# DFSA Cyber Risk Forum

## Remaining resilient in the era of transformation and disruption

**17 November 2020**
**Bryan Stirewalt, Chief Executive, DFSA**

## Opening Remarks

Good afternoon everyone and welcome to our first edition of the DFSA Cyber Risk Forum. Let me start by saying thank you for making the time to join us for this event, especially our speakers, panellists, and moderators. As 2020 was declared as the year we prepare for the next 50 years in the UAE by the government, this is a great topic to begin our journey. We have assembled a great set of speakers for this event, but most importantly we can all look at ourselves as partners in driving this agenda forward.

As we consider many possibilities for technological advancement, operational resilience, including cyber risks, is one of the most important topics that I see in front of us for the foreseeable future. I am proud of our team's efforts to push this topic forward in an attempt to address the many challenges this topic presents.

### Innovation and Cyber Risk

Last week, we hosted the second edition of RegTech Live where we talked about how technological innovation and digital transformation is reshaping business overall, but specifically in financial services, and even more specifically, in governance, risk management and compliance. It is not a coincidence that we are holding this Cyber Risk Forum immediately following the RegTech Live event.

Technological innovation and digital transformation has accelerated rapidly in 2020, far more rapidly than we envisioned at this time last year, and we are not nearly done yet. While this brings many efficiencies, it also brings new risks, particularly exposure to cyber risks.

The more we innovate, the more complex our critical information systems become. The more complex our systems become, the more potential vulnerabilities we create. And, the more sophisticated we become in our defences, the more sophisticated the attackers become. This cycle goes on and on.

As a consequence, even the best defences cannot eliminate completely the risk of a successful cyber-attack. To those individuals and institutions that are confident their defences are impenetrable, I would remind you there remains one low-tech element that exposes institutions to the highest probability of a cyber incident. That is people. When you're assessing the complexity of your critical systems and deploying advanced defence mechanisms, don't forget to account for the "human factor." Cyber risks have just as much to do with people management and behaviours as it does with software and hardware.

In this globally connected world, we are not only at risk through our own business activities and the people within our own organisation, but we are exposed to the cyber risks of our business partners, our clients, and our counterparties. An attack that impacts one of us, is an attack that threatens all of us.

So what can financial institutions do? Clearly, the priority is to prevent a cyber incident from occurring, but it is a question of when – rather than if – a cyber incident will occur. Therefore, it is vital to have an effective response strategy to ensure that attacks can be quickly detected, analysed and responded. Knowledge sharing and industry collaboration is also important to stay ahead of the curve. Similar to their effectiveness in fighting financial crime, public-private partnerships are critical to cyber prevention and response strategies.

## DFSA Cyber Risk Supervision

At the DFSA, over the past three years, we have been steadily increasing the intensity of our cyber risk supervision programme by focusing our reviews on cyber risk governance, hygiene practices, and resilience capabilities. Very importantly, these efforts support the UAE Cybersecurity Strategy and the Dubai Cybersecurity Strategy, and are designed to strengthen the cybersecurity environment in the DIFC.

- In October of last year, we launched an online incident reporting mechanism for Authorised Firms to report cyber incidents to the DFSA. The objective of the mechanism is to provide the DFSA with consistent reporting of incidents, to make clear to Firms what information the DFSA expects to receive, and provide the DFSA timely information with which to assess the potential for systemic impact.

- Also in October of last year, we hosted our first in a series of cyber roundtables. Constant and open communication has been, is, and will be a key pillar of the DFSA in fulfilling our regulatory objectives. The purpose of these sessions is to deepen our understanding of the challenges Firms face in maintaining effective cybersecurity. We will do more of these sessions.

- In January of this year, we launched the DFSA Threat Intelligence Platform (TIP). TIP is the region's first regulator-hosted cyber threat intelligence platform. You will hear more about TIP at the end of today's session so for now, I will just say that I encourage all DFSA Authorised Firms and DIFC-registered companies to register to use the platform.

- In April, we hosted our first threat intelligence workshop. The workshop was for companies that had registered to use TIP and the purpose was to assist them in understanding how to use TIP and how to use the threat intelligence that is available on TIP.

- In June, we published the findings of our cyber thematic review. The objective of the review was to identify the overall maturity level of cyber security programmes of Authorised Firms.

- This month we posted to our website our approach to cyber risk supervision; and shortly, we will publish a set of cyber risk guidelines.

## Conclusion

Today, we’ll hear from a number of industry experts about what the current cyber threat landscape looks like, including: the impact of innovation, digital transformation and COVID-19 on cyber risk; best practices in protecting from and responding to cyber incidents; transaction monitoring and fraud detection; what we should be doing to protect our own environments; and finally, you’ll hear the DFSA’s views on cyber risk.

I will leave you with one final thought, which I briefly mentioned earlier. Cyber risk is not just an IT problem. It is a problem for the whole organisation. And it is not just an organisation’s problem. It is a problem for the whole industry. The only way to effectively address this problem is through a collective effort of public-private collaboration and information sharing. And that is why we are here today.