INTERVIEW WITH HONG KONG APPLIED SCIENCE AND TECHNOLOGY RESEARCH INSTITUTE (ASTRI)

Interview with Dr. Frank Tong – Chief Executive Officer and Dr. Duncan Wong – Vice President, Financial Technologies of the government-funded Hong Kong Applied Science and Technology Research Institute (ASTRI)

July 4th, 2016 | Hong Kong

With the increasing sophisticated level and impact of cyber-attacks, the Hong Kong Monetary Authority (HKMA) has rolled out Cybersecurity Fortification Initiative (CFI) which consists of three pillars (i) Cyber Resilience Assessment Framework (ii) Professional Development Programme and (iii) Cyber Intelligence Sharing Platform. Dr. Frank Tong, CEO of ASTRI, and Dr. Duncan Wong, Vice President, Financial Technologies of ASTRI, shared their view on the current cybersecurity landscape, development, and what ASTRI can do to contribute to the HK industry.

Dr Frank Tong, CEO at ASTRI

Introduction of ASTRI

Sia Partners (S.P.): What is the key mission of ASTRI?

Frank Tong (F.T.): Our key mission is to enhance Hong Kong (HK)'s competitiveness in technology-based industries through applied research. In order to achieve this mission, we develop high quality R&D, transfer that into HK industries to help them develop. Since HK is a major financial hub in the world, FinTech development is crucial to enhance the strength of the financial services industry in HK.

Duncan Wong (D.W.): Under the FinTech initiative, we have four pillars: (i) cybersecurity, (ii) big data analytics which includes deep learning and artificial intelligence, (iii) blockchain, and (iv) mobile computing.

(S.P.): What is ASTRI's role in Cybersecurity research and development for Hong Kong?

(D.W.): Basically, you can consider ASTRI as the technology arm of HK. Cybersecurity is very important, not just for financial institutions but also for other industries. Being the biggest R&D centre for ICT (Information and communications technologies), ASTRI plays a role in the technology development and promotes the adoption of latest technologies in cybersecurity in order to nurture the industries and enhance the cybersecurity readiness for the entire society.

(F.T.): We are here to build necessary infrastructure such as the ASTRI Security Lab (ASL) for training and the security intelligence sharing platform for people in the industries.

ASTRI has around 500 people with strong expertise, we can do in depth R&D where the small companies are not eager or have no capability to conduct. We do not compete with SMEs. For example, we developed our solutions in open source and could license the solutions to other industry members so that they could utilize it for their customers.

(S.P.): In addition to Cybersecurity, what other key initiatives that ASTRI has taken on?

(D.W.): In addition to cybersecurity, ASTRI has taken on other FinTech initiatives such as blockchain big data analytics, deep learning, and artificial intelligence. All of these technologies are not just for the financial service industry, but also for intelligent manufacturing and other industries.

Especially for blockchain, we are actually investing a lot on this technology because we can see it has a promising future. Right now, blockchain development is still at a very early stage that puts us in the right position and timing to contribute by developing and educating the industry so that they know what the blockchain is.

(F.T.): Blockchain is identified as disruptive and impactful to the entire financial services industry. We have several teams working on blockchain in the past two years. We are working with the external parties, outside and inside HK, trying to bring up the awareness of HK and bring in the technology. We also commissioned to work on a white paper with a proof of concept on blockchain technology which will be ready by the end of this year.

In term of data analytics, we have built the engine together with Hewlett Packard Enterprise (HPE) and the solution is available on the market. The fact that big data analytics is so powerful, we are working on a project with the banking sector. Another area that has high demand is the manufacturing sector as they are particularly interested in predictive analysis.

For cloud based and mobile computing, we have been working on a program that can recognize Chinese characters. In addition, we are also working on facial, biometric and behavioral recognition technology. We also have a group working on algorithmic trading.

(S.P.): Given the increasing demand of Cybersecurity talents, how does ASTRI, which is a non-profit organization, retain or even expand its talent pool?

(F.T.): Increasing demand in cybersecurity talent is a big issue. There is a mismatch between what the students learn in the universities and what the market really demands. As a result, some graduates cannot find jobs and we cannot find the right people. Universities have just recently launched cybersecurity programs, but cybersecurity is a new topic and moving so fast, normally universities will need time to react. The shortage in cybersecurity talent is not just a HK problem, but also a global one.

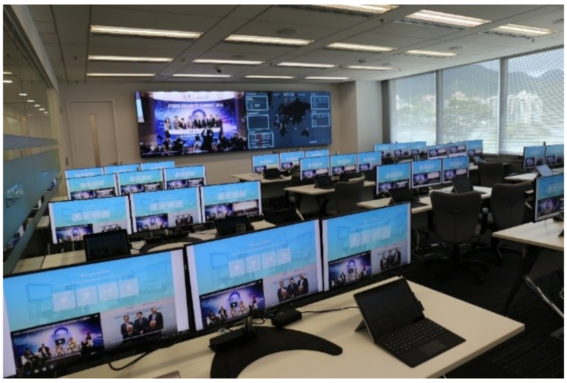
To cope with this issue, we should think about how to work with universities by creating a co-op program, where students can study the program at the university and at the same time work on ASTRI projects and get trained.

(D.W.): We have so many mega projects such as Cyber Range, this is how we can attract, train and further nurture talents locally. Besides that, we are hiring people internationally from Europe, Taiwan, and Ukraine etc.

Cyber Threats

(S.P.): What is the current global landscape on Cyber threat? Which Cyber threat worries you most?

(D.W.): The current global landscape of cybersecurity threat and defense is like an arms race. There are many new attacks. To be more responsive, you will need to have more defenses. At the same time you need to predict what kind of new attacks are forthcoming, and you need to pro-actively think of what kind of defenses need to be deployed before any real disaster happens.



ASTRI Security Lab

Out of the numerous cyber threats, one worries me most still is the Advanced Persistent Threat (APT); even though nowadays many people are talking about ransomware, but it is actually more seasonal instead of something new. Ransomware has been around for a decade, but now the attackers are finding it easier to collect the ransom through bitcoins.

The main problem to the industry is still APT as this kind of attack is more organized and the attackers have a well-planned attack methodology. The entire process may take from six months to almost a year and sometime even few years, to infiltrate the entire system. This could result in huge damage. Most of the APTs are undetectable.

(S.P.): What are the most effective ways to mitigate more and more sophisticated Cyber threat nowadays?

(D.W.): In terms of defense, you need to do it in a consolidated effort rather than in silos. In this regard, the intelligence is very important because you will be able to know in advance what kinds of APT or cyber-attacks may be launched by the attackers.

You also need to deploy defense systems such as firewalls, intrusion detection systems, or even data analytics. By using data analytics, you can identify system abnormalities by analyzing system logs and could have cybersecurity experts looking at the individual cases subsequently. It requires a whole sequence of efforts you need to do in order to make your system secured and get ready against a future attack, so it is not just reactive but also proactive.

(S.P.): What is ASTRI's view of the impact of Cyber threats on corporations and society in Hong Kong as well as worldwide?

(F.T.) As per the report coming from Hong Kong Police Force, increase in the financial loss due to the cybercrime is 15% per year. In term of financial loss in dollars, it is approximately HKD1.8billion. Meanwhile, physical crime has reduced to a relatively low level. Given that cybercrime has no borders, it makes defense even more difficult.

Even though there are cybercrime statistics from the Hong Kong Police Force, but the actual figures may be higher than what reported because some organizations have not reported cases due to reputation risk.

(S.P.): What do you think about the current maturity level of Cybersecurity risk management for banks, insurance companies, blue chip companies and government in Hong Kong? Are they doing well enough to combat the threats posted by Cyber-attacks?

(F.T.) HKMA has recently launched a Cybersecurity Fortification Initiative (CFI). It has three pillars and one of the pillars is the Cyber Resilience Assessment Framework (CRAF) which sets out the standard framework, so that consulting firms like SIA Partners can assess the banks' maturity level of cybersecurity risk management consistently. Right now, there is no standard to assess whether the bank is doing well or not in its cybersecurity risk management, so it is great that HKMA has launched this initiative and hopefully HK can move a step forward in this area.

Another pillar of CFI is the Cyber Intelligence Sharing Platform. The idea is we build this infrastructure for sharing information for the banking sector first and then for the entire financial services sector including securities, asset management and insurance. Ultimately, the goal is also for other industries to access the platform and benefit from it.

Cybersecurity Fortification Initiative

(S.P.): The HKMA launched the CFI at the Cyber Security Summit 2016 on in May and has issued a consultation paper on the Cyber Resilience Assessment Framework (CRAF) which is expected to receive the industry feedback by the end of Aug 2016. This could create additional challenges to banks in term of risk management and regulatory compliance. How do banks, especially small-to-mid sized banks that do not have abundant resources compared to larger banks, meet these challenges?

Dr Frank Tong and Dr Duncan Wong from ASTRI, Helina Lo from Sia Partners in the middle

(D.W.): We are developing the Cyber Intelligence Sharing Platform for the banking industry, there will be 157 banks on this platform. For small-to-mid sized banks, we will encourage them to go into the platform to learn about the latest cyber threat intelligence. They are going to benefit a lot from this first-hand information, so that the platform can enhance cybersecurity readiness for the entire industry. Of course, the bigger banks have more resources so they are going to contribute more in this platform. Ultimately, it is going to be the effort of the entire industry to contribute to this platform. The small-to-mid sized banks can seek support and work closely with the cybersecurity industry such as consulting firms or penetration testing companies. Overall, it is a process to start from the awareness, enhance the readiness, and finally get them more involved.

(S.P.): The HKMA is working with the ASTRI and the Hong Kong Institute of Bankers (HKIB) on the design structure of the Professional Development Programme, targeting to roll it out by the end of this year. What would you suggest the banks and professional firms do to prepare this programme?

(D.W.): Many of them have already been working with us closely including HKMA and HKIB, there are several regular sessions and we are having very active sessions with banks and other stakeholders. We believe the society is ready for setting the standards on the professional development for cybersecurity.

(F.T.): We are negotiating that the qualification issued from the HKIB will be mutually recognized by other countries. We have discussed with Singapore, some of South East Asia countries and United Kingdom etc. We believe that this is a very powerful qualification because once you are certified in HK, you can also be recognized all over the world.

ASTRI is only the technology arm of HK, we cannot fulfill the entire ecosystem. However, we will work together with HKMA, Hong Kong Association of Banks (HKAB), HKIB and also other industries and partners to establish HK as a better place for cybersecurity. This also helps industries better position themselves with China and rest of the world. Cybersecurity is indeed a mega project for HK at this moment.

Future Development in Cybersecurity

(S.P.): How well is Hong Kong doing in Cybersecurity compared with other major financial centres such as New York, London and Singapore? What Hong Kong should do to catch up global standard for Cybersecurity?

(D.W.): HKMA is a driving seed and encouraging the industry to set the standard for cybersecurity, but HK in general needs to do a lot more in cybersecurity especially from other sectors. Nowadays, not just New York City or London, if you look at Israel, they are also focusing a lot on cybersecurity, especially on utilities and critical infrastructure. Other countries are also trying to enhance the cybersecurity profile for airports, electricity and smart grids etc.

(F.T.): Cybersecurity is one of the cornerstones of FinTech. Recently, a professional firm has published a report to rank seven cities as potential FinTech hubs, HK was ranked as 7th, which is the lowest rank.

Compared with Singapore, there are many FinTech initiatives and consortiums. The Singapore government is very proactive. For example, "Global FinTech Hackcelerator" program is launched which has solicited 100 technology problem statements from the financial industry. They have the Agency for Science, Technology and Research (ASTAR) which is much bigger than ASTRI, even they have less population than HK. Singapore has spent a lot of effort to position itself as the APAC FinTech hub.

Those international financial centres such as New York, London, are all associated with the FinTech hub. In order to catch up as a FinTech hub, we need a coherent and holistic approach for R&D in HK. For education, we need to address the mismatch issue, develop relevant programs that are required by the industry. In addition, HK will need to continue to develop the local talents.

(S.P.): In the long term, what do you foresee the Cybersecurity development in Hong Kong? How can ASTRI contribute in the industry along the development?

(F.T.): At ASTRI, we have set FinTech as one of the most important initiatives and identified the areas we should work on. Within cybersecurity, we have a few initiatives. We launched the cybersecurity conference which was well received. Around 900 people attended the conference, and we had invited speakers from FBI, homeland security, Interpol and other experts over the world.

In addition to the conference, we have setup the ASL last May. ASTRI is working with the Hong Kong Police Force on the "CyberRange" program to simulate cyber-attacks where you will have two teams, one is in offensive and the other is in defensive to simulate and research cyber-crime cases. We are building the Cyber Intelligence Sharing Platform for CFI. We also provide training and necessary infrastructure to people in the industry. Furthermore, we have R&D programs for cybersecurity including encryption program, decryption program and processing in the cloud space.

At last, cybersecurity will extend beyond the financial sector. ASTRI continues to conduct R&D in cybersecurity, develop talents, increase awareness and work closely with the Government, regulators and industries in this aspect.

Find the full interview and more in our financial blog: http://en.finance.sia-partners.com