F. Christopher Calabia

Opening Remarks DFSA Cyber Risk Forum

16 November 2021

Have you noticed changes in Dubai? Although I've been here for just six weeks, I've heard from many that the traffic has gotten a lot heavier. Restaurants and shops are doing brisk business again. And the malls seem as crowded as ever.

These are all good signs that public health conditions are improving. Our progress in addressing the pandemic reflects collective efforts from all of us in the public and private sectors. We've protected each other and worked to mitigate harm from the virus while supporting a recovery.

Because of this public/private partnership, many organisations around the world are resuming their in-person operations. We at the DFSA have returned to the office, as have many firms here in the Dubai International Financial Centre. Life in Dubai is beginning to feel a bit more normal, even as we must remain vigilant.

Over the last 18 months, we've learned that a strong digital infrastructure provides greater resilience to financial institutions and their regulators. Most firms had to switch to remote working arrangements almost immediately. Those who hadn't previously made investments in their IT infrastructures faced more challenges than those who were further along in their digital transformation. Cyber criminals took advantage of these gaps and started searching for, and exploiting, poorly secured systems.

And that's why we're hosting today the second edition of the DFSA Cyber Risk Forum. We want to strengthen our collective understanding of the current cyber risk landscape. We want to plan how we can work together to mitigate ransomware and other attacks. Let me begin by thanking you for joining us, especially our speakers, panellists, and moderators.

Even the most sophisticated defences cannot eliminate completely the risk of a successful cyber-attack. Some of the world's best resourced companies and governments have fallen victim to cyber-crimes. So, it's critical not to feel overconfident about the quality of our own defences.

While we can invest in the highest tech to harden our defences, don't forget that the lowest-tech elements of our businesses are sometimes the most exposed to cyberthreats – namely, our people. In 2020, the UAE witnessed a 250% increase in cyberattacks, including an exponential

surge in phishing and ransomware. Studies show that the UAE faced over 1.1 million phishing attacks in 2020 and more than a 33% increase in the number of new ransomware families compared with 2019. Some cybercriminals exploited concerns about COVID-19 in their campaigns, reminding us that although phishing and ransomware are well-known threats, both remain effective means of attack.

When assessing the complexity of your critical systems and deploying advanced defence mechanisms, please remember the human factor. Virtually every employee in a financial institution is a technology user. We must educate everyone to employ good "cyber hygiene" so that we can protect both ourselves and our organisations against cybercrime. When we educate our staff, they can become our greatest allies in our cyber defences.

Cyber security remains one of the DFSA's top priorities. We expect Authorised Firms to invest in sufficient safeguards to protect against a cyber-attack; moreover, we expect Authorised Firms to have appropriate responses when they experience an attack. This includes maintaining a robust governing body to oversee cyber-risk management; effective hygiene practices; and thorough response and recovery plans.

Over the past four years, the DFSA has steadily increased the intensity of our cyber risk supervision programme. We have focused our reviews on cyber risk governance, hygiene practices, and resilience capabilities. I'll summarise briefly six initiatives to enhance our supervision programme:

- First, we launched an online incident reporting mechanism for Authorised Firms to report cyber incidents to the DFSA in a consistent and timely manner.

- Second, we published the findings of our first cyber thematic review in June 2020 on our website. Based on the results of the review, we developed and published the DFSA Cyber Risk Management Guidelines in December 2020 to provide firms with information on good practices that should be applied to manage cyber risk.

    - We will shortly conduct a survey to refresh our assessments of the maturity level of the cyber security programmes in the DIFC and the challenges that Firms are facing. We will share our findings with you to raise awareness of new trends and emerging risks.

- Third, we have conducted extensive industry outreach. Today's forum is one of many we've hosted to raise cyber awareness in the DIFC. These events have included

Dubai Financial Services Authority

  - sessions to discuss our regulatory expectations;
  - cyber roundtables to deepen our understanding of the challenges Firms face; and
  - technical workshops to explore threat intelligence use cases and practical examples of controls described in our Cyber Risk Management Guidelines.

- Fourth, we launched the DFSA Threat Intelligence Platform (TIP). TIP is the region's first regulator-hosted cyber threat intelligence platform. To date, over 170 entities are registered on the platform. Our partners and members of the platform share information on around 160 threats every week, such as malware, ransomware and phishing campaigns. Please tell us how you use this platform and what we can do to improve it. I encourage all DIFC firms to register and start using the platform.

- Fifth, we assess how firms manage cyber risk. This is the heart of our cyber risk supervision programme. We conduct annual desk-based and onsite cyber risk-focused assessments of select Authorised Firms. Each year, we will choose a different group of Authorised Firms to assess.

- Finally, and sixth, we conduct internal training so that all of our supervisors will include cyber risk as a standard element of periodic risk assessments.

Today we'll hear from a number of industry experts about new concepts in cyber security, such as zero-trust architecture, and evolving risks like supply chain cyber-attacks. We will also talk about how we can stand together to face down these threats.

This brings me back to the improvements we've seen for life in Dubai. The progress we've achieved in responding to COVID-19 reflects hard work and collective action between the public and private sectors. Cyber security, too, is a shared responsibility. It's not a problem just for your IT department. It's not a problem for just one institution or one jurisdiction. It is a problem for the whole organisation, for the whole industry, and for all of us.

The swashbuckling heroes of Alexandre Dumas's nineteenth century novel, "The Three Musketeers," had a battle cry that is especially relevant today: "All for one, and one for all!" When any one institution falls prey to a cyber-attacker, it becomes a potential threat to every other institution it works with. If any of them subsequently fall victim to the attack, the damage spreads quickly.

Dubai Financial Services Authority

As the global economy becomes more digital, the challenges of conducting communications, trade, and finance across distances fade away, creating new opportunities for commerce and connection – but also potentially more nodes for cyber risk to emerge.

How can harden our mutual defences against attack? How can we reduce the risk that one of us falls prey to a cyber-criminal? How can we prevent harms from spreading across the sector or to our customers?

We must set aside commercial and competitive interests. We must work across the public and private sectors in partnership. We must truly be all for one, and one for all.

Thank you again for joining our dialogue. I hope that today's forum will inspire you to help us strengthen our shared cyber defences.

Level 13, The Gate, PO Box 75850, Dubai, UAE
Telephone: +971 (0)4 362 1500
Fax: +971 (0)4 362 0801