Logistics Company – Security Management Review

The Situation

Our client is a major logistics company with 1300 sites globally and 45,000 employees. The company comprises a holding company at the group level and six subsidiary organisations. Security has been managed individually at the level of each subsidiary which led to a range of security planning challenges:

- Over 300 contracted security companies with no standardised procurement or project management;
- $ 26 million per annum security spend with no oversight and significant potential for fraudulent activity;
- No coordination across security functions resulting in excessive costs and no identification of economies of scale; and
- No coherent approach to security across the Group, leading to inconsistency, inappropriate resourcing and a lack of assurance at the Group level that security risks were managed in line with the corporate strategy and enterprise risk management policies.

Our Solution

Our solution was to develop a concept of operations for the security function operating at Group level. The model was to involve a centralised security function to provide policy guidance and oversight of security operations, which would still be managed at the subsidiary level. This would allow for consistency and coordination across the Group while allowing the business units to customise the approach according to specific operational requirements. Various elements of the security management framework included: oversight, strategy, resources, cost management, security risk management, policies/plans/procedures, standards, stakeholder management and performance reporting and analysis.

Challenges

Several problems emerged during the implementation of this model:

- There was significant resistance to the framework implementation from the security management structures within the subsidiaries who did not see value in another layer of security management above them
- There was a significant mismatch of skills in the existing personnel resources with those required to perform the roles in the new management framework
- The enterprise risk management processes were not suitable for security risk management applications
- It was very difficult to engage stakeholders to the extent necessary and to generate the buy-in needed to effectively roll out the new policies and procedures.

Outcomes

To address these problems, we worked closely with the client and adjusted our approach to a more organisation-wide, management consulting approach to the problem. This included several streams of activity:

- A much wider stakeholder management focus, involving a broader range of internal stakeholders (the previous approach focused more on external stakeholders and regulators);
- A comprehensive change management program, looking in much more detail at the interdependencies between security functions and the broader operations of the business;
- Development of a clear case for change in the security framework that addressed the entire business rather than just security functions;
- A thorough workforce planning exercise in collaboration with the human resources department to help align existing skill sets with new roles and develop an incentives-based approach to skills transition; and
- Development of working groups, especially with Finance and Risk teams to devise appropriate methodologies that were aligned with the broader organisational processes.

As a result of this process, our client's and Lupine's approach to security risk management frameworks is now more oriented toward organisation-wide management of people and relationships, rather than purely systems and processes. This enables real behavioural and cultural change to ensure that security becomes an integral part of day to day operations and lays the foundation for more effective implementation of security systems and processes.