Case Study Three: Thomson Reuters Develops an Innovative System to Aid Horizon Scanning and Incident Management

How the Thomson Reuters Intelligence Management Dashboard helps protect its people and assets

Thomson Reuters, a global information company, operating in over 100 countries and winner of International SOS Foundation's 2016 Duty of Care Award in the category Innovation, wanted to increase the safety of its people and assets by improving its global 24/7 situational awareness. It developed a web-based Intelligence Management System to improve its capacity to absorb and process relevant information streams and in turn, enhance the risk-based decision-making process.

With the immense volume of information about travel and security incidents available to Thomson Reuters, determining the events which potentially affect its people or assets becomes a challenge. This need fuelled an internal project to find a consistent and systematic way of analysing the information. Also, there was a requirement to streamline the process of taking the right actions to support Thomson Reuters staff and protect assets in all locations. At the same time, this had to be achieved without requiring additional resources.

An expansive approach

The first step for Thomson Reuters was to restructure the way it handled travel and people risk. This responsibility was given to its Corporate Security Department. In the past, Corporate Security had focused more on physical security within the workplace. Now it was to adopt a holistic risk management approach, leveraging strengths of internal resources and existing partnerships and by doing so, managing all aspects of risk faced by their people.

Making the most of intelligence

It helped that Thomson Reuters already had good information resources, both internally, as well as through external partners. This included access to real-time or near real-time information about the latest protests, strikes, terror attacks, weather alerts and more. In addition, Thomson Reuters used International SOS' TravelTracker to track and communicate with travellers, and handled hundreds of alerts per month. Having this information at hand was a great start. The fact that there would be no additional costs in acquiring such information had the added benefit of gaining buy-in from senior management.

To make the most of this information, a new framework was needed. A web-based programme was developed to include a questionnaire and mapping functionality linked to a database. It is called the Intelligence Management Dashboard (IMD). Each Security Analyst must answer a number of short questions on each incident within 10-20 minutes of receiving an alert. It only takes a few moments to do so. Questions clarify aspects such as the time, date and location of the incident, including its proximity to Thomson Reuters offices. Other parameters that are established include incident classification: is it a protest, natural disaster, terrorist attack, a transport strike, etc. Any Thomson Reuters Assets affected (people or property) are recorded. Security Analysts are prompted to describe further events in their own words. They also classify the level of risk posed to the company and its assets. The Analyst then chooses what action to take. Options range from seeking more information to triggering existing crisis management procedures.

The questionnaire process is flexible to the type of event. If an incident is not near Thomson Reuters assets or where travellers are located, then the questions are abbreviated. Events with the potential to affect assets require more robust documentation and follow-up. This consistent, yet streamlined analytical approach allows Thomson Reuters to not only to effectively manage and process incoming feeds, but also ensures that the output is actionable and reliable.

A broad perspective

As well as reporting current events, the database covers thousands of incidents occurring globally in the last three years. The result is a wealth of data plotted against Thomson Reuters assets and people. Users can quickly view dashboard charts and other data to help them analyse any incident. For example, they can quickly measure the trends in frequency, seasonality and type of incident, by region, or over a set period.

IMD has led to increased performance on a cost neutral basis; Security Analysts can quickly process 300% more information feeds than before. At the same time, the quality of their work is consistent across the entire team, and the tool's web-based nature allows users to collaborate to eliminate any potential inaccuracies.

Other benefits

The IMD brings other benefits too. It can help support new business opportunities. It can be used to analyse optimal locations or risk mitigation strategies for offices, events, and projects.
Again, using both current and historical data. For example, if deciding where to locate an office, the information can be used to determine if the area is frequently subject to disruption caused by protests or a has a higher rate of security-related incidents.

The IMD also acts as a management tool. Managers can standardise job performance and set KPIs for Security Analysts according to how well they use the IMD system. For example, they can check the timeliness and accuracy of each report and compare results between different individuals. They can then review the competency of decision-making based on the information received and provide more targeted and bespoke training if warranted.

Daniel Salomonsson, Director, Risk & Compliance, EMEA & APAC who invented the Intelligence Management Dashboard summarises:

"The Intelligence Management Dashboard creates global situational awareness and allows desk officers to mitigate threats to the business quickly and effectively. It's great to know that nothing is missed. We can also review incidents retrospectively to see how they were handled and what can be improved. We believe this system has made a real difference."

Above Arnaud Vaissié, Daniel Salomonsson and Andrew Sharman.

STEPS	BEST PRACTICES IN INNOVATION
Step 1.	Take a holistic approach, encompassing all risks.
Step 2.	Use existing sources of information.
Step 3.	Assess information to establish relevance.
Step 4.	Deepen analysis with historical data.
Step 5.	Optimise opportunities to use the information.