KPMG
cutting through complexity

HK Financial Services Business Continuity Management Forum
香港金融服務界業務持續管理協會

Business Resilience & Incident Response – Are You Ready?

April 2015

It is better to be prepared for an incident than to wait until it happens. As businesses become more reliant on technology and political situations remain changeable, the risk of a market-wide incident due to cyber attacks or extensive disruption is growing by the day. While many organisations have plans to respond to an incident, many of these strategies are only on paper and are not tested thoroughly in a real-life context.

Are you sure you are ready?

Market-wide disruption may be closer than you think

Business resilience and incident response have become increasingly hot topics. In crisis scenarios, financial institutions' operations can be impacted, including service interruptions and branch closures. Contingency plans are activated, such as arrangements to work from home or backup office arrangements to ensure normal business operations. For some businesses, a real-life crisis is their first opportunity to test the effectiveness of their contingency plans.

The regulators have long been emphasising the importance of business continuity for financial institutions. In general, financial institutions' heavy reliance on information technology has given rise to cyber threats and cyber attacks. In recent months, the world's largest companies, including well-known financial institutions and large corporations, have been targeted by increasingly sophisticated hackers, leading to large-scale service disruptions and data leakage.

As the financial system is closely connected to various financial institutions which support the system in one way or another, it has reached the point where a market-wide disruption must be thought of as a 'when' rather than an 'if' for all financial institutions. All key staff members, including top management and crisis managers, should be trained and ready for such an event.

Common Existing Business Continuity Drill Issues

Business continuity plans and incident response procedures

Most financial institutions have business continuity plans (BCPs) and incident response procedures in place to prepare for an incident. However, most BCPs and incident response procedures lack the clarity or the level of detail required for management to make the right decision when an incident occurs. For example, most organisations rely on the Crisis Management Team (CMT) to make decisions during an incident. However, since the established BCPs and incident response plans may not be able to cover the many possible scenarios, CMT management may not have the necessary knowledge or be aware of the key factors to make a quick decision.

Many organisations arrange regular BCP drills to enhance management awareness and test the organisation's incident response capabilities. The following drills are usually conducted regularly:

(1) IT disaster recovery drills

(2) Business continuity drills

(3) Fire evacuation exercises.

However, these drills are usually staged without taking into consideration the complexity of a real-life incident. Below is a description of the drills and their weaknesses:

Drills	Primary objective	Weaknesses
IT disaster recovery drills	To test whether the backup data centre can effectively support the IT systems in case of a failure in the production data centre	• The drill focuses on IT systems, with less emphasis on the wider operations (e.g. communication with customers and regulators). • IT disaster recovery drills are usually thoroughly planned to ensure their success. However, they do not take into account 'surprise' elements that may occur in a real-life crisis scenario. • The rise of cyber threats raises the question of whether the traditional disaster recovery arrangement – having replicated sets of IT environments in the production and backup data centre – is effective. In a cyber attack scenario, both environments deploying the same technologies will be vulnerable to the same cyber threat, rendering both production and backup environments inoperable.
Business continuity drills	To test the effectiveness of the established BCP	These drills are usually performed on a departmental basis, without considering an organisation-wide scenario that could affect several functions at the same time. Therefore, the interdependencies among various departments are often neglected in the drill.
Fire evacuation exercises	To test the response in case of a fire incident	A fire evacuation exercise is usually pre-planned and lasts for less than an hour. It does not consider the possibility of actual damage of office equipment after the fire or other impacts to business resulting from the incident.

Observations in Real-life Incidents

Real-life Incidents

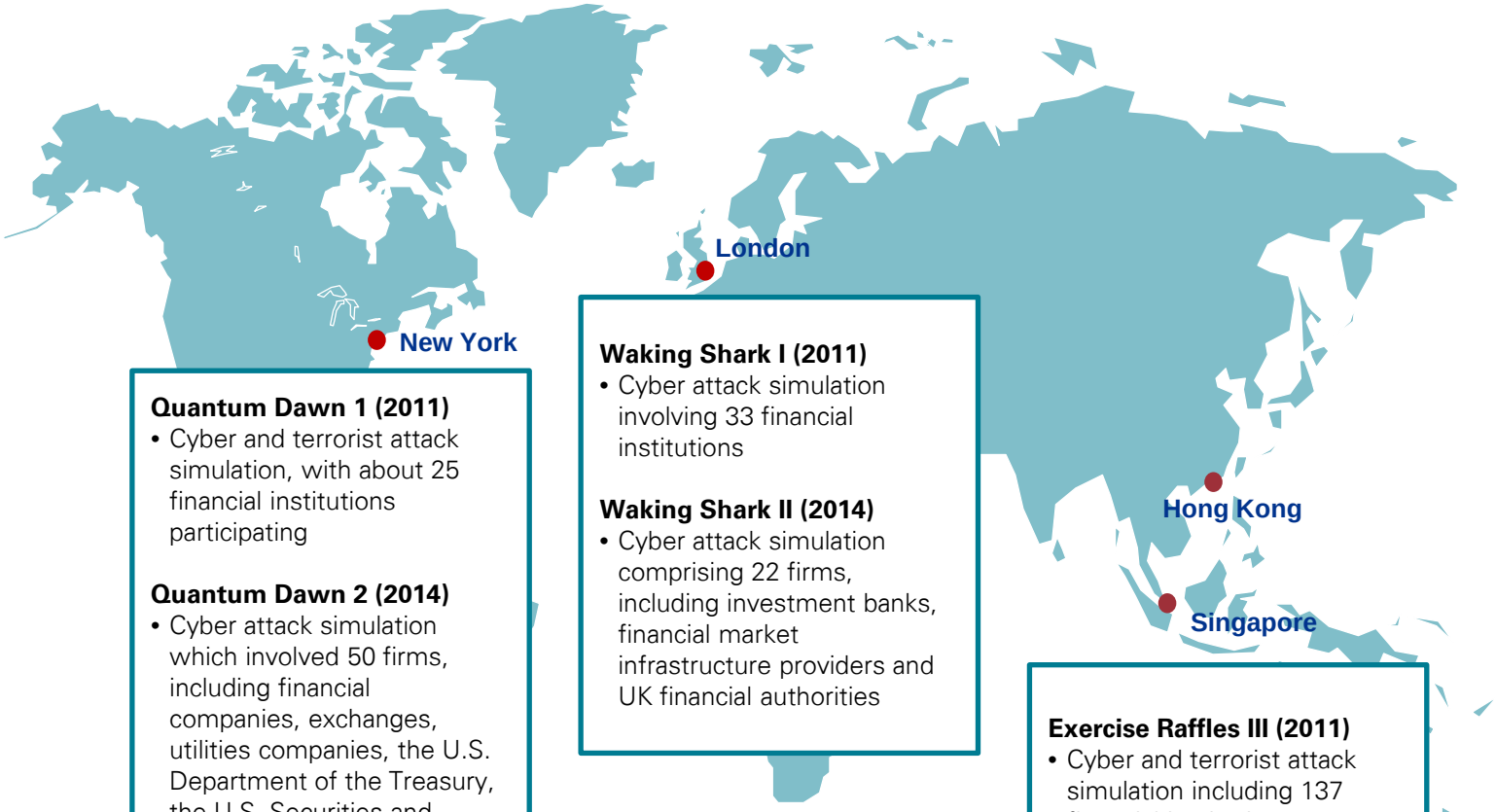
As some organisations may have experienced, real-life incidents seldom go according to plan. Every incident is different and it is very difficult to have a plan that can cater for all possible scenarios. Individuals' knowledge and experience are crucial to a well-prepared incident response function, and can only be accumulated through frequent practice and involvement in different types of real-life crisis drills. Our observations of real-life incidents usually involve the following aspects that cannot be completely planned in advance or learnt from regular IT disaster recovery drills, BCP drills or fire evacuation drills:

Real-life incidents	Common observations
Incidents usually occur unexpectedly and need to be addressed urgently, highlighting the need to make immediate decisions based on incomplete information.	The CMT is not confident enough to make decisions 'on the fly' due to lack of experience, leading to delays in crisis management.
Incidents can impact multiple business functions simultaneously. Different functions need to work together as one team to manage the crisis.	Business heads are not trained to work together in a crisis situation, leading to unclear responsibilities and confusion when managing a crisis.
Organisations will be pressed to respond immediately to never-ending queries from the media and customers. Established/existing press releases cannot address all the queries.	A substantial amount of time is required to vet press releases, which can lead to media speculation and negative publicity.
Regulators will require an immediate incident report, and thereafter, regular status reports until the close of the incident.	The compliance function is unable to fulfil regulatory reporting obligations due to a lack of clarity about the incident.

Most of the common observations above result from the responsible functions' lack of knowledge and experience, and these weaknesses can only be identified during real-life scenarios or a realistic crisis management drill. It is important that all parties responsible for managing a crisis are well trained so that they are prepared.

Crisis Management Drills around the World

Key financial services industry players, including financial services regulators, have acknowledged the need for realistic, market-wide exercises to enhance the effectiveness of financial institutions' crisis management capabilities in the event of market-wide disruptions. Such market-wide exercises have been conducted in a number of global financial centres including London, New York and Singapore.



Quantum Dawn 1 (2011)
- Cyber and terrorist attack simulation, with about 25 financial institutions participating

Quantum Dawn 2 (2014)
- Cyber attack simulation which involved 50 firms, including financial companies, exchanges, utilities companies, the U.S. Department of the Treasury, the U.S. Securities and Exchange Commission, the U.S. Department of Homeland Security, and the Federal Bureau of Investigation

Waking Shark I (2011)
- Cyber attack simulation involving 33 financial institutions

Waking Shark II (2014)
- Cyber attack simulation comprising 22 firms, including investment banks, financial market infrastructure providers and UK financial authorities

Exercise Raffles III (2011)
- Cyber and terrorist attack simulation including 137 financial institutions

Exercise Raffles IV (2014)
- Cyber attack simulation involving 141 financial institutions, the Singapore Exchange, financial market infrastructure organisations, as well as the Monetary Authority of Singapore (MAS)

Hong Kong has planned a similar exercise scheduled for Q4 2015 called 'WISE 2015', whose key objective is to enable both individual financial institutions and the financial sector as a whole to test their response plans in order to maintain effective and orderly markets and protect clients in the event of a market-wide disruption. WISE 2015 will be organised by the Hong Kong Financial Services Business Continuity Management (HKFSBCM) Forum, which consists of a group of senior business continuity management professionals employed in a wide cross section of firms in the financial services industry. KPMG will be supporting and contributing to this event.

WISE 2015

"A crisis is any situation which is **unexpected**, **unfamiliar**, **urgent**, **complex** and has **high stakes**. During a crisis, there is no luxury of time. Yet, decisions must be made, even though the situation may be unclear, and there is often conflicting information. **The worst decision in a crisis is no decision**."

Willem Hoekstra, *Chairman of the Hong Kong Financial Services Business Continuity Management Forum*

Around 20 business continuity management (BCM) professionals employed in Hong Kong's financial sector have joined forces to organise WISE 2015, a true industry-wide crisis management exercise where all participating Crisis Management teams (CMTs) can jointly experience a large-scale crisis situation and practice their ability to respond to it.

The objective of WISE 2015 is to enhance the:

- Understanding of systemic risks to the financial sector during major operational disruption, including cyber security threats, affecting the Hong Kong financial sector
- Specific management skills that allow managers to effectively make decisions during a crisis situation
- Preparedness of the financial services sector by providing the opportunity for organisations within the sector to test the effectiveness of their own crisis management process, contingency plans as well as communications across the financial sector and other stakeholders
- Overall readiness of the industry by integrating financial sector planning and crisis responses with relevant stakeholders.

For four hours on 9 October 2015, a 'disaster situation' will unfold in Hong Kong. Fortunately, this will only be a semi-live simulation. All participating CMTs, made up of senior management, will gather. A central simulation team will then use a secured internet portal to send so-called 'injects'. These injects are designed to look real and can take the form of mock-up news reports through web portals, simple situation reports on paper, videos, or simulated phone calls or emails with news. In addition, the simulation team will role-play third parties such as financial authorities, the media, emergency services and the government, thus creating a realistic picture of a crisis situation. Through dedicated phone lines and email addresses, the CMTs can communicate with the third parties. In addition, they can communicate and coordinate amongst themselves. One bank could, for example, take the lead and invite all CMT leaders to join in a conference call.

The scenario will remain undisclosed prior to the exercise, to simulate the element of surprise and the uncertainty that would come with a real situation.

The CMTs will need to respond to and manage the situation as if it were real, and decide on actions such as internal and external communication, and the potential use of BCP. A BCP could, for example, allow staff to work remotely, transfer activities to other branches, use work area recovery sites, activate IT disaster recovery solutions, or ultimately close down certain businesses.

The exercise remains contained. For instance, it is not intended that actual building evacuation takes place or real IT disaster recovery is activated. It is therefore referred to as a 'tabletop exercise'.

Most financial institutions already organise annual crisis simulations and/or 'tabletop walk-throughs' of particular scenarios for their own firms. WISE 2015 gives participating institutions a unique opportunity to jointly exercise, practice and develop their capacity to manage a crisis situation. Without any risk of repercussions or looking bad, every participant can enjoy a near-real experience of a major event jeopardising the continuity and potentially the very existence of their firm, so that if and when such event happens, the situation can be tackled with confidence and professionalism.

This exercise is organised by and for the industry, in close collaboration with experts and authorities.

Industry-wide exercises are already common in most other global financial hubs. In the UK and Singapore, similar exercises are organised by a collaboration between financial authorities and industry, mostly executed by consultancy firms. The scenarios that have been played include pandemics, terrorism, and most recently, a wide-scale cyber attack. In the US, the exercises are organised by SIFMA. These are, however, of a more practical nature and go beyond that of tabletop exercises.

For further information related to WISE 2015, please contact:

Willem A Hoekstra
Chairman, HKFSBCM
Tel: +852 6686 0939
E: willem.hoekstra@hkfsbcm.org

WISE 2015 project office
E: info@hkfsbcm.org

What can you do?

Every organisation's CMT should be familiar with its crisis management process and be able to make quick decisions during a crisis. The WISE 2015 event on 9 October 2015 will provide a good opportunity for organisations within the financial sector to test the effectiveness of their crisis management process, business continuity plans, and communication across the financial sector and other stakeholders.

KPMG can help you establish or update the existing policies and practices for dealing with a major crisis, from a people, process and technology perspective. We have tried and tested approach that cover: risk assessment, business impact analysis, strategy selection and development, crisis management, business continuity, and IT disaster recovery plan development and implementation (including testing, training and ongoing maintenance strategies). Our multi-skilled Business Continuity Management team, within our information security consulting group, combines business continuity and risk management experience across multiple industries, with a focus on developing practical and effective business continuity solutions.

Contact us

If you have any questions about the matters discussed in this publication, please feel free to contact us:

Henry Shek
Partner, Management Consulting
KPMG China
Tel.: +852 2143 8799
E: henry.shek@kpmg.com

Kelvin Leung
Senior Manager, Management Consulting
KPMG China
Tel.: +852 2847 5052
E: kk.leung@kpmg.com

kpmg.com/cn