the third-party ecosystem.

The investigation revealed:

- **Employee Concerns:** Multiple vendors and customers displayed indicators for insider threat, from employee dissatisfaction to leaked credentials, which could lead to unauthorized access or malicious actions.
- **Security Culture Gaps:** Several organizations lacked robust employee training and awareness initiatives, making them more susceptible to human-driven risks like phishing and credential misuse.
- **Geopolitical Influence:** Vendors tied to unstable regions were at heightened risk of intellectual property theft or employee compromise through coercion.
- **Organizational Stress Indicators:** High turnover and employee complaints suggested operational or cultural challenges that could amplify risk exposure.

The assessment found no immediate threats to the Client's infrastructure but highlighted significant risks associated with third-party vendors. These risks - particularly in relation to intellectual property, reputational damage, and potential cyberattacks - could have serious long-term consequences for the Client's operations.

Outcomes from the investigation included:

- **Enhanced Awareness:** Highlighted the human factors contributing to third-party vulnerabilities, from insider threats to geopolitical influences.
- **Improved Risk Mitigation:** Recommended tailored actions, including employee security awareness training, credential management improvements, and robust vendor oversight.
- **Proactive Solutions:** Helped the Client prioritize high-risk partnerships and adopt preventive measures, ensuring business continuity in a complex operational environment.

Let's **Connect**

Nisos is the Managed Intelligence Company®. Our services enable security, intelligence, and trust and safety teams to leverage a world-class intelligence capability tailored to their needs. We fuse robust data collection with a deep understanding of the adversarial mindset, delivering smarter defense and more effective response against advanced cyber attacks, disinformation, and abuse of digital platforms.
Learn more at **nisos.com**.

For more information:

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

Proprietary and Confidential Information - Copyright© 2024 - All Rights Reserved - Nisos®