Case Study Four: OCBC Adopts a Holistic Approach to Crisis Management

How OCBC developed a centralised system to better respond to events

OCBC winner of International SOS Foundation's 2016 Duty of Care Award in the category Thought Leadership forged a new path to adopt a holistic, enterprise-wide approach to dealing with crises and other events. The financial institution was better able to improve business continuity and meet Duty of Care obligations to employees.

Risk management is a crucial business function. Employers need to assess, prioritise and mitigate threats to their operations and people. OCBC recognised that it is critical to identify and manage these risks effectively to enhance resiliency. In much of the financial sector, risk management has been siloed; physical security, intelligence and business continuity functioned independently. At times, this could lead to slower decision-making, when rapid responses were required.

A fresh approach was needed: an end-to-end approach to detecting, monitoring and responding to any incident or crisis situation. This, in turn, required cooperation across the business and innovative thinking.

Integration and collaboration

The first move was integrating Physical Security (PS) and Business Continuity Management (BCM) into a single organisation. Its task is to provide governance and an oversight function to ensure business units are engaged and aware of the prevalent risks.

John Francisco, Head of Corporate Security explains: "With the integration of PS and BCM, OCBC is able to manage the full lifecycle from the initial response to business continuity. Its strength lies in having a barrier-free exchange of information and responsiveness during crisis situations."

This active governance role extends to risk assessment. A robust programme is in place to ensure regular assessments across the business to identify any risks or threats that employees or the company could face. It is again the process of collaboration — between business units and corporate security — that makes the difference.

Centralised operational systems

Next, a Global Incident Management Centre (GIMC) was created to detect, monitor and respond to crises or incidents. It actively examines a range of online information sources to spot emerging threats. Various security systems covering ATMs, individual branches, data centres and office locations are monitored centrally at the GIMC as well.

Information is assessed, tracked and updated at each operator's console and projected onto a video wall. This enables the GIMC team to understand the current threat situation holistically.

GIMC also maintains the Health and Safety dashboard where employees obtain information about travel classifications, air pollution information, contact numbers and all travel advisories.

Leading edge communications

Another key feature of this centralised system is the Incident Response Information System (IRIS). IRIS is linked to the HR database for up-to-date synchronisation of employee contact details. It can activate real-time crisis communication with all employees and perform employee roll-call health checks; communications can be targeted at specific groups (for example, staff in a particular location) and seek their responses. The status of the sent message, its receipt and the recipient response is tracked so employee wellbeing can be monitored in real-time.

Left Arnaud Vaissié, Marc Tse, Patrick Chew and Andrew Sharman. **Right** Singapore's busy financial sector.

Communications and instructions can be sent through various channels. These include SMS, voice messages and email to staff registered mobile, office phone and email accounts. IRIS has the capability to send 600 SMS messages and more than 300 emails per minute.

IRIS enables GIMC to communicate with multiple incident response teams, coordinate and track multiple complex tasks, collate and provide real-time updates to the Crisis Management Team and provide an auditable trail of actions.

IRIS takes away the need for CMT members to be physically present. It can initiate a Virtual Command Centre connecting CMT members by a conference call bridge and provide visual information on the status of the crisis via smart mobile devices.

Strengthened risk culture

Corporate Security has put in place awareness programmes and operational risk accreditation programmes to ensure employees are always ready to manage an incident or crisis. This is vital as OCBC expands into new territories. OCBC also organises Corporate Security Seminars to raise employee awareness of security, travel and medical risks in different countries.

The involvement of Corporate Security subject matter experts in this process is another example of this mindset change aimed at enabling broad collaboration throughout the business.

As John Francisco concludes: "In the past, we had numerous manual processes which were time-consuming and slowed our response time during crises. The GIMC and IRIS provide real-time information so that the responsible stakeholders can make informed decisions in a coordinated fashion. We can reach out to targeted employees quickly and in certain circumstances, locate them when required. This provides our people and our organisation peace of mind that the entire lifecycle of an incident is managed effectively."

STEPS	BEST PRACTICES IN THOUGHT LEADERSHIP
Step 1.	Integration and collaboration throughout the business.
Step 2.	Centralised operational systems.
Step 3.	Robust communications capability.
Step 4.	A strong risk-aware culture.