HKFSBCM

# WISE2017

# Whole Industry Simulation Exercise

WISE2017: Whole Industry Simulation Exercise Evaluation Report

January 2018

**Hong Kong Financial Services Business Continuity Management Forum (HKFSBCM)**

Information Classification:  Public

# Table of Contents

# 1. Executive summary

WISE (Whole Industry Simulation Exercise) is a biennial, market-wide crisis simulation exercise for Hong Kong, organised by the Hong Kong Financial Services Business Continuity Management Forum (HKFSBCM), by the industry, for the industry. This year, Control Risks was retained to plan, provide secretariat support and deliver the exercise. HKFSBCM is a not-for-profit industry group of business continuity management professionals employed in the financial sector in Hong Kong. The objectives of WISE include:

- Increase awareness of contemporary and emerging threats facing the financial sector.
- Provide organisations with an opportunity to review their preparedness.
- Enable individual firms to exercise their crisis management plans and teams.
- Develop the skills to strategically respond to major incidents, including stakeholder management and coordination, crisis communication and crisis management skills.

WISE2017 was the second exercise of its kind in Hong Kong. The scenario included a cyber-attack and a physical terror attack. The senior crisis management teams (CMTs) of 45 financial institutions participated from their own offices in a realistic four-hour crisis scenario on 27 October 2017. Every CMT was connected to the central command centre, from which newscasts, emails, social media and market data were released in real-time, and to which CMT responses, such as updates to authorities, could be sent.

The exercise was a success and met its objectives. The following observations were made:

### WISE2017 met its objectives

- Observation 1. Industry-wide exercises continue to be an effective and efficient way to test and develop the industry's resilience
- Observation 2. For WISE2017, contracting a specialised firm (Control Risks) to help deliver the exercise relieved the strain and dependency on individual professional volunteers
- Observation 3. Different firms have different challenges
- Observation 4. Interactive scenario delivery makes the exercise more challenging and immersive
- Observation 5. Different levels of maturity when facilitating CMT exercise

### Crisis management capabilities vary across the industry

- Observation 6. There is a wide variety in structure and maturity in crisis management between different organisations
- Observation 7. Interaction between firms during a crisis can improve
- Observation 8. Social media is not generally used for crisis communications

### Firms distinctly recognise the cyber threat, but can improve their preparedness

- Observation 9. CSIRT (Cyber Security Incident Response Team) is common, but not many companies have a cyber incident response policy or cyber incident business response plan
- Observation 10. Most companies have integrated cyber incident response with crisis management structures

### Firms see physical threats as less challenging

- Observation 11. Physical terror threats are considered less concerning than cyber threats

## Suggestions for future exercises

- Improve planning and preparation
- Increase staff numbers to handle the interactive element of the exercise
- Deliver more bespoke scenarios
- Collaborate with other jurisdictions in the region
- Organise an industry-wide training programme based on best-practice regarding crisis management facilitation

## 2. Introduction

WISE is an industry-wide initiative conceived and organised by HKFSBCM. HKFSBCM is a group of senior business continuity management professionals employed in a wide cross-section of firms in the banking and securities industry. HKFSBCM aims to collaboratively address the concerns of business continuity in the industry. Through regular meetings, HKFSBCM discusses current affairs, looming threats, regulatory requirements and best practices in the areas of business continuity management and crisis management.

WISE2015 provided the first secure and managed platform for participating organisations to test and improve their crisis management and business continuity procedures. The CMT of each participating organisation faced a variety of primary operational disruptions to exercise their decision-making abilities and deliver a coordinated response to key stakeholders. The exercise was aimed at increasing industry resilience as a whole, in addition to exercising individual organisations' responses to specific threats. An estimated 400 senior managers from 25 organisations participated in the exercise, including local and foreign banks, finance companies as well as securities firms.

After the success of WISE2015, HKFSBCM embarked on organising WISE2017. The fundamental objective, to enhance the crisis resilience of the Hong Kong financial services sector with opportunities to evaluate and strengthen the capabilities of their CMTs, remained unchanged. In addition, the general set-up and delivery methods remained the same. However, this second instalment had some key differences:

- **Wider industry participation:** Participation increased from 25 to 45 organisations (including banks, securities firms and asset management companies).
- **Third-party management:** To ensure sustainability, an external party (Control Risks) was contracted to help plan, provide secretariat support and deliver the exercise together with the corps of professional volunteers.
- **Individual benchmark reporting:** For participating organisations to understand how they fare against the industry as a whole.

# 3. WISE

## 3.1. What is WISE?

WISE creates a unique opportunity for participating organisations to exercise their response strategies to a potential crisis situation, where the whole industry is affected. The first, smaller scale exercise was conducted in 2013, when a group of financial institutions individually but simultaneously responded to a simulated, unfolding pandemic crisis. In 2015, a full-fledged exercise – WISE2015 – simulated a wide-scale transport disruption, followed by a serious internet disruption and data leakage. WISE2017 focuses on potential cyber threats. Similar industry-wide exercises are organised in other countries, for instance the Quantum Dawn exercises in the US, Waking Shark in the UK and the Raffles/IWE exercises in Singapore.

## 3.2. What is crisis management?

Crisis management is the process by which an organisation responds to a significant event/issue that has the potential, if not managed appropriately, to harm the organisation, its stakeholders or the general public. The issues are typically so important, unexpected, extraordinary, urgent and/or sometimes emotional that normal management is insufficient. It involves procedures and plans, but also individual skills and practices. In many countries, banks jointly engage in industry-wide table-top exercises, where the CMT from each organisation discusses the response to a challenging hypothetical situation, or scenario, which unfolds from a central simulation centre. WISE is an industry-wide crisis management exercise where participating organisations jointly exercise their abilities to respond to different crisis scenarios.

## 3.3. WISE2017's objectives

The key objectives of the WISE2017 programme include:

- Increase awareness of contemporary and emerging threats facing the financial services sector.
- Provide organisations with an opportunity to review their preparedness.
- Enable individual firms to exercise their crisis management plans and teams.
- Develop the skills to strategically respond to major incidents, including stakeholder management and coordination, crisis communication and crisis management skills.

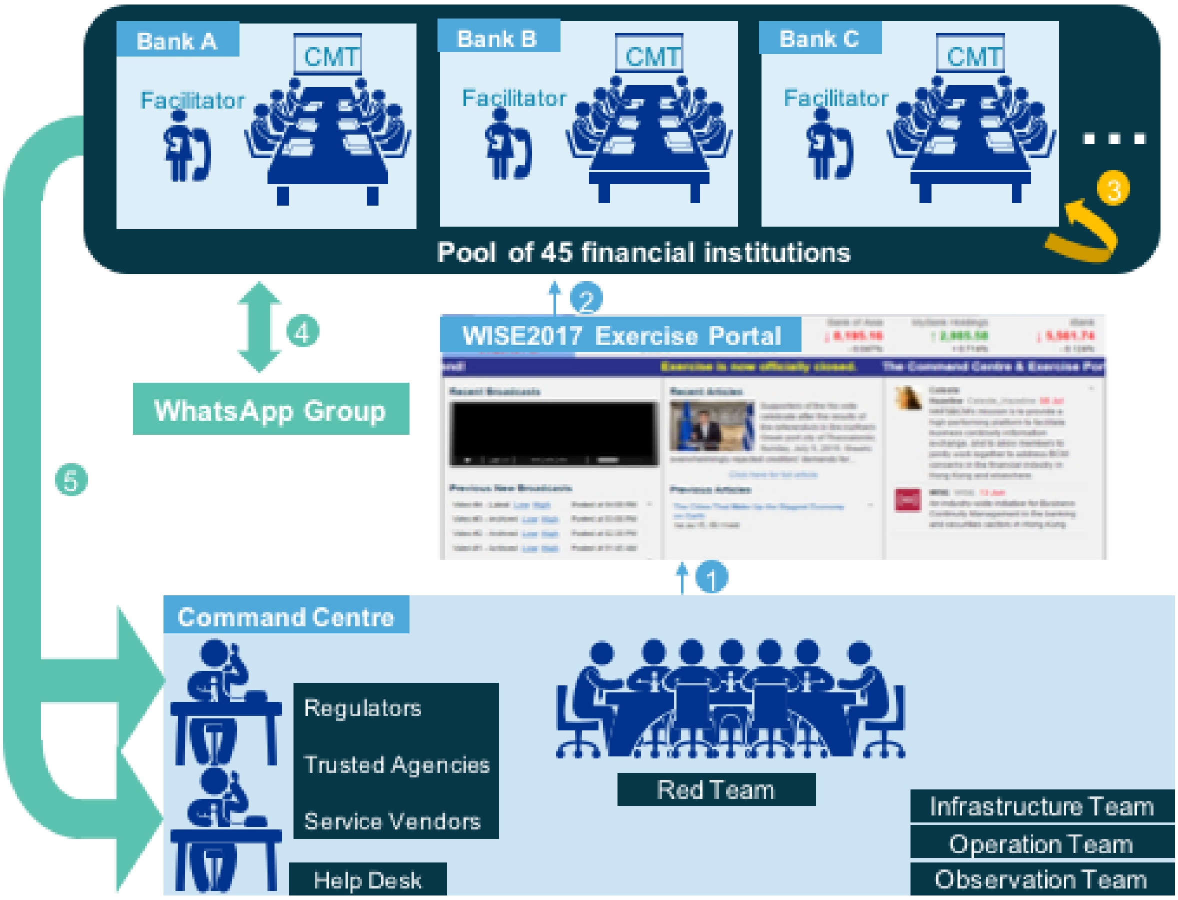
The benefits of participating for individual firms include:

- Cost-efficient way to undergo a high-quality crisis management scenario exercise.
- Full participation in a simulated exercise involving the CMT.
- Access to subject matter expert briefing sessions in the months leading up to the exercise.
- Regular briefings on crisis management and crisis communications.
- Complimentary train-the-trainer seminars for facilitators on effective crisis management.
- Company-specific confidential debriefing, benchmarking and industry report.

## 3.4. How is WISE delivered?

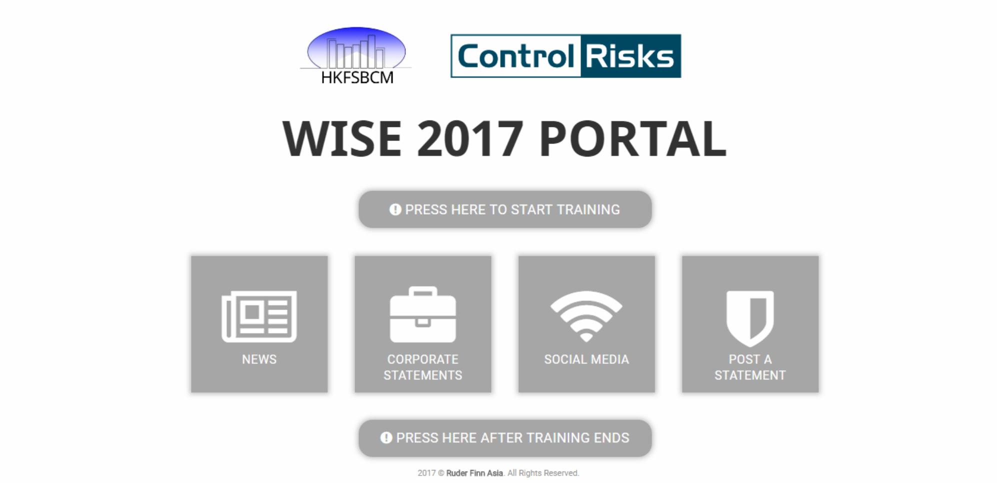
The WISE exercise is delivered in a table-top exercise to CMTs at a pre-announced date and time. What participating CMTs do not know, however, is the scenario that will unfold. Through so-called 'injects', which can be situation reports, emails, phone calls or newscasts, the CMTs are informed of developments of a crisis situation. A simulation team in another location controls these injects through a specially designed web portal, to which each firm has access. The CMT members will then respond, live, as if it was real. As this is a table-top exercise only, no actual actions are taken, for example, evacuating a building or activating a recovery site. However, they give these commands to the simulation team, who will, in real time, role-play several parties and respond as if the actions were real. This includes the confusion and misinformation that is generally an outcome of such situations.

## 3.5. Practical setup



- Each participating bank's CMT gathers in their own office.
- Through an exercise web portal, they see the crisis scenario unfold through injects. The portal shows an ongoing sequence of general news articles, news videos, stock market developments and social media.
- The developments presented on the portal are supported by phone calls and emails sent from the central command centre, creating an immersive scenario reality.
- The central command centre is staffed with dozens of subject matter experts to direct the events. Its proceedings are observed by a range of invited parties.
- The CMTs are expected to discuss the developing situation and decide on actions. These can include:
    - Calling or emailing parties such as the authorities, police and other entities/organisations. To this end, the subject matter experts in the command centre impersonate these entities to provide realistic responses.
    - Sending out general or social media statements. Through the portal, posted statements are visible to all participating CMTs.
    - Taking internal actions. These actions are confined to the CMT exercise.

## 3.6. The WISE portal



HKFSBCM Control Risks

WISE 2017 PORTAL

2017 © Ruder Finn Asia. All Rights Reserved.

The WISE portal is the main interface between the central command centre and every participating CMT.

HKFSBCM owns the URL, www.hkwise.org, which was used for the 2015 and 2017 exercises, although a different vendor, Ruder Finn, provided the portal back-end software and hosting. Access to the portal is password protected and ample time is given for testing, as several companies need to white-list the portal for functionality.

The portal automatically refreshes and gives access to all released injects throughout the scenario. Injects can take different forms, but typically include: newscast videos, news articles, social media and stock exchange ticker.

In addition, the portal contains static data, such as a directory of phone numbers to be used in the exercise: contact numbers for every participating organisation, as well as the numbers on the simulated parties in the central command centre.

New for 2017 was that the portal allowed for participants to make media statements. These public statements became visible to all participants.

Unfortunately, some participants reported they experienced a delay in receiving injects and it was noted the portal became slow at certain stages.

# 4. WISE2017

## 4.1. Participants

Where WISE2015 attracted 25 different financial institutions to participate, WISE2017 covered nearly double that number, with 45 participating organisations.

Although at the outset, all subsectors of the financial industry of Hong Kong were invited, the scope was later narrowed down to banks, securities brokers and asset managers only. Other companies, like exchanges, clearing houses, financial data providers, insurance companies, authorities and government were de-scoped to make the complexity of a scenario more manageable. The following organisations participated:

- Allianz Global Investors
- Australia and New Zealand Bank
- AXA Investment Managers
- Bank Julius Baer
- Bank of America Merrill Lynch
- Bank of China (Hong Kong)
- Bank of China International
- Bank of Communications
- Bank of East Asia
- Barclays
- BlackRock
- BNP Paribas
- BNY Mellon
- China Construction Bank (Asia)
- Chiyu Bank
- Chong Hing Bank
- Citi Hong Kong
- Credit Suisse
- Dah Sing Bank
- DBS
- Deutsche Bank HK
- Fidelity International
- Fubon Bank
- Goldman Sachs
- Hang Seng Bank
- Hongkong and Shanghai Banking Corporation
- HSBC GB&M
- ICBC Asia
- JPMorgan Chase Hong Kong
- Macquarie
- Morgan Stanley
- Nanyang Commercial Bank
- Natixis
- Nomura International (Hong Kong)
- OCBC Wing Hang Bank
- Public Bank (Hong Kong)
- Rabobank
- Schroder Investment Management
- Shanghai Commercial Bank
- Société Générale
- Standard Chartered Bank
- State Street
- UBS
- Wells Fargo
- Wing Lung Bank

## 4.2. Preparations

The organisation was structured into a Scenario Development Committee and a Planning & Logistics Committee, where HKFSBCM volunteers and specialists were teamed up with Control Risks. In addition, an Oversight Committee was formed where the board of HKFSBCM and Control Risks leadership monitored overall progress.

### Oversight

The WISE Oversight Committee was formed in October 2016 to oversee project development and designation of tasks for WISE2017. The WISE Oversight Committee comprised the board of HKFSBCM and the Control Risks project team. Meetings were held fortnightly throughout the project to ensure WISE2017 was kept on schedule, momentum and coverage.

The initial planning phase of the exercise involved driving awareness of WISE2017 across the industry. HKFSBCM board members and Control Risks team members met with a wide variety of organisations and officials to explain and promote the initiative. This included all relevant authorities, government departments, financial market associations, various Hong Kong police units, financial market parties and media.

The public kick-off took place in March 2017 with two industry-wide briefing sessions, hosted by the Hong Kong Monetary Authority (HKMA) and Securities and Futures Commission (SFC), respectively. With the support of the Asia Securities Industry and Financial Markets Association (ASIFMA) and the Hong Kong Association of Banks (HKAB), more than 50 institutions were invited to attend the briefings, including banks, clearing houses, securities companies and asset management firms.

*Note: HKFSBCM and Control Risks briefed the Office of the Commissioner of Insurance and the Hong Kong Federation of Insurers on WISE2017. Although members of the insurance sector did not participate this year, many individual insurance companies showed interest in joining the exercise.*

Registration for WISE2017 was open from April to August 2017. A total of 45 organisations registered to join the exercise. The fee for WISE2017 was set at HKD 45,000 per participating organisation, a marginal increase compared with WISE2015. HKFSBCM is a not-for-profit organisation; the fees were used to cover expenses.

## Planning, logistics and facilitation

In May 2017, a Planning, Logistics & Facilitation Committee was established, joining members of the HKFSBCM community with Control Risks' resources. This committee was responsible for preparing the designated WISE2017 facilitators for their tasks, as well as arranging logistics for WISE2017, including the physical and technical set-up of the exercise command centre.

### Training workshops

Two training workshops were held to prepare all participating institutions for the exercise and to give them more information about what to expect and how to prepare.

- The first briefing was held on 22 August 2017 at UBS' offices. This was a chance for participants to understand more on readiness for the exercise in October and gain insight into crisis management best practice. Willem Hoekstra, Chair of HKFSBCM, opened the session with a reminder of WISE 2017's objectives, and Julian Heath, Senior Partner at Control Risks, led the briefing with a session on "Crisis management – The contemporary challenge and a health check".
- The second briefing was held on 21 September 2017 at HSBC's offices. This session comprised a presentation by Nicolas Reys, Associate Director at Control Risks, on the topic of "Cyber threats to the financial sector: Trends and forecast for the year ahead." In addition, participating organisations were given a month of complimentary access to Control Risks' Cyber Threat Intelligence platform.

A number of useful tools were presented during these briefings, which remain available on HKFSBCM's website.

### Facilitation

Every participating CMT had to identify a facilitator. The delivery of WISE depended strongly on the actions of the facilitator. Their tasks included:

- Arrange logistics: ensure the CMT members are invited, a room is available, the technical facilities, such as phones, web portal and projectors, are in place and tested.
- Although facilitators should not be part of the CMT or provide answers or solutions, they ensure discussions do not stall, for example, by injecting prompting questions or giving immediate feedback on the proceedings in the CMT. So, although they do not help the CMT to respond, they ensure members stay focused and the scenario does not leak into the "real world".

- Be the eyes and ears of the central command centre. If the injects become overwhelming or are too slow, are misunderstood or fail to engage, the central command centre has some flexibility to change course or pace for that specific CMT.

Three briefing sessions were organised to prepare the facilitators for their role: introduce the portal for delivering injects, run through the high-level scenario and discuss logistics to ensure the successful delivery of the exercise within their organisation.

- The first briefing was on 19 September 2017 at Nomura's offices.
- The second briefing was on 9 October 2017 at Bank of America Merrill Lynch's offices.
- The third briefing was on 25 October 2017, hosted online via WebEx.

These briefing sessions were supported by a comprehensive facilitator information pack, which included an outline of the scenario and a range of supporting information. The pack also included materials and a DVD with all injects in case the live portal could no longer be used.

**Command centre**

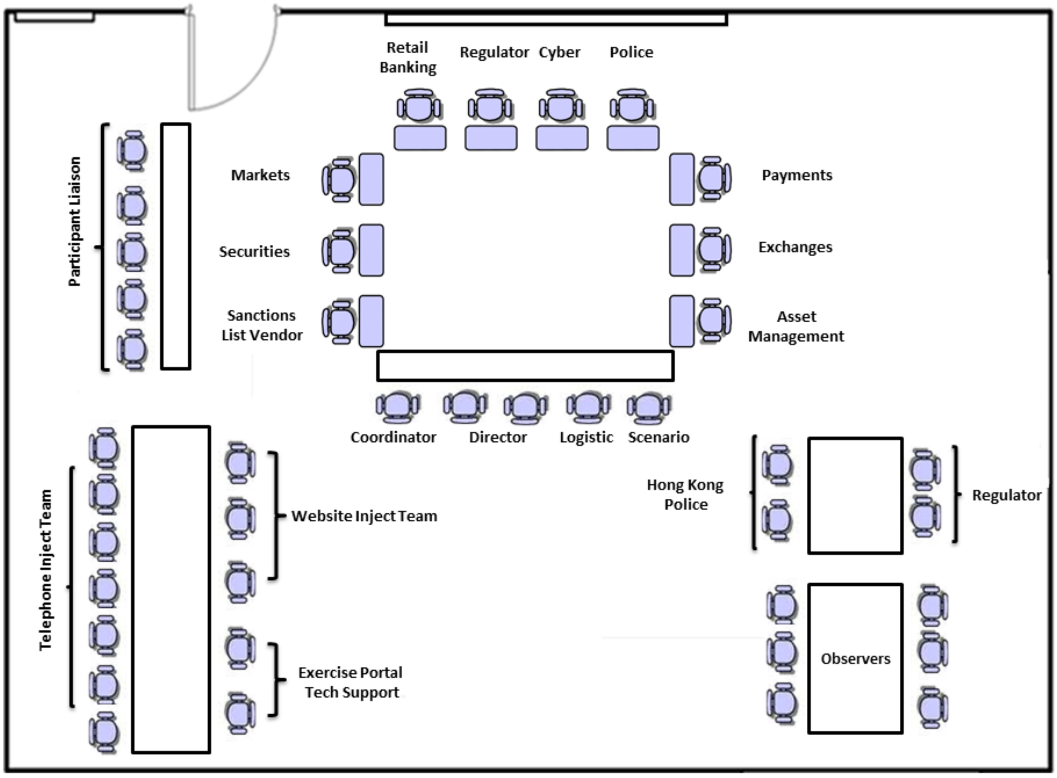
The command centre is the heart of the exercise. This is where central control of the unfolding scenario injects took place, but also where the outside world was simulated. Volunteers took up positions in the telephone injector team, participant liaison team and role-played various authorities, including law enforcement, regulatory authorities and journalists. This also included a red team that could deliver more challenging or customised injects where needed.

Several observers joined the command centre to witness the delivery of the exercise:

- Hong Kong Monetary Authority
- Securities and Futures Commission
- Hong Kong Police Force
- The Monetary Authority of Singapore
- Central Bank of the UAE

The command centre was equipped with 32 desks with laptop and dedicated phone lines, plus 10 seats for the external observers. Because of its pivotal importance, the command centre was set up days in advance, while dry-runs were rehearsed multiple times in the weeks leading up to the event.

Command Centre



## Scenario development

The Scenario Development Committee was established in early May 2017. The team was tasked to develop the scenario, as well as manage the production of the various injects. The exercise scenario included two main threads: a cyber attack and physical security incident.

The design and development of each scenario thread was allocated to a member of the Scenario Development Committee. Once a thread was drafted, this was shared with the full committee for feedback and revisions before being split into injects and aggregated into the master events list by Control Risks. The scenario threads were divided into several independent sub-events or incidents, with each inject allocated its own time segment. The scenario injects were based on the exercise objectives and requirements, and alluded to topical trends and incidents. For instance, a ransomware incident was included to reflect recent cases of cyber criminality. The aim was for the scenario to offer participating organisations the opportunity to estimate potential impacts of each incident, and provide an initial response within a short period of time. To add to the realism and stress within the CMTs, some injects were released simultaneously, e.g. compromise of sanctions lists, compromise of order management systems and a ransomware attack.

The following factors were considered during the development of the scenario:

- Level of realism
- Type of threat
- Location of the threat
- Optimal date and time for delivery within the exercise timeframe
- Differing levels of crisis management 'maturity' in the participating organisations

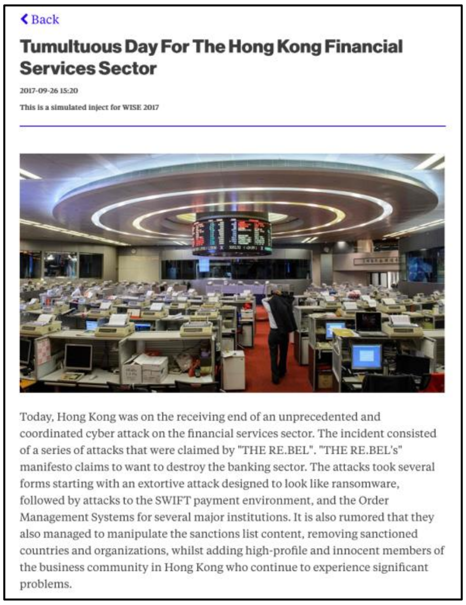
All parts of the scenario needed to be realistic, plausible and challenging. The scenario was designed to be extensive and challenge each participating CMT, helping organisations to identify potential areas of weakness. In addition, the exercise was structured to encourage interaction and cooperation with external parties, and seek advice and collaborate under challenging circumstances.

During the inject production period, the Scenario Development Committee considered the following criteria:

- Ensure the scenario is sufficiently challenging to incite in-depth discussions within the CMT
- Ensure the scenario covers the specialisations of all participating organisations, e.g. securities, asset management, retail, private banking firms
- Confirm whether the scenario is credible and topical for the Hong Kong financial services sector, while avoiding geopolitical tensions or sensitivities
- Estimate the consequences of disruption caused by the scenario to avoid overwhelming the industry, which might lead to closure of the market. One of the key aims of the exercise is to challenge the industry without closing the market
- Ensure the scenario is sufficiently diverse to encompass systemic risks across the market, rather than risks that could be managed by a single organisation in isolation

In preparing a realistic timeline for the scenario, it was important to allow sufficient time for participants to understand and respond to the various injects.

To ensure the effectiveness and credibility of the scenario, the WISE2017 Organising Committee invited several trusted organisations to provide advice and review the master events list. The Scenario Development Committee called upon the expertise from a wide variety of subject matter experts, including industry professionals from the HKFSBCM forum, HKMA, SFC, Hong Kong Police Force (most notably the Cyber Security and Technology Crime Bureau and the Critical Infrastructure and Security Command Centre), the Stock Exchange of Hong Kong, Bloomberg and Control Risks. This approach presented valuable insights and reinforced the credibility of the exercise.



**Tumultuous Day For The Hong Kong Financial Services Sector**

2017-09-26 15:20

This is a simulated inject for WISE 2017

Today, Hong Kong was on the receiving end of an unprecedented and coordinated cyber attack on the financial services sector. The incident consisted of a series of attacks that were claimed by "THE RE.BEL". "THE RE.BEL's" manifesto claims to want to destroy the banking sector. The attacks took several forms starting with an extortive attack designed to look like ransomware, followed by attacks to the SWIFT payment environment, and the Order Management Systems for several major institutions. It is also rumored that they also managed to manipulate the sanctions list content, removing sanctioned countries and organizations, whilst adding high-profile and innocent members of the business community in Hong Kong who continue to experience significant problems.

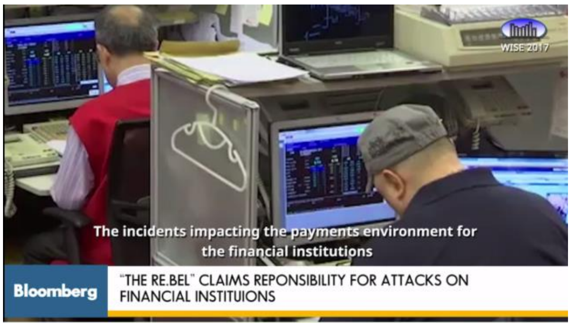
## Inject production

Individual scenario injects were designed for delivery to participating organisations through the WISE2017 online exercise portal. The communications consultancy, Ruder Finn, was subcontracted by Control Risks to provide the exercise portal platform and design the aesthetic aspects of the scenario injects. Each organisation was provided with three unique login credentials to access the portal.

Examples of scenario injects:

- News videos and articles from simulated Bloomberg sources
- A “live” ticker to update participants on market movements, simulating the Hang Seng Index
- Static social media posts, e.g. Twitter, Facebook posts, Instagram
- A “live” Bloomberg ticker to highlight important scenario information (e.g. breaking news) and important exercise announcements (e.g. commencement of the exercise)
- Press releases/corporate statements

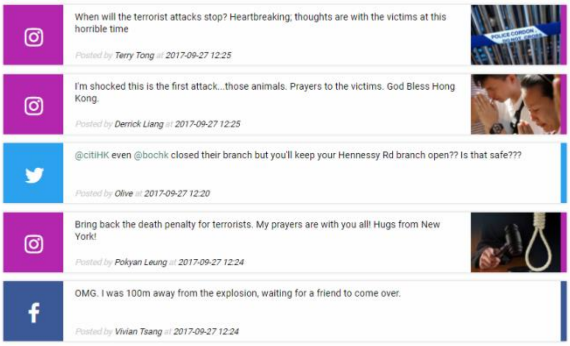
As well as receiving scenario injects, participants could post press releases and corporate statements to the online portal to simulate their crisis communications strategy. Any press releases/corporate statement posted on the portal could be viewed by other participants and members of the command centre. Once a post had been made, it was not possible for the organisation to edit/delete it, which reflects the process in a real-life crisis situation.



WISE 2017

The incidents impacting the payments environment for the financial institutions

Bloomberg "THE RE.BEL" CLAIMS REPONSIBILITY FOR ATTACKS ON FINANCIAL INSTITUIONS



When will the terrorist attacks stop? Heartbreaking; thoughts are with the victims at this horrible time

Posted by Terry Tong at 2017-09-27 12:25

I'm shocked this is the first attack...those animals. Prayers to the victims. God Bless Hong Kong.

Posted by Derrick Liang at 2017-09-27 12:25

@citiHK even @bochk closed their branch but you'll keep your Hennessy Rd branch open?? Is that safe???

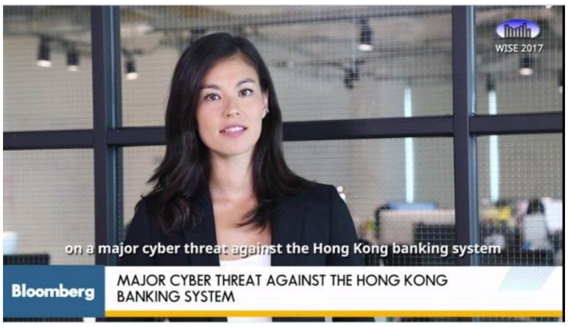
Posted by Olive at 2017-09-27 12:20

Bring back the death penalty for terrorists. My prayers are with you all! Hugs from New York!

Posted by Pokyan Leung at 2017-09-27 12:24

OMG. I was 100m away from the explosion, waiting for a friend to come over.

Posted by Vivian Tsang at 2017-09-27 12:24

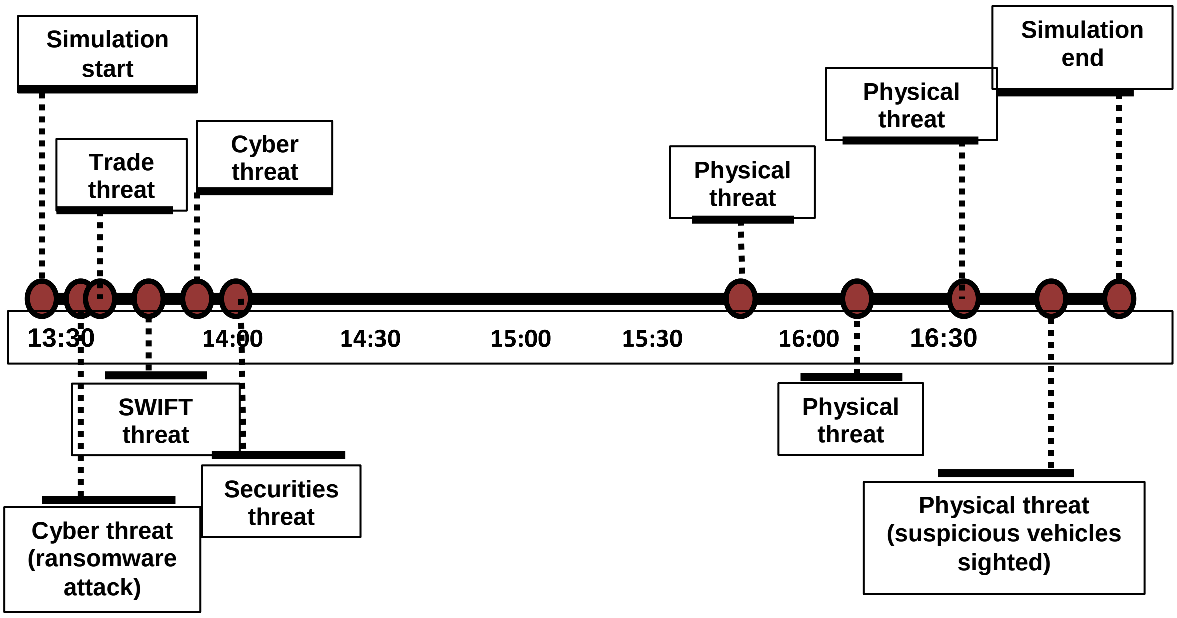


WISE 2017

on a major cyber threat against the Hong Kong banking system

Bloomberg MAJOR CYBER THREAT AGAINST THE HONG KONG BANKING SYSTEM

## 4.3. Scenario



The scenario consisted of two distinct crisis situations, spread out over two virtual days. A time-jump was made during the four hours real time of the exercise, moving the scenario to the next day.

The first situation involved a set of parallel storylines regarding cyber threats. The first strand was a malware infection on a major Hong Kong retail bank's core banking system. Due to the interdependencies of participating organisations on order management systems, this required firms to gauge local impact and manage communications to regulators and customers. The second strand was related to a SWIFT payment system compromise. The third related to ransomware on the order management system with breaches potentially affecting the day-to-day running of the banks and their clients/customers. To ensure this was addressed by all participating firms, the portal reflected the names of all firms to ensure this was discussed. Following the ransomware attack was a sanctions list hack, which meant some firms were not conducting accurate Know Your Customer checks and therefore at risk of regulatory reprimands. Within the scenario, several injects involving comments from regulators (HKMA and SFC), the Hong Kong Financial Secretary, as well as market volatility added pressure for firms to respond. As firms were responding to previous injects, a DDoS (Distributed Denial of Service) attack interrupted a number of banks' internet banking services, causing widespread public impact.

The second situation began after a time jump moving the events to the following day and centred around a physical terror attack in Hong Kong with focus on the financial sector. To ensure relevance, the impact areas were carefully considered to cover the geography of all participating firms. While the first day focused on business impact following cyber threats, the second day tested the CMTs' crisis management, employee accounting and communication processes. External pressure from the public was intensified using social media posts via the portal, forcing participating firms to actively respond rather than relying on default media comments. In tandem, extreme market volatility as a result of the events from the previous day exacerbated the situation, requiring CMTs to prioritise response decisions.

# 5. WISE2017– Findings and observations

The general observations of WISE2017 can be summarised as:

- WISE has met its stated objectives
- Crisis management capabilities vary across the industry
- Firms distinctly recognise the threat of a cyber incident, but can improve their preparedness
- Firms see physical threats as less challenging

## 5.1. WISE has met its stated objectives

There were four objectives set for the WISE programme:

- Increase awareness of contemporary and emerging threats facing the financial services sector
- Provide organisations with an opportunity to review their preparedness
- Enable individual firms to exercise their crisis management plans and teams
- Develop the skills to strategically respond to major incidents, including stakeholder management and coordination, crisis communication and crisis management skills

These objectives have all been met, but led to the following observations.

### Observation 1. Industry-wide exercises continue to be an effective and efficient way to test and develop the industry's resilience.

Crisis management exercises are seen as an effective way to develop the specific skills required to face a crisis or major incident. Most firms already organise scenario exercises for their CMTs, either through an external consultancy firm or fully in-house. Organising an exercise requires significant logistical effort, as well as in-depth subject matter expertise over a very wide area, ranging from IT and physical security to specific business processes and forecasting market sentiments. Organising an industry-wide exercise allows for a better scenario, dwelling on more subject-matter expertise, while at the same time being more efficient by sharing efforts. A joint exercise also creates uniformity of crisis management structures between firms, based on industry best practice, rather than individual or team preferences.

From a global perspective, WISE can compare itself with initiatives run by other financial hubs around the world. What makes it unique, however, is the "by industry – for industry" concept, rather than being an authority-led initiative. WISE is initiated and organised directly by business continuity management professionals from the industry, making it less prone to politics or tick-the-box attitudes, and allows access to the collective expertise of nearly the entire industry.

The delivery model where each CMT gathers in their own office, using scenario injects through a web portal operated by central command centre, works well.

The significant increase in participation compared to the previous exercise is evidence of this formula being successful.

There are, however, limitations to this exercise. It is clearly unrealistic to expect all members of a CMT to be gathered in a room, waiting for a pre-announced crisis to occur. A real-life situation requires escalation and invocation decisions to be made, and then attempts to swiftly gather individual members in a conference call or crisis room – assuming phone lines and/or the office is still available. Another limitation of this simulation exercise is the stress factor. Although there will be some peer pressure, an exercise in this format will not simulate the levels of stress and anxiety a real event might cause.

### Observation 2. For WISE, contracting a specialised firm to help deliver the exercise relieved the strain and dependency on individual professional volunteers.

WISE2015 was a big success. It was, however, fully dependant on a vast number of professional volunteers, several of whom contributed many hours, if not days and weeks, of their time. This led to concerns over the sustainability of the WISE initiative. One of the WISE2015 conclusions therefore was to seek a commercial partner to help deliver the exercise, while maintaining the unique benefits of WISE: being organised by an independent not-for-profit body of professionals. Following a market evaluation and request for proposal process, Control Risks was selected to ensure continued momentum in the logistical preparations for WISE2017, and also contribute experience and expertise. This formula of collaboration and synergy with a contracted party proved successful, although the effort and contributions put in by the professional volunteers should not be understated.

### Observation 3. Different firms have different challenges

The WISE2017 scenario was written to challenge a wide array of different businesses and functions. The simulated events were designed not only to engage the CMTs of the very different participating organisations, such as banks, brokers and asset managers, of varying sizes, but also to engage all functions within the CMTs, such as front office traders, legal, compliance, operations and HR.

Undeniably, the challenge for including a wide range of organisations was higher than for a single-product firm. Although the concept of individual bespoke scenarios was considered, WISE2017 did not go that far. Nonetheless, certain injects were only released to organisations for whom it was relevant, and some arrangements were available in the central command centre to allow scripted ad-hoc injects if a particular CMT demonstrated a high level of crisis management ‘maturity’.

As expected, not every firm was equally affected or challenged by the different scenario story lines, but generally there was captivating engagement overall.

### Observation 4. Interactive scenario delivery makes the exercise more challenging and immersive

Compared to WISE2015, this exercise not only allowed for, but solicited more active interaction of CMTs with the outside world. A team of knowledgeable role players in the central command centre were contactable, not only by phone, but also by email. In addition, the portal allowed for postings in the exercise public domain, by means of press statements or social media posts. This increased interaction was successful and led to more participant engagement. It was no longer an option to passively “watch TV” and maintain an “I would probably do that…” attitude. Instead, real actions could be taken and consequences faced, within the confined and safe space of the exercise.

### Observation 5. Different levels of maturity when facilitating CMT exercise

During the preparation of the exercise it was soon noticed the levels of seniority and experience of the CMT members varied significantly across the participating organisations. Equally, a wide variety of seniority levels were observed among the CMT chair and facilitator. These two leading roles are crucial for the success of the exercise. The CMT chair needs to lead the team through the challenges presented, while the facilitator needs to have enough stature and credibility to observe and give feedback to the team, which is likely more senior to them.

For several facilitators, this was the first exercise of its kind in which they participated. Not knowing what to expect of the exercise put them at a disadvantage. An experienced facilitator would know the “tricks of the trade,” for example that facilities like multiple screens, whiteboards and a printer in the room can make the exercise considerably easier to manage. The post-exercise survey showed nearly half of the facilitators did not have a well-prepared CMT room with multiple screens to view the WISE2017 portal.

During the three briefings before the exercise date, Control Risks and the WISE2017 team made substantive efforts to train and prepare the facilitators for their role. To make the experience less dependent on individual skills, the facilitators were also provided with a list of moderator questions to prompt activity or reinvigorate stalled discussions.

## 5.2. Crisis management capabilities vary across the industry

A CMT that follows best practice will: have a clear decision maker and structure, process and mandate, be well-organised with a senior crisis director and all relevant officers immediately present, properly consider facts, assumptions and implications before taking decisions, assign a minute taker to log decisions and actions, form sub-groups, allow strategic crisis management discussion without being interrupted by news events, but at the same time continue to closely monitor events and outcomes.

### Observation 6. There is a wide variety in structure and maturity in crisis management between different organisations

Some firms have a well-structured, mandated and experienced major incident or crisis management team. They swiftly activate the crisis management structure as habitual response to an incident. The team uses all of its available expertise without letting this delay a prompt response.

However, other organisations rely on ad-hoc gatherings in incident situations, which can be overwhelmed by events. Some teams are dominated by individuals, instead of using all members.

Throughout the exercise, many organisations did not clarify the roles and responsibilities of their CMT members. Consequently, there was some confusion over the delegation and execution of tasks during the simulation. A clear CMT structure and better delegation of tasks will increase the efficiency and effectiveness of resolving a crisis situation.

In the post-exercise self-assessment survey, several firms scored themselves in a lower quadrant with regard to efficient decision making and clear communication of these decisions. The CMT chair of nearly 20% of the firms did not record, track or follow-up on decisions taken. A similar percentage did not efficiently assess or respond to the situation. Furthermore, the majority of organisations did not set aside time to summarise and review information and actions. Especially when events happen quickly, it is important to set aside time to ensure the whole CMT understands all relevant information and there is a level of consensus on decisions.

The survey showed only 64% of the firms prioritised staff safety, and only 66% considered the impact of the scenario on their supply chain. Less than 50% of all firms submitted their responses to the authorities on time.

Despite the above, the majority of CMTs claimed in their post-exercise feedback that their approach to decision-making was effective during the exercise.

### Observation 7. Interaction between firms during crisis can improve

One of the major goals in conducting WISE2017 was to provide an opportunity for participating organisations to practice interbank and interagency coordination. The majority of participating organisations' CMTs engaged heavily with their internal specialist departments, such as IT, information security and operations.

Similarly, in the command centre, simulated groups, such as the Hong Kong Police and regulators, were heavily relied on to provide clarification and advice.

While participating firms were provided with their peers' contact details as part of the exercise, this information was not frequently utilised to discuss incidents, compare notes and benchmark response.

### Observation 8. Social media is not generally used for crisis communications

Most firms have formal procedures and processes for communicating with their stakeholders, most notably with customers (86%). A similar percentage has identified key external audiences, messages and preferred communication channels, and an effective media engagement protocol.

For internal communications, the majority of organisations benefitted from automated and manual call trees. However, while some organisations were well-prepared in the event of a telecommunications failure, others did not have a contingency platform in place.

Social media plays an ever-increasing role in shaping the general public's opinion, and can do so swiftly. Yet, very few companies actively monitor and engage with social media during crisis situations, whereas this would be the media of choice for customers and wider public to vent frustrations. Managing a response to social media frenzy can be important to limit damage to the brand and reputation of the individual firm, but also to the industry at large.

Clearly, the demographics and nature of the clients play a substantial role here. Retail banking markets will clearly be more affected than wholesale brokerage services in this respect.

## 5.3. Firms distinctly recognise the threat of a cyber incident, but can improve their preparedness

With an average score of 4.13 out of 5, the simulated SWIFT compromise was considered the most challenging scenario by participants, followed by the compromised order management system, which had a score of 3.47.

### Observation 9. CSIRT is common, but not many companies have cyber incident response policy or cyber incident business response plans

Half of participants do not have adequate or tested plans in place to deal with cyber extortion.

### Observation 10. Most companies have integrated cyber incident response with crisis management structures

Only 84% of the organisations integrated cyber incident response with the crisis management protocols. Note: A contact number was provided for the RE.BEL, the attacking entity, yet only one company tried to contact them.

## 5.4. Firms see physical threats as less challenging

### Observation 11. Physical terror threats are considered less concerning than cyber threats

The SWIFT compromise scenario was deemed most challenging for the majority of participating firm's CMTs. In comparison, the firms saw physical threats as least challenging. A couple of reasons could explain this.

First, in a physical threat scenario, corporate management expects directions from the public authorities and building management. Even without a corporate security team, corporate services will generally have a direct connection with building management in regard to evacuation or shelter-in-place decisions. Building management recommendations are provided via police advice, so internal CMTs see physical threat response decisions as being guided by professionals and act accordingly in regards to staff safety. Irrespective of size, most firms have a corporate security department that plays an active role in the support of crisis response. Corporate security generally has experience and connections with emergency services (police, fire) and are able to provide professional advice to guide CMT decisions. In this context, it was observed that direct communication between police/first responders and firms is limited, typically routed – and potentially delayed – through building management organisations.

Firms are expected to at least have protocols and policies in place for emergency notification or communication with all staff, allowing them to account for safety and whereabouts of everyone.

Second, there is an element of public trends in threat perception. Especially when it relates to events, public memory is short and selective. Although the actual threat of, for example, a pandemic or natural disaster does not change, the perception, and consequent management attention, on these topics changes significantly over time. Generally, if a high-visibility event happened, the topic rises on the threat agenda, whereas several years without event occurrence easily leads to complacency. There have been no high-visibility terror attacks in Hong Kong in recent years.

## 5.5. Benchmarking

One of the key pieces of feedback received from WISE2015 was that participating organisations wanted individual benchmarking, where they could assess their effectiveness against the industry and best practice. We also received feedback from local regulators that they wanted to gain a better grasp of the spread of the industry's effectiveness as compared to industry best practice.

In response to this, WISE2017 will provide individual feedback to participating organisations and the industry as a whole. The detailed report will cover the following topics:

- **Crisis management skills**
  The internal organisation of the CMT and the CMT facilities for the exercise.

- **Communication**
  The communication practices of the organisations from a high-level understanding of formal procedures to activities taken during the exercise, including the submission of public statements/ social media posts and response times. This covers internal and external communications from an information vetting perspective to information dissemination.

- **Information management**
  Information can be an advantage and disadvantage in a crisis. The process of understanding, communicating, discussing and recording information is key to ensuring a CMT effectively manages itself and the situation.

- **Decision making**
  An effective CMT allows effective management of an incident. This topic will look at the effectiveness of CMT members' involvement in the discussion and decision-making process. It also helps show the integration of the cyber element into response plans, as well as staff welfare and the recording, review and execution of decisions and tasks.

While this report gives participating organisations the ability to gauge themselves against the industry and best practices, and provides recommendations, each organisation should take this feedback and determine for itself what changes or improvements it might have to implement to its processes to help improve its crisis response. One solution does not fit all and each organisation is unique; as such, it might have an effective crisis management and response team and process even if it does not fully align with industry best practices.

# 6. Considerations for WISE2019

The majority of participants were neutral in the post-exercise survey, as to whether they needed more crisis management training. This means WISE2017 was effective and we should continue with a biennial industry-wide exercise. Nonetheless, it is recommended organisations conduct internal training and drills, on a regular basis, to strengthen crisis resilience and emergency response.

For WISE2019, the following consideration should be made.

### Improve planning and preparation

The overall exercise would benefit from timelier planning. For example, earlier release of draft documents and surveys will allow for more review, and an earlier start to testing of technical facilities will support corrections and review rounds, boosting overall quality of deliverables. Finally, the availability of rooms and people can be an issue with late scheduling.

Some participants experienced a delay in receiving injects and the performance of the exercise portal became slow at certain stages during WISE2017. Consequently, future exercises should include more stress testing of the exercise portal to increase performance.

As many facilitators were overwhelmed by information from the exercise portal, phone calls from the command centre and requests from their CMT, it would be advisable in future exercises to designate more than one individual to facilitate the exercise in each organisation.

Structural setup of the CMT can also be a challenge, so future exercises should delve more into the exact make up, roles and responsibilities of CMT members to facilitate better response and triaging of responsibilities.

### Increase staff numbers required to handle the interactive element of the exercise

One observation is, for future exercises, a larger red team is needed to challenge less engaged participants. This year, members of the red team were stretched in terms of the number of calls they placed.

Volunteers who were involved in the WISE2017 command centre provided post-exercise feedback. One observation was that there was insufficient manpower in the command centre to manage incoming enquiries, particularly for those roleplaying the regulatory authorities and Hong Kong Police Force.

Future exercises should carefully compare the number of participating organisations with the number of available volunteers in the command centre to avoid a shortage in manpower. As a fairly limited number of organisations provided volunteers to join the command centre, WISE2019 should increase awareness and promote volunteer participation at a much earlier phase in the project development, indicating or even requiring a minimum number of volunteers from each participating organisation. As part of this initiative, organisers can summarise the benefits of volunteering. Those who volunteered in WISE2017 emphasised it was a valuable and engaging learning experience.

### Have more bespoke scenarios

From the feedback, it was found specialist companies, such as asset managers, could use a more challenging scenario with more injects, as many injects were not applicable to them. For example, several companies are not subject to regulations of the HKMA; therefore, the requirement to provide status reports and updates does not apply.

By creating more bespoke scenario injects, where not every company is challenged with the same scenario, details can make the experience better and more immersive. For example, a specific scenario line for insurance companies might add value, but would not be useful for a broker or custody firm.

Also, more bespoke scenario injects will accommodate the maturity level of the different CMTs, as well as their corporate culture in decision making. Future exercises might target organisations in batches, categorised by their size and level of experience.

### Collaborate with other jurisdictions in the region.

In future, collaboration with other geographical markets could transform WISE into an Asia Pacific-wide exercise to simulate systemic and geopolitical risk at a regional level. The root cause of a crisis, such as cyber issues, extreme weather or terror events, know no borders, and can hit several markets simultaneously. What Asia has in common is that it is the first region to open on a business day.

Many companies work with regional management, including regional crisis management and business continuity teams. Providing an exercise that challenges regional coordination and local cooperation into a coordinated regional crisis response could be a welcome and necessary contribution to industry resilience.

Obvious partners for collaboration would be the financial centres of Singapore, Sydney and Tokyo, but smaller markets could be in-scope as well.

### Organise an industry-wide training programme based on best practice regarding crisis management facilitation

In addition to the services provided by management consultants, as well as the certification training provided by the BCI partners and the DRII, HKFSBCM could consider organising formal management training around crisis management. Target group and set-up can vary, from classroom training for junior business continuity management staff on the basics of supporting crisis management, to senior management coaching of the CMT chairs by senior consultants.

## Appendix A – Credits List

WISE2017 would not have been possible or a success without the generous help and contributions of an army of determined professional volunteers, assisted by numerous professionals.

### WISE2017 Oversight Committee

| HKFSBCM (full Board) | | |
|---|---|---|
| Hozefa Badri, UBS | Mark Caparros, State Street | Willem Hoekstra, Nomura (Lead) |
| Jason Bailey, HSBC | Leigh Farina, HSBC | Catherine Lo, BAML |
| **Control Risks** | | |
| John Macpherson | Ben Wootliff | Will Brown |
| Neal Beatty | Stewart Petty | Gordon Wong |

### WISE2017 Scenario Development Committee

| HKFSBCM | | |
|---|---|---|
| Rolly Aldovino, Bloomberg | Kiran Denniz, Nomura | Sherine Lim, BNP Paribas |
| Hozefa Badri, UBS | Martin Eber, HSBC | Catherine Lo, BAML |
| Jason Bailey, HSBC | Leigh Farina, HSBC (Lead) | Brad Mitchell, HKEX |
| Mark Caparros, State Street | Dexter Ho, DBS | Elizabeth Tam, HSBC |
| Chris Choi, HKEX | Willem Hoekstra, Nomura | Simon To, State Street |
| Satyam Das, BlackRock | Karen Lee, Macquarie | |
| **Control Risks** | | |
| Julian Heath | Will Brown | Ben Wootliff |
| Neal Beatty | Stewart Petty | Gordon Wong |
| Jim Fitzsimmons | Mikk Raud | Tony Booth, BCDR Consultants |
| **Ruder Finn (production)** | | |
| Plato Chow | David Ko | Terry Tong |
| Charles Lankester | Derrick Liang | Joshua Wang |

With special thanks for their advisory

| Name | Organisation |
|---|---|
| Joyce Cheung | Hong Kong Monetary Authority (HKMA) |
| Teresa YT Chu | Hong Kong Monetary Authority (HKMA) |
| Rogers Chan | Securities and Futures Commission (SFC) |
| Bénédicte Nolens | Securities and Futures Commission (SFC) |
| Thomas TH Wong | Securities and Futures Commission (SFC) |
| Roger Law | Hong Kong Police Force, CISCC |

| Name | Organisation |
|---|---|
| Roger Wong | Hong Kong Police Force, CISCC |
| Rachel Hui | Hong Kong Police Force, CSTCB |
| Joseph Luk | Hong Kong Police Force, CSTCB |
| Dicky Wong | Hong Kong Police Force, CSTCB |
| Brad Mitchell | HKEx |
| Rolly Aldovino | Bloomberg |

### WISE2017 Planning, Logistics and Facilitation Committee

| HKFSBCM | | |
|---|---|---|
| Hozefa Badri, UBS (Lead) | Willem Hoekstra, Nomura | Jean-Nicolas Phan, Credit Suisse |
| Mark Caparros, State Street | Karen Lee, Macquarie | Ritesh Singh, Standard Chartered Bank |
| Andrew Chan, HSBC | Rebecca Lentchner, BNY Mellon | Simon To, State Street |
| Sonya Chung, HSBC | Raymond Ng, Standard Chartered Bank | |
| **Control Risks** | | |
| Will Brown | Sara Calvert | Ben Wootliff |

### WISE2017 Central Command Centre

| Name | Organisation | Command centre role |
|---|---|---|
| Leigh Farina | HSBC, HKFSBCM Board | Exercise manager |
| Willem Hoekstra | Nomura, HKFSBCM Board | Volunteer |
| Neal Beatty | Control Risks | Role player |
| Will Brown | Control Risks | Exercise manager |
| Sara Calvert | Control Risks | Role player |
| Nadav Davidai | Control Risks | Role player |
| Jim Fitzsimmons | Control Risks | Role player |
| Julian Heath | Control Risks | Exercise manager |
| Jessie Huang | Control Risks | Role player |
| Alanna Miles | Control Risks | Role player |
| Stewart Petty | Control Risks | Role player |
| Maxine Riley | Control Risks | Role player |
| Gordon Wong | Control Risks | Role player |
| Ben Wootliff | Control Risks | Role player |
| Joe Ng | International SOS | Role player |

| Name | Organisation | Command centre role |
|---|---|---|
| Tony Booth | BCDR Consultants | Role player |
| Plato Chow | Ruder Finn | Portal support and inject delivery |
| David Ko | Ruder Finn | Portal support and inject delivery |
| Derrick Liang | Ruder Finn | Portal support and inject delivery |
| Terry Tong | Ruder Finn | Portal support and inject delivery |
| Joshua Wang | Ruder Finn | Portal support and inject delivery |
| Mark Hayman | AIA | Volunteer |
| Ivy Lau | HSBC | Volunteer |
| Claire Turner | HSBC | Volunteer |
| Carly Wong | HSBC | Volunteer |
| Chris Choi | HKEx | Volunteer |
| Brad Mitchell | HKEx | Volunteer |
| Rolly Aldovino | Bloomberg | Volunteer |
| Tyn van Amelsfoort | Panalpina | Volunteer |
| Theo Chung | BAML | Volunteer |
| Alex Dam | BAML | Volunteer |
| Stanley Ho | BAML | Volunteer |
| Alan Leung | BAML | Volunteer |
| David Sunter | BAML | Volunteer |
| Kittee Yeung | BAML | Volunteer |
| Simon To | State Street | Volunteer |
| Don Weinland | Financial Times | Volunteer |
| Bénédicte Nolens | SFC | Observer |
| Thomas TH Wong | SFC | Observer |
| Joyce Cheung | HKMA | Observer |
| Teresa YT Chu | HKMA | Observer |
| Jacky HY Lau | HKMA | Observer |
| Dicky Wong | HKP-CSTCB | Observer |
| LUK Chun-chung, Joseph | HKP-CSTCB | Observer |
| Roger Law | HKP-CISCC | Observer |
| Roger Wong | HKP-CISCC | Observer |
| Yee De Biao | Monetary Authority of Singapore | Observer |
| Evangelos Tabakis | Central Bank UAE | Observer |
| Bjorn Lenzmann | Emirates NBD | Observer |
| Katrina Hackett | Dubai Financial Services Authority | Observer |

## Others who have contributed/special thanks

- Regus
- ASIFMA
- HK Association of Banks
- Financial Services and the Treasury Bureau
- HK Insurance Authority
- HK Federation of Insurers
- Nic Reys (Control Risks)

HKFSBCM would like to thank the HKMA, SFC, ASIFMA and HKAB for their invaluable support in driving awareness of WISE2017 by hosting information sessions and/or sharing information on the exercise with their membership.

The central command centre team

## Appendix B – Data collected after the exercise

Immediately after the exercise, every CMT was asked to submit a questionnaire. Several facilitators used this survey to query CMT members on their experience and consolidated this for an overall response. The scores are self-explanatory (the score is from 1-5, where 5 is most positive). The variance is a measure of the dispersion of data around the mean, showing consistency of responses. A variance of 0 means all 45 companies provided the same answer, whereas a high number reflects a large difference.

| | Min/No | Avg | Max/Yes | Var |
|---|---|---|---|---|
| **COMMUNICATION** | | | | |
| 1.1 Do you have formal procedures and processes for communicating with customers? e.g.:<br>- communication channels, procedures and decision making processes are in place | 2 | **4.2** | 5 | 0.46 |
| 1.2 Key external audiences, messages and preferred communication channels have been identified, e.g.:<br>- Regulators, vendors, media, law enforcement etc.<br>- Social media, press release, etc. | 3 | **4.3** | 5 | 0.42 |
| 1.3 Do you have effective media engagement protocols?<br>- Approved media spokespersons identified and known to CMT members<br>- Approved media spokespersons have the right skills for media interaction | 2 | **4.3** | 5 | 0.46 |
| 1.4 Effective internal communications channels and protocols for disseminating information to staff have been identified, e.g.:<br>- Intranet, text message, call cascade, etc.<br>- Manual or automated call trees | 3 | **4.4** | 5 | 0.38 |
| 1.5 During the exercise, did you initiate communications (i.e. make the decision to communicate, or release communications) with: | | | | |
| - Staff | 1 | **4.8** | 5 | 0.72 |
| - Press (press statement through exercise portal corporate site) | 1 | **4.6** | 5 | 1.35 |
| - Customers | 1 | **4.6** | 5 | 1.35 |
| - Social media platforms (through exercise portal corporate site) | 1 | **3.3** | 5 | 3.93 |
| - Regulators | 1 | **4.9** | 5 | 0.36 |
| - Counterparties | 1 | **4.3** | 5 | 2.31 |
| - The RE.BEL | 1 | **1.2** | 5 | 0.71 |
| - Other external stakeholders (vendors, clearing house, police, etc.) | 1 | **4.8** | 5 | 0.74 |

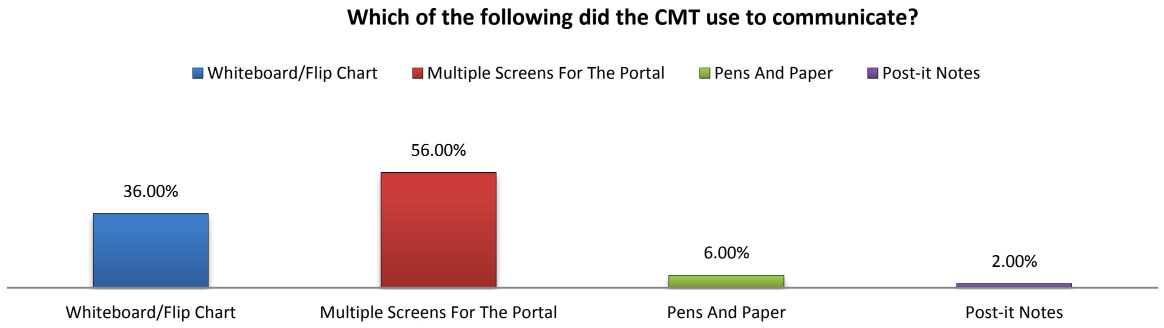
| | Min/No | Avg | Max/Yes | Var |
|---|---|---|---|---|
| **INFORMATION MANAGEMENT** | | | | |
| 2.1 The CMT can effectively assess and respond to the situation, e.g.:<br>- you are confident in a real incident there are protocols in place to provide you with business impacts, management information/performance statistics<br>- there are sufficient tools available to support effective decision making | 3 | **4.1** | 5 | 0.41 |
| 2.2 A record was made of all incoming and outgoing information, along with internal discussions, e.g.:<br>- actions / information log (manual or automated)<br>- meeting minutes | 2 | **4.1** | 5 | 0.72 |
| 2.3 All CMT members shared information effectively, e.g. members were forthcoming with sharing information and providing relevant knowledge for their business area updates. | 3 | **4.4** | 5 | 0.43 |
| 2.4 The CMT regularly set aside time throughout the course of the incident/meetings to summarise and review current information/actions, etc. | 2 | **3.9** | 5 | 0.61 |
| 2.5 The CMT set aside specific team members to assess the incoming information on the exercise portal/inject materials. | 2 | **4.0** | 5 | 0.72 |
| 2.6 A roll call of the CMT was conducted at the start of the exercise to ensure all business areas were represented. | 1 | **4.4** | 5 | 0.85 |
| **DECISION MAKING** | | | | |
| 3.1 All members of the CMT understood their roles and responsibilities. | 2 | **4.4** | 5 | 0.61 |
| 3.2 Is cyber incident response integrated into your CMT and protocol? | 1 | **4.2** | 5 | 0.82 |
| 3.3 The CMT's approach to decision making is effective, i.e. decisions were made and communicated clearly? | 3 | **4.2** | 5 | 0.56 |
| 3.4 CMT decisions were translated into actions and tasks, recorded, tracked and followed up by the chair throughout the exercise. | 2 | **4.0** | 5 | 0.51 |
| 3.5 The CMT membership is appropriate – the correct people around the table or available to support effective decision making | 2 | **4.1** | 5 | 0.62 |
| 3.6 Does/did your organisation; | | | | |
| - Have a policy on paying ransoms in relation to cyber extortion? | 1 | **2.5** | 5 | 3.88 |
| - Choose to pay the ransom in this exercise scenario? | 1 | **1.0** | 1 | 0.00 |

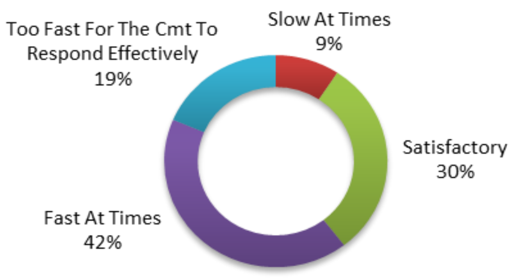
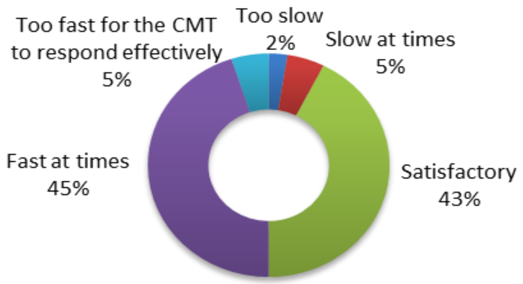
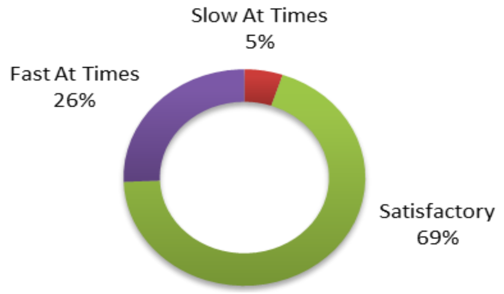
| | Min/No | Avg | Max/Yes | Var |
|---|---|---|---|---|
| **THE EXERCISE** | | | | |
| 4.1 The exercise helped develop my personal confidence as a CMT member | 3 | **4.3** | 5 | 0.40 |
| 4.2 The exercise identified I need more training in my role and responsibilities | 1 | **3.1** | 5 | 1.13 |
| 4.3 The exercise was well organised (internally) | 3 | **4.4** | 5 | 0.38 |
| 4.4 The information I was provided before and during the exercise was sufficient | 1 | **4.0** | 5 | 0.77 |
| 4.5 The hot debrief/feedback session was useful. (Did it capture areas of strength? Did we capture issues? Did you feel it was a good assessment of the exercise?) | 3 | **4.0** | 5 | 0.42 |
| 4.6 Which scenario did you find most challenging during the exercise? (rate the most challenging as '5' and the least challenging '1' – use each rating only once). | | | | |
| - OMS compromise | 1 | **3.4** | 5 | 1.13 |
| - Physical security incidents | 1 | **3.0** | 5 | 1.81 |
| - Ransomware | 1 | **2.8** | 5 | 1.20 |
| - SWIFT compromise | 1 | **4.0** | 5 | 0.95 |
| - Sanctions list compromise | 1 | **2.3** | 5 | 1.43 |

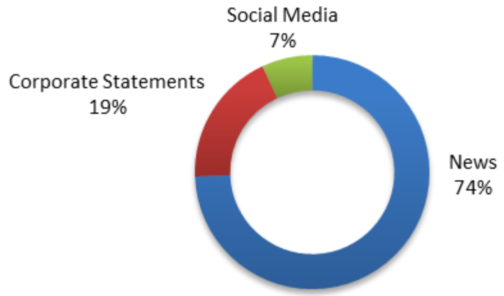
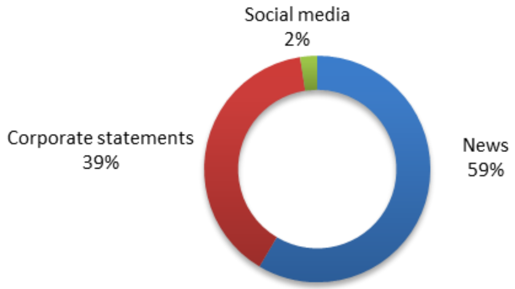
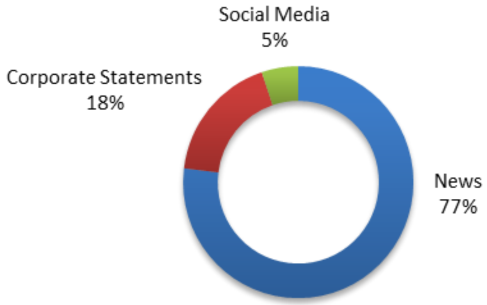
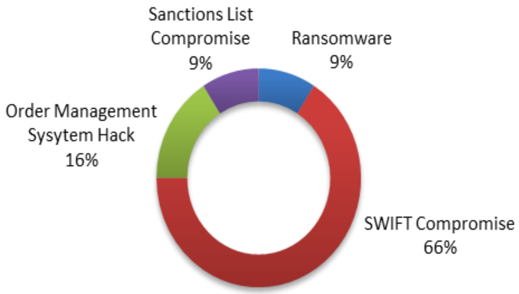
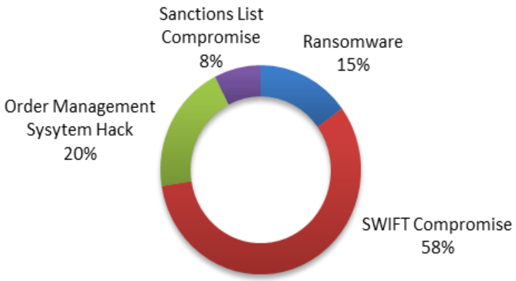
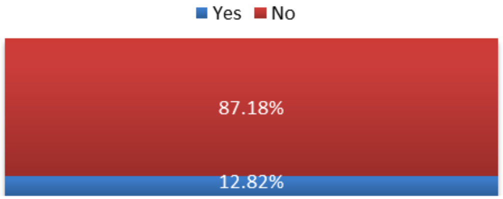
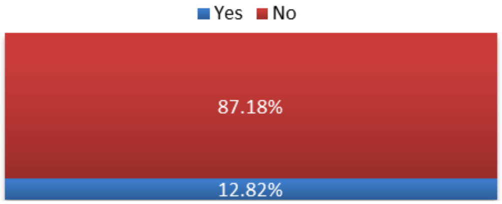
# Appendix C – Data collected during the exercise

## Commencement of the exercise

- 100% of participating organisations' technology was tested and working as expected at the commencement of the exercise at 13:30
- 98% of the organisations were well-prepared with their designated CMT members present and ready for the commencement of the exercise at 13:30
- 100% of the organisations successfully logged into the WISE2017 exercise portal for the commencement of the exercise at 13:30
- 56% of the organisations were well-prepared with multiple screens to enable their CMT to easily view the WISE2017 portal
- 36% of the organisations had a flip chart or whiteboard available for deliberations



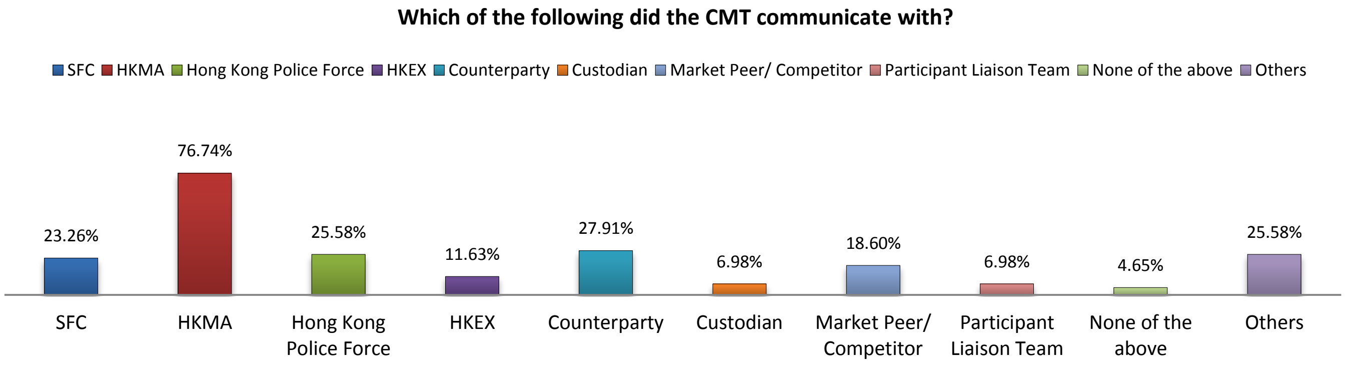
| Area | 45 minutes into the exercise | 90 minutes into the exercise | 135 minutes into the exercise |
|---|---|---|---|
| Tempo |  |  |  |
| | • Satisfaction at the tempo of the exercise increased as the exercise progressed, but a significant portion still found it too fast at times. | | |

| Area | 45 minutes into the exercise | 90 minutes into the exercise | 135 minutes into the exercise |
|---|---|---|---|
| Ransom payment | | 100% of the organisations refused to pay the ransom. The most common reason for this decision was uncertainty over the outcome of making a payment. The second most popular reason for refusing payment was the reputational risks associated with such a decision | |
| Monitoring |  |  |  |
| Most challenging scenario |  |  | |
| Use of new tools | |  |  |

| Area | 45 minutes into the exercise | 90 minutes into the exercise | 135 minutes into the exercise |
|---|---|---|---|
| | • 90 minutes – The 13% that introduced new tools relied on WhatsApp communications, internal communications and video conferencing<br>• 135 minutes – The 13% that introduced new tools relied on staff mapping tools, Criticall, an in-house "Global Security Centre" and Travel Tracker | | |

<table>
<tr><th>Area</th><th>Communications with regulatory authorities</th></tr>
<tr><td><b>45 minutes into the exercise</b></td><td>

- 77% of the CMTs communicated with the regulatory authorities. In addition to those recipients listed below, some CMTs contacted their customers and vendors

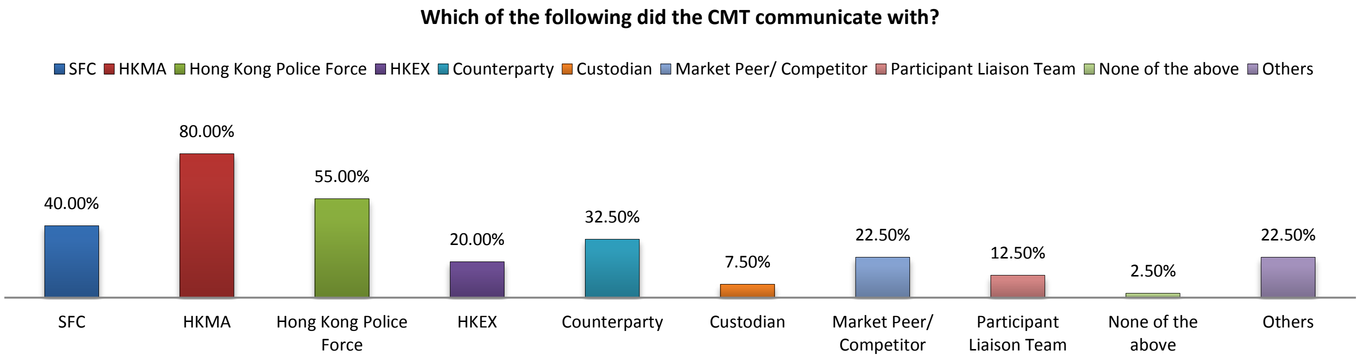


Which of the following did the CMT communicate with?

</td></tr>
<tr><td><b>90 minutes into the exercise</b></td><td>

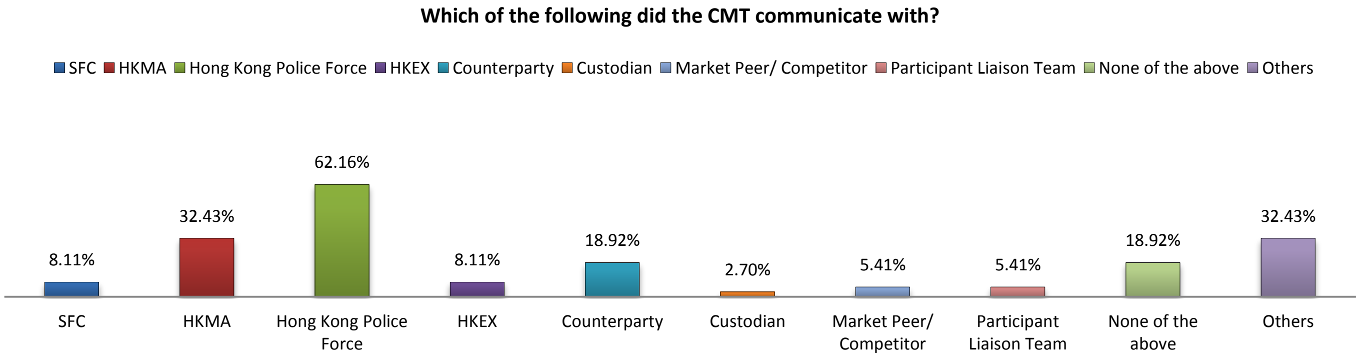
- 80% of the CMTs communicated with the regulatory authorities, an increase of 10% of participants compared with the first 45 minutes of the exercise. At this point in the exercise, 55% of the CMTs contacted the Hong Kong Police Force, compared with 26% of the CMTs in the first 45 minutes of the exercise

</td></tr>
</table>

<table>
<tr><th>Area</th><th>Communications with regulatory authorities</th></tr>
<tr><td></td><td>


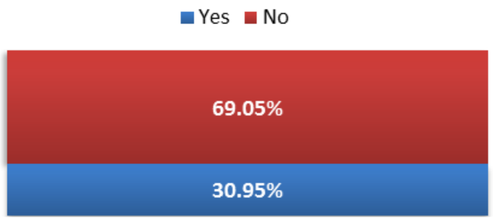
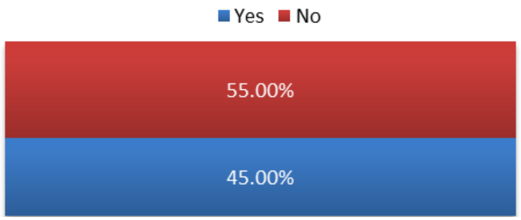
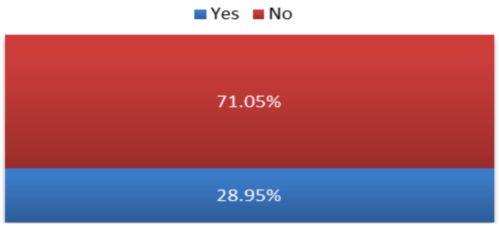
</td></tr>
<tr><td>135 minutes into the exercise</td><td>

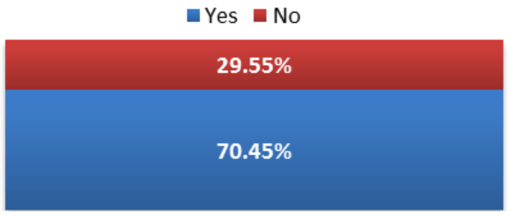
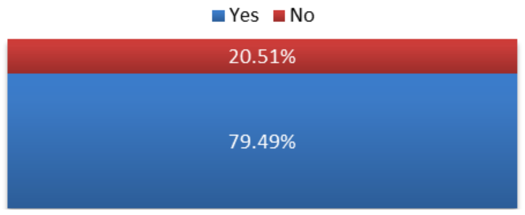
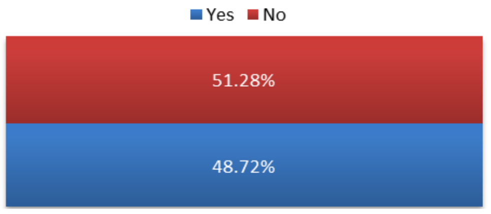
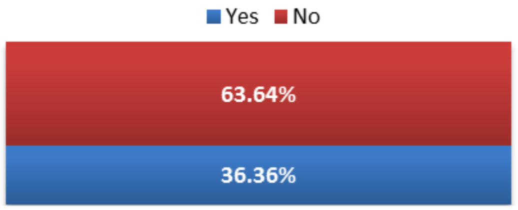
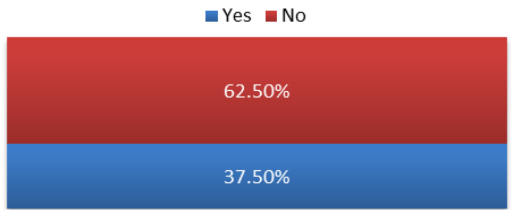
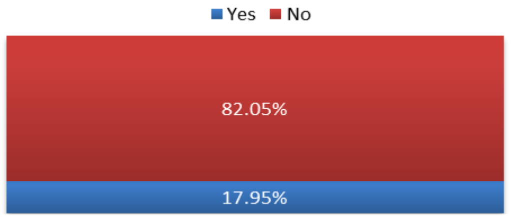
- 62% of the CMTs communicated with the Hong Kong Police Force
- 32% of the CMTs contacted staff (local and those travelling to Hong Kong), hospitals, building management, clients, the FinTech conference and NetCraft (internet security service providers), and the liquidity support team

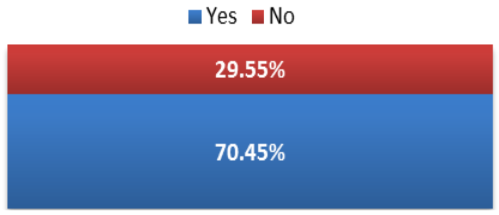
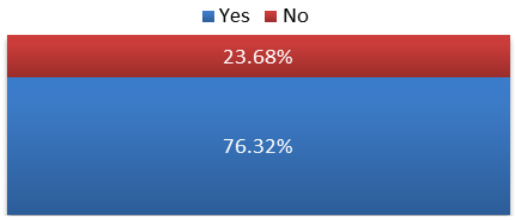
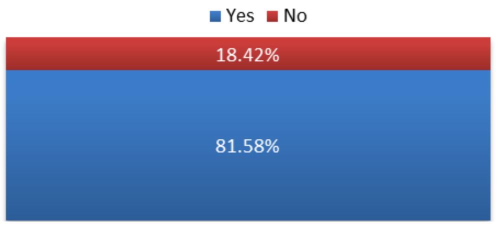


</td></tr>
</table>

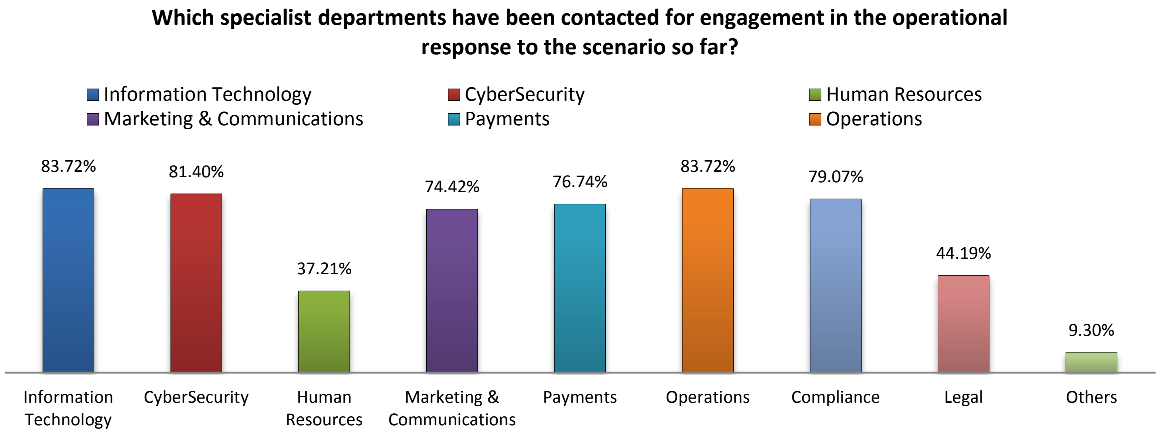
| Area | 45 minutes into the exercise | 90 minutes into the exercise | 135 minutes into the exercise |
|---|---|---|---|
| Reasons for third party contact | • Discuss the SWIFT compromise incident<br>• Seek assistance in understanding the current status | • Confirm the status of operations and recovery efforts<br>• Discuss bitcoin ransomware demand with | • Report to HKMA and Hong Kong Police Force that Wan Chai branch operations were suspended |

| Area | 45 minutes into the exercise | 90 minutes into the exercise | 135 minutes into the exercise |
|---|---|---|---|
| | • Discuss the ransomware incident<br>• Provide updates to the regulatory authorities | the Hong Kong Police Force<br>• Inform HKMA and SFC of the latest situation with regard to the SWIFT compromise incident<br>• Verify the physical status of counterparties<br>• Request confirmation from the regulatory authorities on the situation<br>• Confirm status of the internal banking system<br>• Confirm market positions<br>• Confirm there is no abnormality of service<br>• Confirm receipt of operational incident response form submission with HKMA<br>• Address customer enquiries<br>• Trigger the business continuity plan | • Contact staff to ensure their safety and provide advice through internal call trees<br>• Communicate instructions to staff to relocate to alternative sites<br>• Update the regulatory authorities on status<br>• Seek advice from the Hong Kong Police Force on the incident status and evacuation<br>• Check trading capabilities<br>• Report the closure of branches (e.g. Great Eagle Centre)<br>• Issue communications to the public<br>• Confirm the safety of the two senior executives through a call-back procedure<br>• Discuss the latest developments with HKEX and other banks/institutions<br>• Confirm the HKMA received submission of operational incident reporting form<br>• Shut down the online system<br>• Report ransomware incident to Hong Kong Police Force<br>• Contact NetCraft to implement anti-phishing services |
| Exercise directory use |  |  |  |

| Area | 45 minutes into the exercise | 90 minutes into the exercise | 135 minutes into the exercise |
|---|---|---|---|
| Discussion of impact to their sector and/or supply chain |  |  |  |
| Command centre contact |  |  |  |
| Information supplied to key stakeholders | • Instruct them to extend operating hours<br>• Confirm trade position<br>• Update on current status and ongoing monitoring<br>• Issue a holding statement/press release after collecting facts from key stakeholders<br>• Inform customers of ongoing investigations and set up a hotline for queries<br>• Report ransomware attack to senior management<br>• Instruct stakeholders to verify payment instructions<br>• Assess the integrity of news articles recently published related to the incidents<br>• Issue a security alert to all potentially affected parties<br>• Request information from third-party | • Address client concerns<br>• Provide external web portal access to customers (backup)<br>• Provide situation update, monitoring and confirmation of trade<br>• Provide set scripts to the customer services department to pre-empt questions from customers<br>• Provide instructions to head of payments/customer services<br>• Share information from corporate clients<br>• Provide updates to the regulatory authorities<br>• Inform global crisis committees of the latest status<br>• Prepare client communication<br>• Clarify arrangements for the clearing houses | • Provide feedback from customers to management<br>• Deliver status update on incident to all staff; in some cases a message to lockdown premises and invacuate, in other cases a message to evacuate<br>• Activate the business continuity plan for alternative site<br>• Issue advisory to avoid the Wan Chai area<br>• Provide update to customers – accounts are safe, but certain services are restricted<br>• Issue press release to public and customers<br>• Confirm the bank's current position<br>• Advise customers to use hotline for trading rather than online banking portal |

| Area | 45 minutes into the exercise | 90 minutes into the exercise | 135 minutes into the exercise |
|---|---|---|---|
| | vendors<br>• Instruct technical department to assess impact to own institution. | • Communicate with internal stakeholders, staff, distributors and counterparties<br>• Suspend payments and dealing<br>• Bolster client confidence that their accounts are safe<br>• Issue a press release<br>• Manage customer enquiries<br>• Update operational status from “business as usual” to “extended operating hours” | |
| Sought additional expertise/ sub-teams |  |  |  |

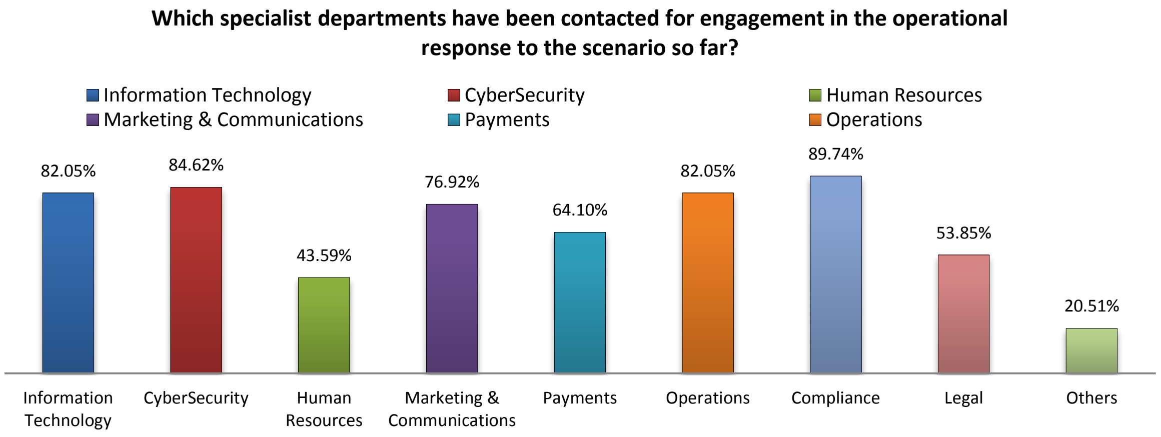
| Area | Communications with specialist departments |
|---|---|
| 45 minutes into the exercise | • The CMTs contacted several specialist departments as part of engagement in the operational response to the scenario. The two departments that received the highest frequency of contact were Information Technology (84%) and Operations (84%) |

<table>
<tr><th>Area</th><th>Communications with specialist departments</th></tr>
<tr><td></td><td>


Which specialist departments have been contacted for engagement in the operational response to the scenario so far?

</td></tr>
<tr><td>90 minutes into the exercise</td><td>

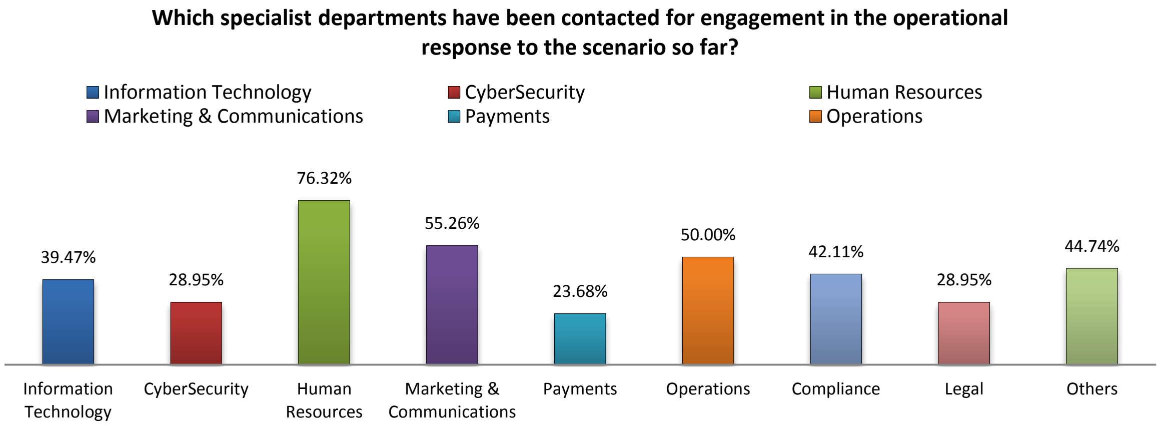
- The CMTs contacted several specialist departments as part of engagement in the operational response to the scenario. The two departments that received the highest frequency of contact were Compliance (90%) and Cybersecurity (85%)

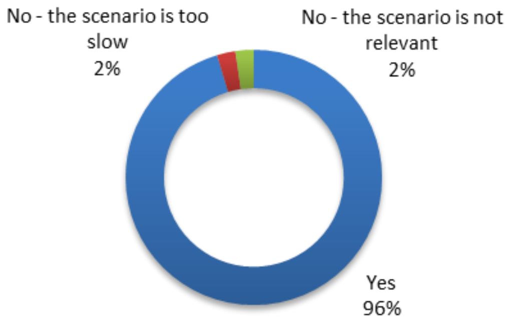


Which specialist departments have been contacted for engagement in the operational response to the scenario so far?

</td></tr>
<tr><td>135 minutes into the exercise</td><td>

- The CMTs contacted several specialist departments as part of engagement in the operational response to the scenario. The two departments that received the highest frequency of contact were Human Resources (76%) and
</td></tr>
</table>

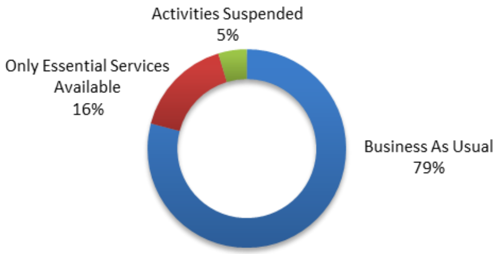
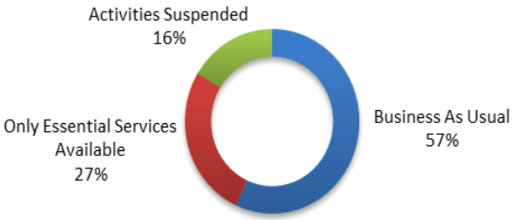
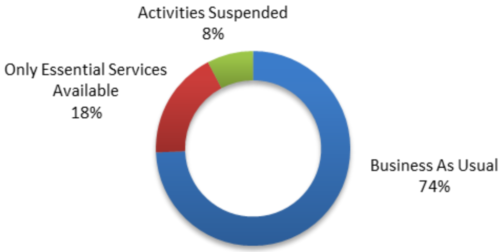
| Area | Communications with specialist departments |
|---|---|
| | Marketing & Communications (55%)<br> |

| Area | 45 minutes into the exercise | 90 minutes into the exercise | 135 minutes into the exercise |
|---|---|---|---|
| CMT engagement |  | 100% of the CMTs felt engaged and were actively discussing the scenario | 100% of the CMTs felt engaged and were actively discussing the scenario |
| Key decisions and actions | • Conduct business impact analysis<br>• Trigger the business continuity plan<br>• Suspend the OMS<br>• Unplug all personal computers | • Unplug all affected personal computers<br>• Cease all payments<br>• Notify counterparties the institution will start end-of-day processes earlier to expedite reconciliation | • Suspend affected branches and announce to the public<br>• Liaise with building management<br>• Decide how to formulate a message to all staff |

No - the scenario is too slow
2%
No - the scenario is not relevant
2%
Yes
96%

| Area | 45 minutes into the exercise | 90 minutes into the exercise | 135 minutes into the exercise |
|---|---|---|---|
| | • Gather information on the incident to ensure continuity<br>• Decide not to release statement to the media, but in the interim, contacted clients directly to explain the situation and contacted the payments team to gather information<br>• Decide not to meet RE.BEL's demand and pay the ransom<br>• Manually conduct sanctions screening<br>• Decrease online banking thresholds for third parties only<br>• Extend ATM service hours<br>• Enhance physical security measures for the trading floor<br>• Collaborate with other participating organisations<br>• Revert trade transactions to manual execution<br>• Isolate the Hong Kong banking network<br>• Engage relevant technical teams<br>• Convene crisis management bridge to prepare internal and external communications<br>• Make no specific comments to the press<br>• Put traders on notice<br>• Report to the regulatory authorities<br>• Prepare script for the customer service team and statements for public websites<br>• Cease payments<br>• Actively monitor banking system's | • Fix the system after the ransomware attack<br>• 'Hot to process payments' (?)<br>• Send staff home for safety reasons<br>• Follow instructions from the HKMA<br>• Tie up all outstanding trades<br>• Decide whether to pay the ransom and report to the Hong Kong Police Force<br>• Shut down the OMS<br>• Continue investigations on the current status of the incidents<br>• Handle all payments manually<br>• Freeze all payment systems<br>• Suspend any new account openings<br>• Update event management team<br>• Respond to all client enquiries<br>• Invoke a plan to transfer work to other financial hubs within organisation's network<br>• Conduct health check of all banking systems including ATM, card system and bank trade systems<br>• Shut down the trading systems<br>• Monitor the status of the institution and market positions<br>• Close branches<br>• Activate the business continuity plan<br>• Activate IT security recovery plan<br>• Devise plan to confront liquidity issues following cessation of payments | • Decide to invacuate<br>• Decide how to confirm staff safety<br>• Inform global business continuity management team and activate the business continuity plan<br>• Decide whether to limit the availability of certain services<br>• Confirm availability of alternative sites<br>• Decide how to confirm a list of staff that attended the FinTech conference to ensure their safety<br>• Decide whether to close branches<br>• Send members of the security department to Wan Chai<br>• Decide to continue with "business as usual"<br>• Decide to lock down part of building and discontinue shuttle services<br>• Write succession plan for management<br>• Decide what information to provide as an update to the regulatory authorities<br>• Obtain additional HKD and CNY in cash for liquidity reserves<br>• Conduct health check on all banking systems (hardware and software) for ATM network, e-banking, card system and bank trade system<br>• Decide to shut down OMS<br>• Extend hours of service to 8:00pm<br>• After sanctions lists were confirmed to be corrupted, cease using SafeWatch screening and switch to an alternative |

| Area | 45 minutes into the exercise | 90 minutes into the exercise | 135 minutes into the exercise |
|---|---|---|---|
| | infrastructure | • Contact vendors to verify the integrity of sanctions lists<br>• Back check all received and processed orders<br>• Extend business service hours | source of sanctions list<br>• Decide not to pay the ransom |
| Biggest concerns | • The cessation of payments<br>• Protection of customer data<br>• Erroneous trades<br>• Occasional irrelevance of the scenario to certain CMTs<br>• How to communicate with internal and external stakeholders<br>• Hack of internal systems<br>• Balance between managing the impact on customers and providing a timely response to the regulatory authorities<br>• Loss of bank data; fears over its recovery<br>• Maintaining customer account security<br>• Extent of the impact generated by the scenario<br>• How to clarify internal business impact<br>• Extended suspension of SWIFT payment processing<br>• Regulatory requirements<br>• Managing a high volume of customer enquiries<br>• Reputational risk to the company<br>• Managing public concerns<br>• Assessing the accuracy of existing sanction lists | • Trade execution and positions<br>• Consequences of restricting SWIFT payments<br>• Hack into trading systems<br>• CCASS transactions being impacted<br>• Hostage situation<br>• Suspension of the OMS<br>• Fear that compromise of the OMS will reach global level<br>• Confirm the validity of information received through the news site; too much information<br>• Consider whether to stop trading<br>• Trigger the business continuity plan<br>• Questions over the safety of the banking system and potential customer impacts<br>• Provide update to regulatory authorities within the given time frame<br>• Protect customer assets<br>• Physical attack on trading floor<br>• Sanction list compromise may affect compliance with AML guidelines<br>• Time pressure to make conscious decisions<br>• Recovery of data and operations | • Staff and customer safety<br>• Ensuring backup site is available and ready<br>• Procedure for maintaining contact with staff<br>• Procedure to invacuate/evacuate staff<br>• Panic owing to news reports of injuries and deaths<br>• How to communicate without a live phone network<br>• Impact on the business<br>• Compromise of the OMS<br>• How to secure an alternative workplace<br>• Time pressure to make wise decisions |

| Area | 45 minutes into the exercise | 90 minutes into the exercise | 135 minutes into the exercise |
|---|---|---|---|
| | • Responding to market volatility<br>• How to formulate a response under time pressure<br>• Safety of customer funds | • System performance after recovery<br>• Handling influx of customer enquiries<br>• Assessing the validity of threats<br>• Fears over internal fraud threats<br>• Questions over how to complete the settlements process | |
| Operational status |  |  |  |

## Appendix D – Feedback post-exercise debrief

All WISE facilitators were invited to join a feedback session on 8 December 2017, presented by Willem Hoekstra and hosted by State Street in Two IFC. Forty people participated in the five discussion sessions, each on a specific topic.

### The exercise: Feedback, lessons learned and ideas for 2019

| Experience/issue/observation | Suggestions/comments |
|---|---|
| Scenarios to cover non-banks, i.e. insurance and brokerage | Some banks have these business groups, but they have not been included in the exercise. Good for the organiser to remember for next time. |
| Insufficient inject language options | Depending on who is taking the call, the control room should allow the participants to choose their inject and command centre response language. |
| Scenario pace is too fast or too complex | The CMT does not have time to perform impact analysis. Slower pace or fewer scenarios will be better.<br>The quality of the response is more important than the number of scenarios covered. |
| The role of HKMA/HKAB can be included in the exercise | As a number of scenarios will involve a decision that affects a number of banks, HKAB/HKMA should throw in the appropriate guidance/response at the right time and save participants from trying to find out what others are doing. They should do so with systemic issues. |
| Late release of facilitator materials | Materials were sent too late for the facilitator to have a good walkthrough as it is rather complicated. Also, given good advance planning, the injects can be released internally via trusted agents in the relevant department. The distribution of emails to a blanket group is not a realistic practice.<br>Counterparties calling and involvement could also be improved with adequate planning. |
| Time lapse of the scenarios | Although real time is good, a time lapse will allow more time to think through and summarise actions. It is moving so fast that taking down actions is difficult.<br>Having more time would allow for exercise scope to include incident response and escalation, and have the organisation process the information. |
| Transparency in the actions taken by other banks | It will be good if there is a channel where participating banks can communicate (not just for the exercise, but for general crisis use). |
| The CMT has interpreted the scenario and made too many | The information revealed or the response by the CMT could include more detailed steps to restrict the possibility for |

| Experience/issue/observation | Suggestions/comments |
|---|---|
| assumptions | making assumptions.<br>It could dictate more about the impact to the company so they do not make assumptions. |
| Social media may not be relevant to some organisations. Some banks do not have a policy on social media response and no dedicated communications team | The organising committee can do a better pre-planning survey to understand social media use for each participating bank and then tweak from there. |
| Fees are reasonable | The price is value for money. An increase to this price will still be a reasonable price to pay for the quality of the exercise. |

## Facilitating: How to prepare facilitators for their role

| Experience/issue/observation | Suggestions/comments |
|---|---|
| **Training and awareness** | |
| • The exercise raised the professional image of the business continuity management function<br>• The exercise raised the professional image of facilitators with executive leadership<br>• The exercise raised the standard of business continuity management exercises through its realism and intensity – this has driven a desire to review crisis management teams, practices and resources required to support a real event<br>• Challenged management complacency (especially new participants)<br>• The exercise was viewed as a success in raising the standard of preparedness across the industry (on an individual organisation and highlighted the need for interbank coordination in major events) | • It was viewed as a stretch test for all organisations (except asset managers, who required greater direct impact to generate the similar level of intensity as banks)<br>• While a good exercise, many participants reported the style of the exercise did not develop the professional skills required in a crisis event<br>• The pace of the exercise was too fast and there were too many issues to deal with (out of the normal structure of crisis management meetings) |
| **Preparation** | |
| • Of the 12 participants in the feedback group, seven provided a broad (without scenario detail) briefing to the CMT, five briefed the chair on the scenario and zero gave no advance briefings | • Much earlier distribution of exercise materials needed (one month)<br>• A full dress rehearsal with facilitators is a requirement for future exercises<br>• Requirement to brief some key personnel (IT, chair) to make the scenario relevant to participants and enable the best possible learning experience<br>• Greater advice should be provided in how to effectively facilitate and what is required of the facilitator (including practice sessions and dry runs) |

| Experience/issue/observation | Suggestions/comments |
|---|---|
| | • The facilitator set up session should have been held much earlier and with greater advice on staffing and organisational requirements<br>• Recommend facilitator support:<br>○ Compliance team (more than one)<br>○ Communications to have a support team (most successful organisations had large communications support teams participating)<br>○ One person to manage phone<br>○ One person to manage emails<br>○ One person to monitor and complete the survey<br>○ One person to manage the portal<br>○ One note taker (possible additional for support)<br>○ Two observers/parking lot, priorities and summarise actions<br>○ One person to record and track actions<br>○ Require more than one screen |
| **The exercise** | |
| • Facilitators were overloaded with too much information and too much to do<br>• Inject delivery was confusing and circumvented the facilitator, making it difficult to manage the flow of the exercise (phone calls, emails direct to CMT members, injects difficult to find – in the portal (across the screens) and with organisations posting<br>• Phone call injects caused issues and made it difficult for facilitators to control the flow and pace of information | • Survey was too much, too long, unclear on usefulness to the command centre and needed to be scrolled back up in WhatsApp group.<br>• Each survey should have been sent individually<br>• Email injects were difficult to manage, with more successful (and experienced organisations) printing hard copies and distributing by hand<br>• Flow of exercise and injects was difficult with two docks to balance; would prefer a single run book with the timing, type, inject summary and prompt questions |
| **General** | |
| • Sanctions list was very positively received – made lot of organisations think beyond obvious scenario<br>• Four hours is a long time – what more was learnt than could have been done in two hours | • Exercise should be shorter<br>• Scenario was overly complicated, feedback to consider exercising fewer issues and challenge for greater detail of responses<br>• Consider a multiday exercise, simulating greater realism and no contact number for HKICL<br>• Consider including HKAB in the exercise development and as a coordinating body |

## CMT best practices: What makes a CMT successful?

| Experience/issue/observation | Suggestions/comments |
|---|---|
| The prominence and role played by the CMT head is pivotal for the effective running of a CMT. The more | Although training is important for all CMT members, particular focus should be paid to CMT chairs, as part of the standard exercise, but potentially also in the provision of |

| Experience/issue/observation | Suggestions/comments |
|---|---|
| effective chair strikes a balance between being open to dissenting opinion or bad news, while being decisive and having the final say when a decision is needed, in often dynamic and uncertain situations | additional training for crisis specific topics, e.g. crisis communications, staff welfare and accountability |
| The composition of a CMT is important in ensuring the right representation from the organisation at the correct level of seniority is present in the room to deal with the incident<br>One member organisation highlighted the difficulty that can be encountered when key functions on a CMT are split geographically, e.g. management is based in Hong Kong, but technology is based in Singapore | There are several steps the CMT can take to ensure its membership and composition is correct and suitable:<br>• The CMT head can remember at the start of a CMT meeting to do a brief roll call to ensure full representation is in the room; if not, the CMT admin function can chase absent members to ensure full representation is achieved<br>• Similarly, as CMT meetings are held, the chair can check with each individual area on the impact to them before deciding next steps<br>• A CMT may need to flex its representation to fit specific incidents, e.g. a power outage will require input and representation from premises, but maybe not IT security, conversely a malware attack may not require premises to be present. As a result, a CMT may consider having a core membership that attend all incidents and auxiliary members who are called in depending on the specifics of the incident |
| Those CMTs that have tested and involved their supporting sub-teams in rehearsals are better placed to interact with these teams in an actual incident. This also applies to escalation to global or regional CMTs | Future rehearsals and testing should focus on links between a CMT and its subordinate sub-teams as well as escalation into higher CMTs (if applicable). This will have the dual effect of making rehearsals more realistic, but also stressing the links between these groups to identify areas of improvement and ensure they work effectively in an actual incident. |
| Those CMTs that have been through real incidents inevitably have a greater level of maturity than those who have only convened during rehearsals and briefings | Obviously, real incidents cannot be planned to order; however, business continuity management teams should consider, as part of their training and briefing of CMTs, whether they can leverage other CMTs or individuals within their organisations who have been through real incidents and what insights they can convey to the CMT on live incident management. |

## Cyber preparedness and systemic elements

| Experience/issue/observation | Suggestions/comments |
|---|---|
| We observed cyber threats in general are real and not just an inconvenience due to their potential impacts and unknown severity of the impacts. The impacts can range from data leakage to systems outages to disruption of business processes | We would suggest that apart from preparing for the various threats to an organisation, the CMT should also be connected to the cyber response actions of the organisations. |
| We agreed cyber threats will not fade over time as technology advances, connectivity increases and online transactions increase; we believe attacks will become more | Due to technology changes over time, there should be a regular review and update of Business Continuity Plan (BCP) responses and corporate policies to these changes |

| Experience/issue/observation | Suggestions/comments |
|---|---|
| sophisticated | |
| The systemic threats suggested for our industry would impact exchanges, widely used third party vendors and mobile devices that access corporate networks, e.g. mobile banking apps | Similar to immediately above, BCP responses need to evolve with the threats. Perhaps information sharing with exchanges and third party vendors. In future, joint BCP simulation exercises could be possible. |
| It was agreed firms should prepare for “when” scenarios as opposed to “if” scenarios to prepare for cyber attacks | There is a range of exercises to prepare for cyber attacks. Some suggested examples are:<br>• Central cyber monitoring<br>• Penetration testing<br>• Awareness training for staff<br>• Scenario training<br>• Email phishing tests<br>• Engage expert consultants<br>• Connect business with technology divisions for collaboration<br>• Engage CMT to provide resources for preventative measures |
| It was agreed we need a separate business response plan for cyber, beyond the traditional plans covering building, people, IT and vendor outages | It was suggested BCP responses be upgraded to include cyber incidents as a cyber attack could impact across the established spectrum of BCP outages. The responses could include:<br>• Incorporate the other suggestions on cyber<br>• Escalation procedures to stakeholders<br>• Reporting mechanisms and metrics<br>• Understanding connections to network e.g. vendors<br>• For global organisations, speed of information exchange<br>• Upgraded policies and procedures |

## The exercise: Feedback, lessons learned and ideas for 2019

| Experience/issue/observation | Suggestions/comments |
|---|---|
| **Facilitation** | |
| Team structure | At minimum two CMT leads (one main and one backup/observer/challenger)<br>At minimum two exercise facilitators (to manage the portal, WISE feedback (surveys), injects, participation, etc.) |
| Logins | Apparently many could log in using the same ID, however, this was not made clear and would have been beneficial to those with large number of participants in multiple locations. (i.e. no need to lock down the number of logins per participant.) |
| Injects | Ideally, all participants should submit their key contacts for direct input/feedback from the WISE team to recreate reality as much as possible, e.g. IT/Compliance/Corp Sec/Corp Properties. Rather than calling the IMT or facilitator. |

| Experience/issue/observation | Suggestions/comments |
|---|---|
| Dry run | Essential next time for the facilitators is to understand the flow of the exercise and expectations. |
| Regional participation | Larger participants would like to see an expansion of the exercise to cover APAC not just HK. |
| **Scenarios** | |
| Scenario not always relevant and more time is required to delve into the scenarios presented (e.g. SWIFT/OMS) | In order to do this, have a "multi-choice" on the scenarios they wish to participate in (to be determined before the exercise begins), i.e. which stream they are choosing, e.g. bank, asset management, insurance, etc. |
| Start the process two weeks beforehand | Release news and information to lead the groups to a full blown scenario, e.g. two weeks, one week, four days, two days and exercise day. This will help the teams determine the scope better and come better prepared to respond appropriately in a real scenario that usually develops over time (e.g. pandemic) |
| Scenario review process | Participants would like to review the scenarios with sufficient time for changes to be implemented to ensure they understand and it makes sense for their organisation (in their preparation) |
| **Technology** | |
| The IE/Chrome issue was very distracting for participants | All portal/technology should be locked down one week prior to the exercise |
| The portal is over complicated | Great data, but difficult to use with limited screens to show all the data necessary<br>Suggest we minimise the portal and have more information on the one screen to make it obvious<br>Suggest having "queues" to determine when we should be switching to look at other sensitive data |
| Downloads | Suggest using a website download rather than CD-ROM/ USB |
| **Other comments** | |
| • It was deemed the fees were reasonable<br>• The facilitators pack was received very late and teams would like it well in advance<br>• Some participants would welcome CMT training from the HKFSBCM forum<br>• Overall favourable comments on the exercise; it was found well worthwhile<br>• Knowledge sharing sessions prior were helpful (cyber) and (CMT), and more would be welcomed | |