CASE STUDY

Lighthouse Red Flag Report Prevents Proprietary Data from Being Taken by Departing Employee

A NATIONAL COMPANY SUSPECTED DEPARTING EMPLOYEES OF TAKING VALUABLE ENTERPRISE IP WITH THEM. LIGHTHOUSE IMPLEMENTED PROACTIVE RISK REPORTING AND PREVENTED IP EXFILTRATION BY AN EMPLOYEE TO AN INDUSTRY COMPETITOR.

Key Actions

- A global company partnered with Lighthouse to create a proactive departing employee program to prevent data loss and theft.
- Lighthouse forensics experts prepared Red Flag Reports for every departing employee that fell within a specific category of employees. Each report outlined the risks associated with the departing employee based on a skilled forensic examination of their activity and data.
- Soon after implementing the program, a Lighthouse Red Flag Report alerted the company to suspicious activity by a departing employee indicating a high risk for data loss.

Key Results

Because of Lighthouse's analysis and quick response, the company was able to:

- Prevent sensitive data from being disseminated outside the company.
- Avoid costly litigation associated with proprietary data loss.
- Reevaluate the departing employee's severance package due to breach of contract, resulting in additional cost savings.

LIGHTHOUSE

What they needed

A global company was dealing with an increased risk of data loss and theft from departing employees.

The company retains large volumes of proprietary data spread across their entire data landscape. Much of that data is also highly sensitive and would create a competitive disadvantage for the company if it were to end up in competitors' hands. The company was also facing a higher volume of employee turnover—especially within roles that had access to the company's most sensitive data (e.g., company executive and management roles).

The company was concerned that these factors were creating a perfect storm for data theft and loss. They realized they needed a better system to catch instances of proprietary data loss before any data left the company. Company stakeholders reached out to Lighthouse because they knew our forensics team could help them build a proactive, repeatable solution for analyzing and reporting on departing employee activity.

How we did it

Lighthouse forensics experts worked with the company to create a custom departing employee program for data loss prevention. With this program, Lighthouse experts prepared a Red Flag Report for every departing employee that fell within specified high-risk categories (e.g., employees above a specific seniority level, or employees that had access to highly sensitive company data, etc.).

Each Red Flag Report was prepared by a Lighthouse forensics expert and summarized the data theft risk associated with the underlying employee. Every report contained:

- A high-level summary of the risk of data theft presented by the employee.
- A collection of attachments with highlights and comments by the Lighthouse forensics examiner (for example, a list of files stored in an employee's personal cloud storage account, with an explanation of why that activity may indicate a higher risk of data theft).
- A forensic artifact categorization with associated risk ratings (e.g., if there were no suspicious search terms found during a scan of the employee's Google search history, the examiner assigned that category a lower risk rating of "1").
- Recommended next steps, with options for substantiating high-risk employee behavior.

Reports were delivered to a cross-functional group of company stakeholders, including IT, human resources, and legal groups.

The Results

The Lighthouse program very quickly paid off for the company. Soon after initiation, Lighthouse escalated a Red Flag Report for a departing employee that showed a high risk of data loss. Specifically, the Lighthouse forensics examiner flagged that the employee had connected two different external thumb drives containing sensitive company data to their laptop. This activity was flagged by the Lighthouse forensics examiner as high risk because:

- The employee had already been directed by the company to return any device that had corporate data saved on it; and
- The employee had previously indicated that they didn't have any devices to return.

As soon as Lighthouse escalated the Red Flag Report, company stakeholders scheduled an interview with the employee. This interview resulted in the employee admitting that they had taken corporate data with them, via the two thumb drives.

Because Lighthouse was able to quickly flag the employee's suspicious activity, the company was able to retrieve the thumb drives before the proprietary data was disseminated to a competitor. The company was also able to reevaluate the employee's severance package due to the breach of company policy, resulting in a significant cost saving.

Even more importantly, the company now has a proven, proactive, and customized solution for preventing data loss and theft by departing employees—implemented by Lighthouse's highly skilled forensics team.

Contact us to find out what Lighthouse can do for your business.

206-223-9690 | lighthouseglobal.com | info@lighthouseglobal.com

LIGHTHOUSE