Post-exercise report

DFSA cyber crisis management exercise 2023

10 August 2023

Dubai Financial Services Authority
Level 13, West Wing, The Gate, Dubai International Financial Centre, PO Box 75850, Dubai, UAE

Control Risks (Middle East) Limited | PO Box 506669 | DIFC Al Fattan Currency House, Tower 2, Level 26 |
Sheikh Zayed Road Dubai | United Arab Emirates
+971 43723 000 dubai@controlrisks.com

About us

Control Risks is a specialist risk consultancy that helps create secure, compliant and resilient organisations. We believe that taking risks is essential to success, so we provide the insight and intelligence you need to realise opportunities and grow. And we ensure you are prepared to resolve issues and crises. From the boardroom to the remotest location, we have developed an unparalleled ability to bring order to chaos and reassurance to anxiety.

In a changing world, we make the difference.

At Control Risks, our mission is to understand risk, cut through uncertainty and empower our clients to make better decisions. We keep opportunity moving forward and support organisations to benefit the communities and environments they work in. Through insight and experience, we help to mitigate threats, whatever form they take. In times of hope and times of crisis, we stand alongside our clients. When what matters most is on the line, we make the difference.

Table of contents

Prepared by Control Risks
for Dubai Financial Services Authority

Executive summary

The Dubai Financial Services Authority (DFSA) engaged Control Risks to prepare and facilitate an inaugural crisis simulation exercise for its Authorised Firms, aimed at enhancing cyber resilience across the Dubai International Financial Centre (DIFC). Seventeen Authorised Firms took part.

Control Risks and the DFSA chose cyber activism, often referred to as "hacktivism," as the crisis for the exercise, as it could be replicated in a simulation with the realism, context, and complexity of real attacks. To bolster the exercise's authenticity, we developed a scenario that merged several real-life elements of cyber activism, such as insider threats and the proliferation of malicious tools. Each firm provided two exercise facilitators to manage their respective logistical and infrastructure arrangements and to support exercise delivery to ensure that the experience was engaging for their Crisis Management Teams (CMTs). The exercise was held on 25 May 2023 and took place over five hours.

This report presents Control Risks' consolidated observations and a benchmarked assessment of the participants' performance and response on nine different criteria. We used a simple, four-level grading system to categorise the participants' performance within each criterion: excellent, proficient, developing, and needs improvement. (See Table 1: Summary of participants' performance by criteria on the following page.)

Participants were given the opportunity to evaluate their own performance immediately after the exercise. Overall, firms expressed confidence in their ability to manage a large-scale crisis such as the one we presented. However, there are areas where enhancements can be made to strengthen resilience capabilities. These include familiarising teams with crisis management protocols, mobilising resources for cyber incident response, improving communication within teams, identifying and prioritising affected stakeholders, and making decisions in uncertain circumstances.

Table 1: Summary of participants' performance by criteria

Category	Sub-category and definition	Number of members at each level
Crisis management planning and response	**Cyber incident response** Pre-defined actions and procedures that your firm follows when responding to a cyber incident or breach.	10 4 3 0
	Business recovery Capability to restore affected systems, applications, or data to their normal state.	8 7 1 1
	Roles and responsibilities Clear division of roles and responsibilities within the team.	8 5 4 0
	Scenario planning Ability to envisage the range of possible scenarios (in terms of impact) at the early stages of the crisis.	6 6 5 0
	Objective setting Ability to formulate key objectives.	11 2 2 1
Communication and coordination	**Stakeholder engagement** The team's ability to map and engage relevant stakeholders during a crisis.	8 8 1 0
	Record-keeping Maintenance of logs and effective recording of information throughout crisis scenario.	7 5 3 2
Decision-making	**Decision-making** Effectiveness of the decision-making process, focus on ransom demand.	10 4 3 0

Introduction

The DFSA engaged Control Risks to prepare and facilitate an inaugural crisis simulation exercise for its Authorised Firms, aimed at enhancing cyber resilience across the Dubai International Financial Centre (DIFC). The exercise was held on 25 May 2023, with 17 Authorised Firms taking part, and took place over five hours. It was facilitated by a team of consultants from Control Risks operating from a crisis command centre in the DIFC and supported by additional role-players from the DFSA.

This report presents Control Risks' consolidated observations and assessment of the participants' performance and response during the exercise. The purpose of this report is to acknowledge the participants' actions, identify strengths, and bring attention to areas that can be improved upon. It is not intended as a pass/fail assessment but to foster growth and enhance crisis management capabilities.

Control Risks thanks Ian Johnston, Justin Baldacchino, Ken Coghill, Otar Gogolashvili, Christian Cameron, and Mohamad El Khalil from the DFSA for their support and guidance during the preparation for this exercise.

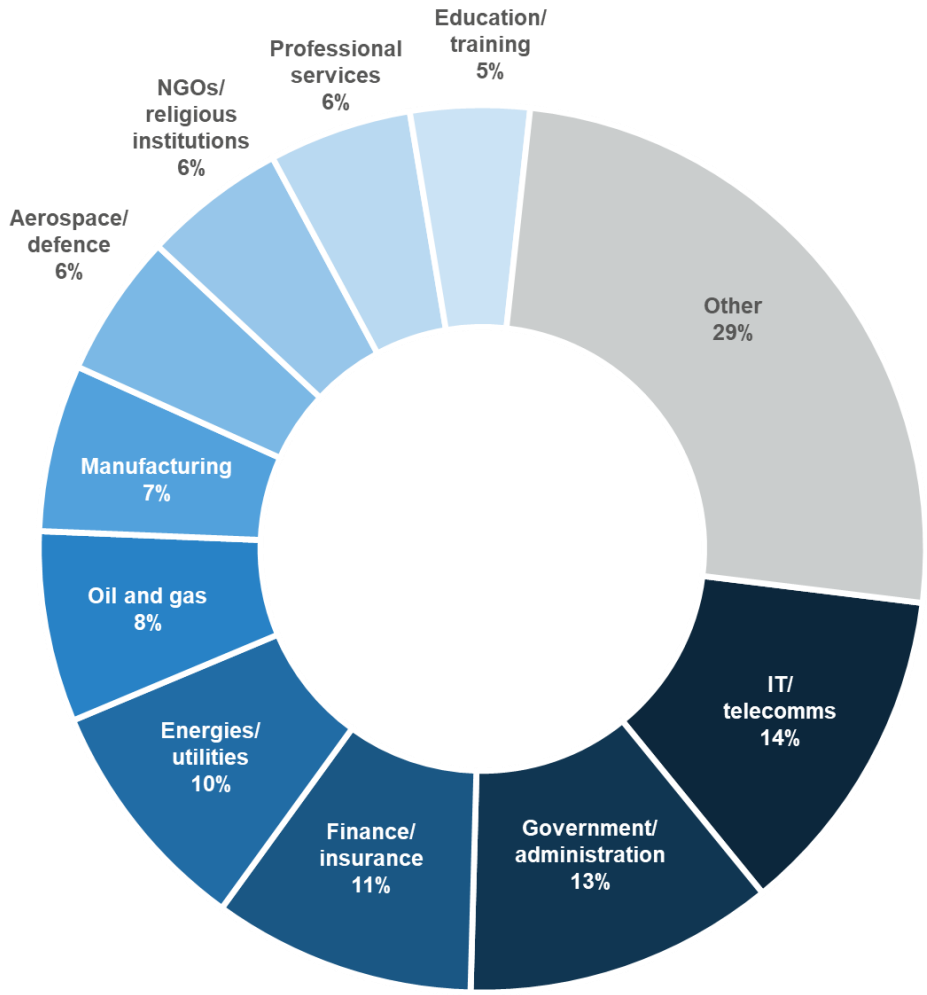
Cyber threats to the UAE

The UAE is one of the fastest-growing financial hubs, with a financial services sector that has undergone rapid digital transformation in recent years. This has led the UAE to become one of the most targeted countries globally by cyber threat actors, as attackers are attracted by high levels of internet penetration, mobile banking, and perceived wealth, and are motivated to exploit perceived low levels of cyber security awareness. Geopolitical tensions in the Middle East have also contributed to the UAE being targeted by advanced state actors for espionage, disruption, and financial gain.

The UAE's financial sector is a leading industry from a technology and innovation perspective and plays a key role in facilitating global transactions and cash flows. However, the sector's strong interconnection with a global supply chain of suppliers, network providers and partners has also made it an attractive target for cybercriminals motivated by fraud, extortion, identity and data theft, and money laundering. Attackers targeting the financial sector increasingly look for weaknesses in supply chains and third-party vendors.

Improving resilience requires both technological solutions, as well as an understanding of real-time cyber threats, conducting regular threat and risk assessments, and establishing incident response plans to recover from potential breaches.

Figure 1: The most targeted sectors in the UAE for cyber-attacks over the last two years



Source: Control Risks' Cyber Threat Intelligence

What is crisis management?

Crisis management is the way in which an organisation deals with a major event or problem that has the potential to harm the organisation, its stakeholders, or the general public, if not managed properly. These issues are usually critical, unexpected, extraordinary, urgent, and sometimes emotionally charged, making normal management methods inadequate. Crisis management involves following established procedures and plans, as well as using individual skills and practices.

ISO 22361[1], the latest guidance standards (published in 2022), provides clear definitions for *crisis* and *incident*. The standard defines a crisis as an "abnormal or extraordinary event or situation that threatens an organisation or community and requires a strategic, adaptive and timely response in order to preserve its viability and integrity." The definition emphasises terms like complexity, instability, uncertainty, capability, flexibility, and dynamism to highlight the nature of a crisis. On the other hand, an incident is defined as an "event or situation that can be, or could lead to, a disruption, loss, emergency or crisis."

What is a cyber simulation exercise?

A cyber simulation exercise is an activity designed to simulate real-world cyber-attacks or incidents in a controlled environment. It involves creating scenarios that mimic potential cyber threats and vulnerabilities to assess an organisation's preparedness, response capabilities, and effectiveness in managing such situations.

During a cyber simulation exercise, participants, typically members of an organisation's senior management and cybersecurity teams, simulate various cyber-attack scenarios, respond to them, and practice their incident response procedures and consider broader implications of the cyber-attack. Exercising aims to enhance the organisation's readiness and resilience by identifying strengths, weaknesses, and areas for improvement in their cyber defence capabilities.

Why conduct a cyber simulation exercise?

Financial institutions, regulators, and central banks in several countries regularly plan and participate in collective exercises known as industry-wide exercises. The purpose of these exercises is to train and improve the collective cyber resilience and response capabilities of multiple organisations within the industry. It involves bringing together various financial institutions and relevant stakeholders to assess their ability to manage large-scale cyber-attacks or incidents that could impact the entire market.

During these exercises, representatives from each organisation's CMT discuss how they would respond to a challenging hypothetical scenario created by a central command (simulation) centre. While a market-wide cyber simulation for the financial services sector aims to strengthen the sector's collective cyber resilience and improve the industry's ability to respond effectively to cyber incidents, it also seeks to:

- Promote cooperation and coordination among different organisations within the sector, allowing the exercise participants to share information, best practices, and insights, as well as fostering a collective defence approach to cyber threats.
- Identify the interdependencies and potential cascading effects that cyber incidents can have across the financial markets, thus enabling participants to prepare better and strengthen their resilience against such events.
- Assess the response capabilities of participating organisations, including incident detection, response coordination, communication, and recovery procedures to identify gaps, weaknesses, and areas that require improvement in participants' cyber incident response plans.

[1] ISO 22361:2022 Security and resilience — Crisis management — Guidelines (the International Organization for Standardization)

- Provide participants with the opportunity to assess and validate their crisis management plans and procedures in order to evaluate their effectiveness in a realistic and dynamic environment.
- Enhance participants' preparedness for potential cyber threats, allowing them to refine their incident response processes, train their personnel, and identify necessary improvements in their cybersecurity infrastructure.

Objectives of the DFSA exercise

Considering that the exercise was the first such initiative for the DIFC, the DFSA developed a set of objectives that were rigorous yet attainable so that the exercise would provide a solid foundation of knowledge and experience for participants to build upon. These objectives were:

- Build participants' awareness of the importance of cyber resilience.
- Provide participants with the opportunity to exercise and improve the effectiveness of their cyber crisis management capabilities.
- Improve the DFSA's capability to respond to a cyber incident affecting an Authorised Firm.

The simulation exercise 2023

17 firms participated in the exercise, representing the diverse range of sectors operating within the DIFC.

The participants included:

- One firm specialising in arranging and advisory services
- Five firms operating in the brokerage sector
- Four firms offering commercial banking services
- Two firms with operations spanning across diversified activities
- One firm engaged in Crowdfunding
- One investment bank
- Three private banking institutions

Exercise preparation

A threat-led approach

Control Risks and the DFSA chose cyber activism, often referred to as "hacktivism," as the crisis for the exercise, as it could be replicated in a simulation with the realism, context, and complexity of real attacks. It was decided that involving anti-capitalist anarchists would introduce a level of unpredictability and uncertainty during the initial stages of the exercise.

To bolster the exercise's authenticity, we developed a scenario that merged several real-life elements of cyber activism, such as insider threats and the proliferation of malicious tools.

These elements included:

- Activists acquiring knowledge of cybercriminal tactics, techniques, and procedures, including tools for computer network attacks, and demonstrating advanced capabilities.
- Disruptive attacks aimed at organisations through ransomware assaults accompanied by ideological statements, blurring the lines between state-sponsored, criminal, and activist attribution.
- Activists targeting critical organisations and sectors following significant political announcements impacting countries' economies.
- State-affiliated actors increasingly adopting the guise of cyber activists to heighten plausible deniability in disruptive attacks.
- The proliferation of malicious tools, coupled with the rise of the access-as-a-service market, where cybercriminals sell network access, thereby augmenting activists' capabilities.

We introduced two fictitious threat actors into the scenario: a cyber-activist group, and a ransomware operator. These entities played pivotal roles in the exercise, adding complexity and unpredictability to the scenario.

Scenario planning

The scenario plan was based on outputs of the European Systemic Cyber Group [2](ESCG). The Group is part of the European Systemic Risk Board, which defines systemic risk as the potential for a significant event occurring within a single firm that could consequently lead to serious instability or even cause an entire industry or the broader economy to collapse.

The ESCG has created a conceptual model for systemic cyber risk, which can describe cyber incidents from initiation to potential systemic events, demonstrate the link between individual company risk and potential financial system implications, identify system-wide vulnerabilities, support scenario-based analysis, and suggest system-wide interventions.

Although the model is designed for cyber incidents, it can be used for any operational disruption, and comprises four phases:

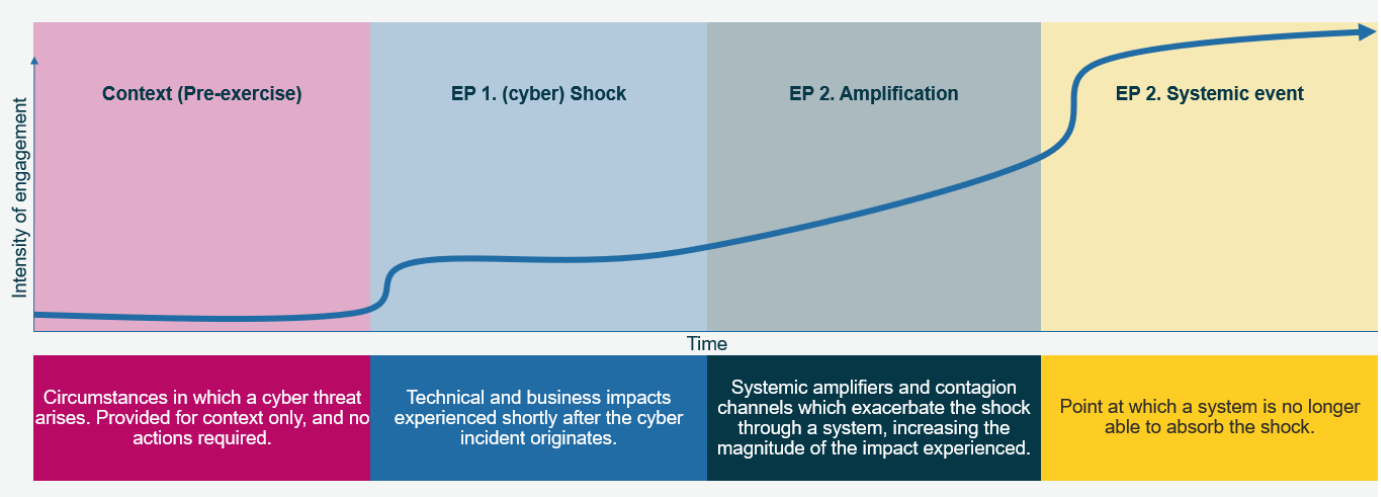
- Context
- Shock
- Amplification
- Systemic event

The ESCG noted that measuring impact is primarily a judgment-based, qualitative exercise that considers subjective or descriptive aspects not easily or comprehensively measured by quantitative metrics. However, it was acknowledged that some numeric or quantitative indicators do exist and could function as useful aids. The authors also proposed that a truly systemic event would require an exceptionally strong combination of negative factors to align. They proposed that more research should be conducted to evaluate the effectiveness of methods intended to lessen these large-scale effects, as well as to develop data-based strategies to quantify each step in the process of how these effects amplify.

The model provided us with a framework to explore the potential systemic risks posed by cyber incidents in the financial sector. We drew several insights from this document into how the complex dynamics and interconnectedness within the financial system can be influenced by cyber threats and use the model in Figure 2 as the basis for the scenario sequence.

[2] European Systemic Risk Board, “The making of a cyber crash: a conceptual model for systemic risk in the financial sector,” ESRB Occasional Paper Series No 16 / May 2020

Figure 2: Illustration of ESCG framework



Source: European Systemic Risk Board

Authorised Firm preparation

Each firm provided two exercise facilitators to manage their respective logistical and infrastructure arrangements and to support exercise delivery to ensure that the experience was engaging for their CMTs. Prior to the simulation exercise, the facilitators were invited to participate in a comprehensive programme of training and awareness sessions, meticulously designed to provide them with essential knowledge and skills in the field of crisis management.

These sessions were aimed at equipping them for their vital role as facilitators. They were provided with guidance on effectively using the exercise portal. To further enhance their preparedness, dedicated question-and-answer sessions and personalised one-on-one consultations were conducted with the facilitators in the weeks preceding the exercise. These measures were taken to ensure that the facilitators were thoroughly equipped and ready to fulfil their responsibilities.

Timing was crucial for the successful execution of, and optimal performance during, the exercise. Facilitators were given handbooks that contained talking points for each episode. This enabled them effectively to guide their CMTs in their responses.

Exercise delivery

Control Risks and the DFSA established a crisis command centre to manage the exercise. This was led by an exercise director and supported by the following teams:

- A facilitator liaison team that monitored the participants' progress and submissions for checkpoint and regulatory responses. This team also discreetly updated the facilitators throughout the exercise.

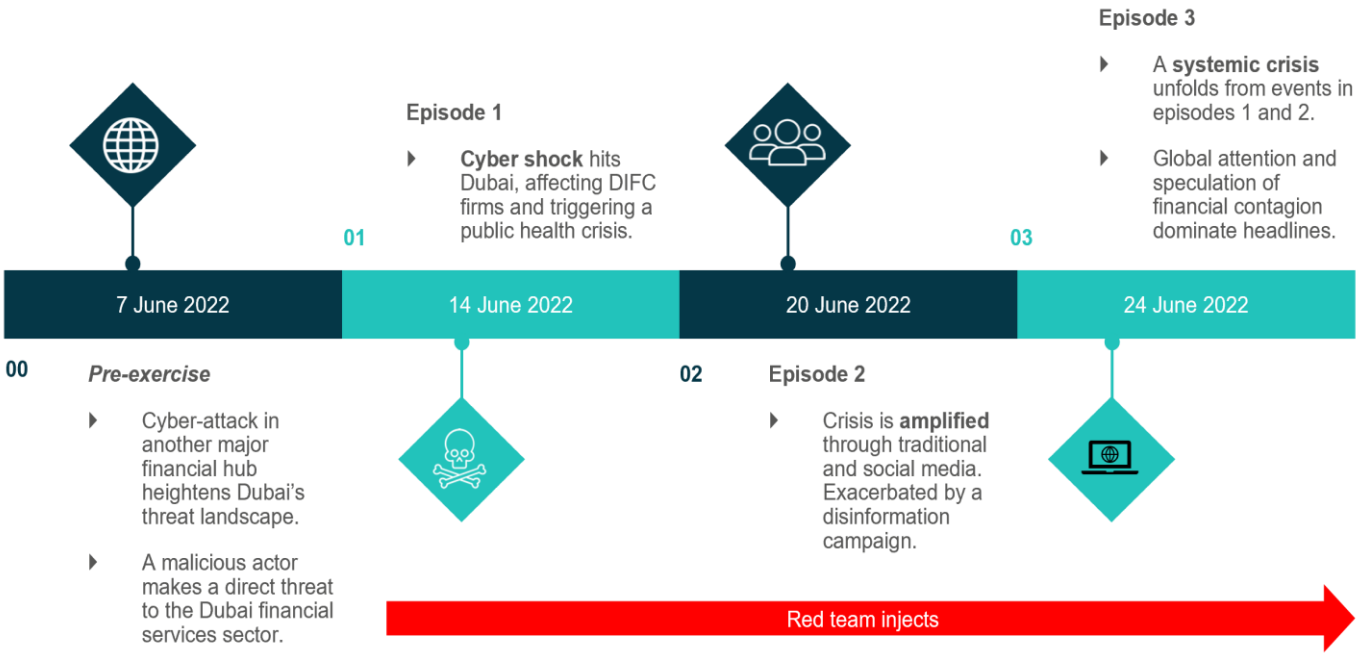
- An injector team of role players to dispense developments via telephone calls, and an 'exercise portal' dispensing news reports, social media updates, and emails, which let the scenario unfold progressively.
- A red team of role players assigned to exploit vulnerabilities or escalate the scenario to challenge the CMTs further, via phone calls from stakeholders and interested parties.
- An infrastructure and operations team to ensure that all technological requirements of the exercise, including the portal, communications, and other infrastructure, were effectively met.

The figure below illustrates how the exercise was structured and how facilitators were positioned to support their respective CMTs.

Figure 3: Exercise delivery structure

The exercise consisted of four episodes (as shown in Figure 4) and based on the structure provided by the ESRB paper discussed earlier. We began with a pre-exercise episode, taking place approximately one week prior in the scenario timeline, to provide participants with background information and context for the scenario. In this pre-exercise period, participants received information about an attack on a (fictional) bank in South Korea and were warned that a similar attack could occur in Dubai.

Figure 4: Scenario outline[3]



The main scenario was divided into three episodes of approximately 60 minutes (real time) each, each signifying a working day within the scenario timeline, with each working day simulation occurring four to seven days apart.

The exercise was designed so that firms would receive information relating to the crisis, known as injects, via a crisis exercise portal and from the role players. Injects were created to challenge the participants and provide them with a series of realistic and dynamic situations. The goal was for the CMTs to identify and analyse emerging issues, make decisions, coordinate resources, communicate effectively, and implement appropriate actions.

Examples of injects used in the exercise include:

- Simulated news reports announcing major events in the crisis and summarising key points at the beginning and end of each episode;
- telephone calls from stakeholders or affected individuals requesting assistance or information; and
- social media posts and emails with updates on the situation, new challenges and regulatory requests for information;

To enhance the pace and realism of the exercise and create a more challenging experience, many of the firms received additional disruptive interaction from the "red team" to escalate the crisis further. These came in the form of telephone calls from role players pretending to be concerned customers, journalists, ransomware operators, and the DFSA itself.

[3] Source: Control Risks, citing European Systemic Risk Board, "The making of a cyber crash: a conceptual model for systemic risk in the financial sector," ESRB Occasional Paper Series No 16 / May 2020

The purpose of doing this in crisis management is to simulate the mindset of potential adversaries and stress test the CMTs by exploiting potential flaws and vulnerabilities in their response or assess the CMTs in adapting to new threats or unexpected situations, to stress test the crisis management system, ensuring it can manage a variety of potential scenarios. Red teaming may also serve to identify vulnerabilities in the crisis response plan that might not otherwise become apparent.

Firms were also requested to submit responses to a series of predetermined questions at various stages ("checkpoints") of the exercise, which were designed to assess the pace and level of engagement from the CMTs, and regulatory requests for information (RFIs) prepared by the DFSA, to understand firms' responses to the scenario. Responses to these questions later formed the basis of our exercise findings.

Exercise findings

In this section we acknowledge the participants' actions, identify strengths, and bring attention to areas that can be improved upon. Our observations are principally based on the information provided by the firms' CMTs via the checkpoint questions, regulatory requests for information (RFIs), CMT record-keeping, and feedback from our role-players.

Our findings are framed under three main categories:

- Crisis management planning and response;
- Communication and co-ordination; and
- Decision-making.

This assessment is subject to certain limitations, which might distort our overall findings. Participating firms represented the diverse range of sectors within the DIFC and varied in size; spanning from large multinationals to smaller, regional firms. In line with this, we observed a pattern: larger firms had more resources to manage and report on the crisis, while those smaller firms with fewer resources tended to furnish only limited information about their responses.

It is important to emphasise that our findings do not necessarily suggest inadequacies in firms' abilities to manage crises. Instead, we have noted areas that firms agreed would potentially benefit from further attention to enhance their resilience capabilities.

To ensure simplicity and clarity, we used a four-level grading system.

Excellent: Participants at this level demonstrate outstanding abilities, making significant contributions and effectively driving the crisis management process.

Proficient: Participants here show a high degree of competence, handling tasks effectively though not as exceptionally as those rated as 'Excellent'. They communicate well, make sound decisions, and are adept at solving problems and coordinating resources.

Developing: Participants at this stage are demonstrating growth in their capabilities but have not yet reached the level of 'Proficient'. They showed potential for improvement, and with continued experience and training, they could enhance their skills in leadership, decision-making, communication, problem-solving, and resource coordination.

Needs improvement: Participants at this stage may face issues with leadership, decision-making, communication, problem-solving, and resource coordination. They require further training, experience, or support to reach higher levels.

This section also provides feedback from a "hot debrief." The hot debrief took place right after the exercise concluded, involving each participating firm answering a series of self-assessment questions. The objectives were twofold: firstly, to aid each firm in evaluating their self-confidence in crisis management and benchmark these skills against each other; secondly, to offer participants a chance to reflect on their actions, measure their performance, and assess the effectiveness of the strategies and procedures implemented during the exercise.

Overall, responses to the hot debrief suggested that the participants have high degrees of confidence in their abilities to manage a cyber-related crisis of the scale simulated in the exercise. However, participants recognised that understanding crisis management protocols, mobilising resources for cyber incidents, ensuring effective communication during crises, identifying and prioritising affected stakeholders, and accelerating decision-making under pressure are all areas in which it is worth enhancing their expertise.

Crisis management planning and response

Crisis management preparations are indispensable in minimising damage and facilitating recovery efforts in the aftermath of a crisis. Comprehensive crisis management planning takes into account the range of processes, responsibilities, and resources required to ensure an efficient, effective, and unified response to a wide array of potential threats.

While our analysis is somewhat constrained by the comprehensiveness of responses to the self-assessment questions, the majority of participants expressed a high degree of confidence in the efficacy of their firms' crisis management and recovery protocols. This confidence extended to their plans' comprehensiveness, the Crisis Management Team's (CMT) implementation thereof, the belief in their potential effectiveness, and the efficient allocation of necessary resources during a crisis scenario exercise.

It is worth noting, however, that only a small number of firms expressed uncertainty regarding their firms' capacity to manage unexpected challenges. There was also minor scepticism concerning whether their CMTs would have successfully mitigated the crisis's impact. Despite these reservations, the overall impression given was one of confidence and preparedness. This showcases firms' commitment to showcasing their readiness for potential crisis scenarios to the regulator, despite the limitations inherent in self-assessment methodologies.

Cyber incident response planning

Cyber incident response is critical for organisations, as it establishes pre-defined actions and procedures to follow when responding to a cyber incident or breach, enabling a rapid and coordinated response. It helps minimise the impact of the incident, mitigate further damage, protect sensitive data, and restore the organisation's systems and operations, safeguarding its reputation and maintaining the trust of stakeholders.

Fourteen of the firms evaluated received an *excellent* or *proficient* score for their demonstrated cyber incident response protocols. The lowest scoring received by firms in this section was *developing*, with three firms placed in this category. The larger firms were more effective at articulating their technical response capabilities and demonstrating how these were supplemented by formalised procedures for cyber incident response ("playbooks"). Furthermore, those firms with operations beyond the UAE successfully harnessed expertise from their international offices, contributing in some

instances to higher evaluation scores. On the other hand, smaller firms placed more emphasis on technical responses than on broader crisis management protocols. Although we assess that the smaller firms' cyber incident response capabilities were less comprehensive than their larger counterparts, there were clear indications of prior planning.

Business recovery

Business recovery is a crucial component of any cyber response plan, aimed at quickly restoring operations and reducing downtime following a cyberattack. On this topic, 15 firms achieved either an *excellent* or *proficient* rating for demonstrating their business recovery capabilities, while two firms were categorised as *developing* or *needs improvement*.

This reflects a significant level of awareness among participant firms about the necessity of organisational resilience; i.e., rapid operational restoration and downtime minimisation after a cyber-attack. Such measures are crucial in mitigating potential losses and ensuring the protection of stakeholders' interests. Furthermore, this highlights the value placed by firms on resilience and readiness, demonstrating that they are prepared to face potential cyber threats effectively, further reinforcing the trust of their stakeholders in their ability to manage crises.

Roles & responsibilities

Clear division of roles and responsibilities within a CMT is vital for effective decision-making, coordination, and a swift response to the crisis. It ensures that each team member knows their specific tasks, eliminating confusion, promoting accountability, and enhancing their overall efficiency in mitigating the impacts of the crisis.

Eight firms were awarded an *excellent* score, while five received a *proficient* score for their responses. Most firms demonstrated the existence of a clear delineation of roles and responsibilities within their teams. These roles varied widely, from managing the technical response to managing stakeholder communications.

A heightened understanding of individual roles and responsibilities within Crisis Management Teams (CMTs) likely played a significant role in firms' performance. This would have led to improved coordination and internal communications, helped avoid role overlaps and misunderstandings, and enabled a comprehensive response strategy that considered the range of risk factors facing the firms.

Scenario planning

Scenario planning is invaluable in crisis management, as it allows organisations to anticipate and prepare for a range of potential scenarios, enabling them to respond swiftly and effectively when faced with unexpected events. Responses

across firms varied, with some firms concentrating exclusively on the cyber-attack and its direct impact on customers. In contrast, the more advanced CMTs accounted for the cascading effects of the crisis. In line with this, 12 firms received either an *excellent* or *proficient* score for articulating their scenario planning; 5 firms received a score of *developing*.

Our assessment suggests that there is room for improvement in distinguishing between incident management and crisis management. The latter requires firms to adopt a more proactive approach in identifying and planning for the range of potential impacts and formulating robust strategies to manage these effectively. This proactive approach promotes resilience in firms. It is important to note that forecasting in crisis management is more of an art than a science, requiring a combination of real-world experience, creative problem-solving and strategic planning.

Objective-setting

Objective setting plays a crucial role in crisis management by providing a clear direction and purpose under highly uncertain conditions. It enables CMTs to define their desired outcomes, prioritise actions, and allocate resources effectively, guiding decision-making and ensuring a focused and coordinated response to the crisis.

Thirteen firms received a score of either *excellent* or *proficient*, indicating that the majority of the participants have a clear understanding of their objectives, and their CMTs demonstrate strong leadership in crisis scenarios. Only three firms scored as *developing* or *needs improvement* in this category. Feedback from these firms indicated a tendency towards a reactive focus; i.e., embodying an incident management mindset, rather than adopting the more strategic approach required in crisis management. These findings resonate with the points discussed in ‘scenario planning’ above.

Communication and co-ordination

Effective crisis management relies on clear, timely, and accurate communication. Information must flow seamlessly among members of the CMT, as well as between different response teams such as technical, communications, and legal. Our evaluation on communication and coordination is based on two sub-categories: stakeholder engagement and record-keeping.

In the hot debrief, participants generally reported high degrees of confidence in their proficiency in recognising and working with external stakeholders during a crisis, and the efficacy of communication among CMT members. However, despite their strong confidence in communication and coordination capabilities, some participants may not have fully recognised the crucial role that good record-keeping plays in post-incident communication and coordination.

Stakeholder engagement

A cyber crisis will directly and indirectly affect a range of stakeholders. These could include employees, customers, shareholders, suppliers, or even the wider community. Identifying and prioritising their needs and concerns is crucial to an effective crisis response and subsequent recovery. This enables organisations to effectively address concerns, manage expectations, and collaborate on solutions, leading to better outcomes and the preservation of long-term relationships. An effective internal process for communicating with stakeholders, including issuing statements and responding to media inquiries, is also vital in crisis management, as it enables organisations to provide timely and accurate information, manage public perception, and maintain control over the "narrative;" i.e., the organisation's messaging, key points, and information shared to shape public perception and understanding of the situation.

Sixteen firms received a score of either *excellent* or *proficient*, with only one firm falling into the *developing* category. These results underscore a significant degree of awareness among firms about the importance of keeping stakeholders informed. These practices help curb speculation and misinformation and safeguard the organisation's reputation by promoting transparency, accountability, and a proactive stance in crisis management.

Record-keeping

Maintenance of logs and effective recording of information throughout crisis management are crucial for several reasons. They provide a documented account of events, actions taken, and decisions made, providing CMTs with a "single source of truth" and enhancing the flow of crucial information between response teams. In this category, twelve firms scored either *excellent* or *proficient*, due to the comprehensiveness of the information they provided. However, five firms only reached the *developing* or *needs improvement* tier due to their provision of limited information and absence of record copies afterwards.

Record-keeping in crisis management is often viewed as an administrative burden. However, CMTs should place more emphasis on this important aspect of crisis management, as it serves a critical function in tracking progress, ensuring accountability, preserving a legal record of events, and facilitating post-crisis reviews for learning and potential improvement.

Decision-making

This is arguably the most challenging aspect of crisis management. Crises are inherently chaotic and unpredictable, often requiring quick decisions in the face of uncertainty. Effective decision-making is vital, as it determines the course of action to be taken by response teams. Timely and well-informed decisions help minimise the impact of the crisis, allocate resources appropriately, and mitigate potential risks, ensuring a swift and effective response that protects both

the organisation and its stakeholders. It is often said that some decision is better than no decision. When faced with a crisis, the urgency and complexity of the situation can lead to a sense of paralysis or indecision.

In the hot debrief, participants generally reported high degrees of confidence in the effectiveness of their decision-making processes.

In this category, fourteen firms secured a score of either *excellent* or *proficient*, leaving only three to receive a *developing* rating. The scenario provided firms an opportunity to practice their decision-making skills in a challenging and complex situation. A critical aspect of the exercise for firms involved deciding whether to comply with the ransomware operator's demand. Role players reported that, when putting pressure on the Crisis Management Teams (CMTs), the majority of firms resolutely declined to satisfy ransomware demands. The emphasis, however, was not placed on the decision itself, but on the considerations articulated by the firms when weighing their options.