Norman T L Chan: Cybersecurity developments for Hong Kong's banking sector

Keynote address by Mr Norman T L Chan, Chief Executive of the Hong Kong Monetary Authority, at the Cyber Security Summit 2016, Hong Kong, 18 May 2016.

* * *

Good morning Mr. M.Y. Wong, Frank, Carrie, Chung Sir, Ladies and Gentlemen,

It is a great honour to be invited to speak at today's Cyber Security Summit.

Importance of cybersecurity

1. It is hard for us to imagine how quickly the digital and internet technology has transformed the way in which we live our lives. Twenty years ago many of us were wondering whether internet banking would become widely accepted as a preferred and trusted channel for conducting banking businesses. Now it would be hard to contemplate how a retail bank can survive a single day if the internet or digital banking services are down for whatever reasons. There are very good reasons why internet banking has gained such high popularity as a channel of service delivery in the banking and other financial sectors. In the cyber world, the usual constraints imposed by the physical world no longer exist. Information, messages and transaction instructions can be communicated between banks and their customers easily and almost instantaneously regardless of the location of the parties concerned. The cyber world offers the convenience and speed in accessing banking and financial services that were unthinkable 10 to 15 years ago. The advance in digital technology meets the needs of the rapidly growing client base with ever increasing demand for a wide diversity of services. However, very often people tend to focus on the ease and low cost of access in digital banking and do not pay too much attention on the security of the cyber world, at least until they are hit by cyber attacks.

2. Given the virtual nature and interconnectedness of the cyber world, clearly the security of the cyber world would require different approach and tools from those used in the physical world. In the real world, you would protect your home and property by installing a safe door with a strong lock. You may want to buy a safe deposit box to store your cash and valuables at home. Some may even subscribe to an anti-burglary system. For those who take their home security even more seriously, they may hire on-site security guards, just like the kings and queens who build heavily guarded forts to protect them and their families from the attacks by their enemies. Well, one thing for sure, all these security or safety measures do not come cheaply but it is the price that people know that they have to pay for the protection of their physical properties.

3. In the cyber world, just like the real world, there are plenty of risks and dangers. Financial crimes will occur whenever there is money to be made and for sure criminals and hackers alike will use their best endeavours to penetrate the defence of the cyber world to rob or steal. The strength of the cyber world also lies its main weakness. Hackers can choose to attack customers and financial firms any time and anywhere because the virtual world is highly interconnected. Cyber attacks can take many different forms. A frequently used method is to make phishing attempts to trick customers into divulging their account information and passwords, or to plant malwares into customers' computers and mobile phones to steal their access credentials. Then the hackers transfer moneys from the victims' accounts. Sometimes the hackers would do something unusual, such as the recent example in

Hong Kong in which some customers' bank accounts had been used by hackers to conduct unauthorized stock trading without stealing money from the victims' accounts. At the bank level, the usual form of attacks would be Distributed Denial of Services (DdoS), whether they are motivated by blackmail, revenge or activism of some sort. There is a worrying trend that this form of attacks is rising very fast in recent years.

Cybersecurity fortification initiative

4. Rather than harbouring the hope that you are lucky enough not to be targeted, it is more prudent and productive to take the necessary pre-emptive steps to protect yourself or your customers from cyber attacks. Cybersecurity is the very foundation of modern banking and without it there is no point for us to boast Hong Kong as a world class international financial centre. While banks in Hong Kong have so far had very few incidents of serious cyber attacks, there is no place for complacency if we wish to maintain Hong Kong's competitive edge as the preferred financial hub in Asia. In this connection, the HKMA has earlier this year set up a new Fintech Facilitation Office, which has taken cybersecurity as its top priority mission. Having worked very closely with the banking industry and other stakeholders, I am very pleased to announce today that the HKMA has decided to launch for the banking system a "Cybersecurity Fortification Initiative", which is known as "CFI" in short. The CFI consists of three pillars:

   (a) a Cyber Resilience Assessment Framework;

   (b) a Professional Development Programme; and

   (c) a Cyber Intelligence Sharing Platform.

Let me elaborate on these three pillars.

Cyber resilience assessment framework

5. We have about 200 banks in Hong Kong and they have a very diverse range of business models with understandably very different channels and modes of service delivery. Depending on the ways and technology platforms in which their businesses are conducted and delivered, the risk or vulnerability to potential cyber attacks varies from bank to bank. Needless to say, the volume and value of banking transactions conducted through the cyber world also matter a great deal. As a result, the level and sophistication of the defence against cyber attacks need not be the same for all the banks in Hong Kong. So what the Cyber Resilience Assessment Framework seeks to establish is a common risk-based framework for banks to assess their own risk profiles and then use these profiles to determine the level of defence and resilience that would be required to accord appropriate protection against cyber attacks, drawing references to the relevant international experiences and good practices.

6. Once the risk profile of a bank and the level of resilience needed are established, the HKMA will require the bank, under the guidance of the senior management and, where appropriate, the board of directors to put in place proper governance arrangements and processes to achieve the level of resilience in cybersecurity commensurate with the risk profile of the bank. Specifically, the HKMA will examine how effectively a bank can detect and protect itself from attacks and, when the bank gets hit, how it will respond and how quickly it can recover. Clearly if there is a shortfall between what is needed and the actual preparedness, the HKMA will follow up with the bank to bring up the level of resilience as soon as practicable.

Professional development programme

7. A crucial factor affecting the success or otherwise of the CFI is the availability of qualified and competent practitioners who can help the banks and the HKMA in the areas of risk assessment, design and implementation of the defence mechanism and the day-to-day management of cybersecurity. Unfortunately, there is a general shortage, globally, in the supply of qualified professionals in the field of cybersecurity and Hong Kong is of no exception. So the second pillar of our CFI is to develop a training and certification programme in Hong Kong so that we may have an increased supply of qualified professionals in cybersecurity going forward. I am very pleased to announce that, in collaboration with the Hong Kong Institute of Bankers (HKIB) and the Hong Kong Applied Science and Technology Research Institute (ASTRI), a new training and certification programme in cybersecurity will be launched. I am also very pleased to say that we are collaborating closely with CREST, the UK cybersecurity certification body, to ensure that the programme in Hong Kong is designed and benchmarked against the latest international standards in this field. I understand that Mr Ian Glover, President of CREST International, is with us today and he and Carrie Leung of HKIB will talk more about this professional development programme later on. What I would say here is that the training and certification programme in Hong Kong will offer three levels of competence: "foundation", "practitioner" and "expert". Suitable arrangements will also be introduced to ensure that relevant or equivalent experience and expertise in the cybersecurity field will be appropriately recognized.

Cyber intelligence sharing platform

8. Last but not least, the third pillar of the CFI is to develop a new piece of infrastructure for the purpose of sharing intelligence on cyber attacks. Just like any conventional warfare, intelligence is the key to success. While individual banks can develop their own intelligence network, the coverage of such intelligence and the timeliness of receiving cyber attack alerts may at times be limited. At the same time, the entry barriers for launching cyber attacks, in terms of costs and the hardware and techniques required, have become much lower. The speed in which hackers may launch cyber attacks, which may well be targeting at not just one bank but several banks at the same time, has greatly increased. So it will be of great help if the banks could collaborate by proactively sharing information and intelligence of cyber attacks or the imminent threats of such attacks. The timeliness of receiving alerts or warnings from a commonly shared intelligence platform will be of immense help for banks to prepare for cyber attacks even before they are launched.

9. I am pleased to announce that the HKMA, in collaboration with The Hong Kong Association of Banks (HKAB) and ASTRI, is going to launch a Cyber Intelligence Sharing Platform, with access open to all the licensed banks in Hong Kong. Arrangements will be put in place to ensure that the platform will gather useful and relevant intelligence, including those communicated in the Chinese language. The platform would also ensure that users would feel comfortable with providing intelligence on cyber attacks without compromising proprietary information. Needless to say, access to the platform will be through secure channels with robust encryption and on a need-to-know basis.

Way forward

10. Ladies and Gentlemen, having announced the launch of the CFI, the HKMA will move full steam ahead in collaboration with our partners and the stakeholders to roll out the programmes I just mentioned with the following timeline:

(a) the HKMA will issue a formal circular to all banks next week, stating clearly that it is a supervisory requirement for banks to implement the CFI;

(b) we will at the same time conduct a three-month consultation with the banking industry on our detailed proposals on the risk-based Cyber Resilience Assessment Framework;

(c) we will work with the HKIB and ASTRI to roll out the first training courses for cybersecurity practitioners by the end of this year; and

(d) we will work with the HKAB and ASTRI to set up the Cyber Intelligence Sharing Platform by the end of this year.

11. I understand that the timeline for rolling out the CFI programmes is very tight. However, if we wish to raise the cybersecurity resilience of our banking system to a level commensurate with Hong Kong's position as the leading international financial centre in Asia, we cannot afford to go slow or lose any time. In a spirit of cooperation to achieve this common goal, the HKMA, the banking industry and our partners will work closely together to implement this ambitious but necessary CFI according to plan. In closing, I would like to emphasise that in the physical world, there are very few, if any, of the defences of the strongest forts that ever existed can prove to be totally impenetrable by attackers. That is why I believe that, in the cyber world, by the same token the fortification initiative against cyber attacks that we are pursuing is not going to be a one-off exercise. It will be an ongoing battle or a fact of life that any successful financial centre must contend with and win if we wish to stay ahead of the game. Thank you!