CLEARFORCE CASE STUDY

# Mitigating Human Risk in the Utility-Energy Sector

## Introduction

The services that make up the energy sector are vital to America's function and progress. Virtually every aspect of daily life is reliant on the uninterrupted availability and flow of energy, whether it's electricity, water, or natural gas.

At the same time, this reliance makes the energy sector a prime target for malicious actors and cybercriminals looking to exploit the necessity of its supply chain. A survey of 1,700 utility companies found that 56 percent had experienced data loss or at least one operational shutdown due to cyberattacks in the last 12 months.

Companies that do not sufficiently prepare to counter these types of growing threats are facing mounting risks, and the consequences can be devastating. In 2018, a critical water utility company in North Carolina was the target of a cyberattack as it was still reeling from the impact of Hurricane Florence. In late 2021, a small utility company in Colorado was the victim of a suspected ransomware attack that wiped out 90 percent of their internal network functions and corrupted a large portion of their data.

Cybercriminals routinely look for weakened entry points to infiltrate their targeted company and carry out their attack. Unfortunately, these entry points can sometimes be employees whose organizational knowledge and access is used, either knowingly or unknowingly, against their employer. Understanding and mitigating the potential risks that could arise from a poorly managed or otherwise compromised workforce is known as human capital risk management, which is an essential but often overlooked form of

workplace management that deserves a place in any discussion about a company's goals and strategic priorities.

Being able to identify employee-related risks to your company allows HR managers the opportunity to intervene and address these risks with the employee before they snowball into something that could seriously compromise the integrity of the organization. Turning a blind eye or not having any visibility to these concerns puts a company at greater risk for a security breach, regulatory noncompliance, revenue loss, legal liability, or reputational harm.

This case study focuses on a large regional energy company and highlights findings that should be useful for business leaders in the utility industry, as they illustrate the benefits and importance of mitigating employee-related risks to an organization.

# Findings

## Employee safety

Within the first month of deploying, one employee who had been arrested for a DUI and open container but did not report that to the company as required. The Resolve platform discovered this incident with a high degree of identity confidence and alerted the company. The platform also provided information on the booking facility so the company could reach out for a copy of the report to support their internal investigation.

As an extra precaution, the company, as part of that investigation, also launched another background check to help confirm the arrest. Once the arrest was confirmed, the Resolve platform enabled secure information sharing within the larger insider risk team that included compliance, security, and other key stakeholders to elevate that employee to a higher level of monitoring.

## Insider Threat Mitigation

Prior to working with ClearForce, the company had a well-defined financial debt policy to prevent employees from being vulnerable to exploitation by outside bad actors or tempted

to take advantage of their position within the company for personal gain. However, there was no automated way to discover the delinquency, or detect the leading indicators without the employee coming forward.

Once ClearForce deployed, it discovered three employees who were in violation of the company's financial reporting policy. After these findings, the company was able to elevate their monitoring and inform not only other key stakeholders, but also their local managers to support mitigation options. In addition to the three employees who were not meeting reporting requirements, ClearForce also identified two other employees that had crossed secondary financial monitoring limits, prompting the insider threat team to open an initial investigation and again share information within stakeholder groups. After a review, the team found both employees to be cleared, but the security team flagged their records to ensure that no negative patterns would develop in the future.

Beyond detecting violations, the ClearForce Resolve platform identified other employees that were accruing rapidly increasing revolving debt and trending in a negative direction. With this early information, the company was able to inform local managers to engage proactively to help the employees and support their retention.

## Planning for the Future

With the deployment of ClearForce's secure workflow, the company will be able to maintain constant communication between its internal legal, compliance, and security departments, as well as support centralized security and risk monitoring for the dozen or so smaller power companies that it oversees. ClearForce, working closely with their insider risk and compliance teams supported enhancements in policy alerting development to better support the company.

# Key Takeaways

In this dynamic environment of evolving threats, the energy sector and utility companies must not only use every tool at their disposal to guard against increasingly savvy and intelligent cyberattacks, but understand how to synchronize technology, company policy, and best practices into an integrated solution. Key to this is internal communication,

documentation, and an active risk mindset. Engaging the services of a cutting-edge behavioral monitoring platform like ClearForce can help identify fault lines within an organization, as well as gain insights into potential growth areas. Most of all, it can provide a company with the best defense against potential insider threats and other unforeseen forces that could threaten their professional credibility or livelihood.