APRIL 15, 2019

CYBERSECURITY ADVANCEMENT PROGRAMME FOR BANKING INDUSTRY IN HONG KONG

FINAL REPORT

THE HONG KONG INSTITUTE OF BANKERS

TABLE OF CONTENTS

1 Introduction

In May 2016, Hong Kong Monetary Authority (HKMA) rolled out the Cybersecurity Fortification Initiative (CFI) in collaboration with the banking industry in Hong Kong. The CFI has taken reference from the CBEST, which is an intelligence-led testing framework in the Bank of England (BoE). The main objective of CFI is to enhance cybersecurity risk management and cyber resilience of the banking sector in Hong Kong.

To keep up with the trends of cybersecurity, the "training and certification" part of the HKMA CFI programme is designed and benchmarked against Council of Registered Ethnical Security Testers (CREST), an international cybersecurity standard initiated by the CREST organisation in the UK. It complements the deficiency of traditional defence mechanism in the increasing number of threats posed by cyber criminals and the attacks from organised cyber activities. CREST provides internationally recognised accreditation for individuals, including penetration testing, cyber incident response and threat intelligence services, which are all essential elements for the cyber resilience of the banks. To improve the cyber resilience level of the local banks, and to fulfil the CFI requirements, CREST qualification is an indispensable factor. The popularisation of CREST could definitely increase the supply of qualified professionals in cybersecurity, which is a crucial factor affecting the success or otherwise of the CFI. However, the industry has raised a practical issue concerning the availability of qualified cybersecurity practitioners to fulfil this requirement. This reveals a strong need for more in-depth understanding of the CREST qualifications, CBEST framework, and the latest cybersecurity technological developments.

In view of this, Hong Kong Institute of Bankers (HKIB) had submitted an application to The Commerce and Economic Development Bureau (CEDB) to apply the Professional Services Advancement Support Scheme (PASS) for the programme: "Cybersecurity Competence Advancement Programme for Banking Industry in Hong Kong". For this programme, a conference, "The Latest Technology Trends of Cybersecurity in Banking Industry Conference", was held on 25 January 2019 at HKIB, to offer an overview of the CREST qualifications and CBEST framework adopted in the UK. Overseas professionals were invited as keynote speakers. The conference provided a platform for the exchange of knowledge between the international and local experts in

their respective fields. The overseas speakers could bring an international insight, enhancing global collaboration and Hong Kong's readiness in cybersecurity. In particular, CREST experts were also invited from the UK for promoting CREST qualifications, which benefited the rollout of CFI. Furthermore, a questionnaire was issued to the participants of the conference, and interviews were conducted with selected participants to collect feedback on their insights of the new cybersecurity framework.

Taking into account of the programme final output, this final project report is formulated and compiled to be shared within the information and communications technology services professionals in the local banking industry to facilitate their understanding of the CREST and CBEST framework, and improve their cybersecurity knowledge.

2 Objectives

The objectives of the Cybersecurity Competence Advancement Programme for Banking Industry in Hong Kong are as follows:

- **Boosting Hong Kong as one of the most advanced global financial centres in the cybersecurity context**

  The implementation of CREST can ensure the stability and excellence of service delivery. The execution of CREST standards in Hong Kong help strengthen the bond between the local and the overseas financial sectors, increasing the exchanges and co-operation of Hong Kong professional services. Through the promotion and the popularisation of CREST standards, Hong Kong practitioners of cybersecurity can deepen their industry knowledge and hence improve their skills.

- **Ensure the effective cybersecurity risk management of the banks**

  With an increase in the awareness of the cyber defence, the cybersecurity level of Hong Kong region can then be improved.

- **Enhance the cybersecurity professional knowledge of Hong Kong's cybersecurity practitioners in the banking industry**

  With the implementation of CREST standards, there would be a continuous supply of certified practitioners through educating and nourishing more future talents in the long run. This would potentially form a sustainable cycle of practitioners being capable of handling more complicated cases and hence training more practitioners. Although CFI is specifically designed for the financial sector, CREST standards can be applied to other industries once the standards gained recognition from the practitioners of other industries.

3 Highlights of the Conference

3.1 Conference Overview

The Latest Technology Trends of Cybersecurity in Banking Industry Conference was a successful launch in gathering decision-makers and industry experts from the financial sector to delve into the latest issues and trends in cybersecurity. Especially for this "Cybersecurity Competence Advancement Programme for Banking Industry in Hong Kong" programme, overseas professionals were invited as speakers at this 1-day conference held on 25 January 2019. This event had provided an opportunity for exchange of knowledge between international and local experts in their respective fields, and hence had attracted over 200 participants. The invited speakers had shared international insights, enhancing global collaboration and Hong Kong's readiness in cybersecurity. In particular, CREST experts were invited from the UK for promoting CREST qualifications, which is beneficial for the rollout of CFI.

3.2 Guest Speakers from IT Cybersecurity Fields

Ms Carrie Leung, the Chief Executive Officer from The Hong Kong Institute of Bankers, delivered the welcoming remarks for the commencement of the conference.

Mr Ian Glover, the President of CREST, was invited from the UK to share the history and role of his organization. In his speech, he introduced the benefits of CREST, cybersecurity professional development, schemes and regions, levels of assurance, etc. He encouraged Hong Kong to move to the next level of creating a wider ecosystem for establishing CREST standards and to have greater collaboration in areas such as the assurance of national infrastructure. His sharing has brought international insights to the local technical information security industry.

Mr Don Randall Mbe, Chief Executive of Don Randall Associates Limited, had talked about the reasons for and the purpose of creating CBEST. In his presentation, he showed the audience the

difference between CBEST and standard penetration testing. His presentation on how Chief Information Security Officer integrates his/her role with Chief Information Officer and Chief Security Officer's had captured many's attention.

Mr Rex Liu, the Director of Security Management of Joint Electronic Teller Services Limited, delivered a session on "Open Banking: The new frontier and challenges in cybersecurity". He first introduced Opening Banking with its objectives and key drivers, then the global and local development of this financial technology. This technological advancement comes with the difficulties of regulations, fraud detection and working with different parties. He provided the solution of APIX with the example of JETCO, which stirred up further discussions and provoked abundant innovative ideas.

Mr Wilson Pang, Senior Manager of HKMA's Fintech Facilitation Office, gave an overview on current landscape of CFI. As Hong Kong's financial regulator, HKMA had shared the importance of cybersecurity in Smart Banking, as well as thefuture roadmap of CFI.

On behalf of Professional Information Security Association, Mr Frank Chow illustrated cybersecurity trends in the financial sector for this year. After reviewing previous cyber incidents such as data breaches and online theft, he highlighted that cyber-attacks could become more sophisticated and so, more synergistic threats could be expected in the future. He also made numerous suggestions for improving cybersecurity. As said, the best practices are to take preclusions and to have rescue plans.

Mr Oliver Church is the Chief Executive Officer of a cyber threat intelligence company Orpheus. As specialist of cyebr threat intelligence, he introduced how and why regulators are around the world expecting organisations to use cyber threat intelligence. From which, he brought up the importance and the effectiveness of such.

During Panel Discussion, Mr Don Randall, Ms Irene Coyle and Mr Oliver Church reviewed the matters on cybersecurity from different aspects, including its future vision, preventatives,

remediation methods, etc. Felix Kan, who is an executive committee member of Hong Kong Computer Society Cybersecurity Specialist Group, acted as the moderator of the panel discussion.

Ms Irene Coyle, the Chief Executive Officer of Orpheus Cyber, shared the importance of cyber threat intelligence for cybersecurity. With the help of intelligence, risks can become predicted and can be avoided in different levels.

Mr Bernard Kan, Senior Consultant of Hong Kong Computer Emergency Response Team Coordination Centre, adjourned the conference day. He spoke on the topic "Cybersecurity Incident Handling for Financial Sector", with incorporated examples of cybersecurity incidents in Hong Kong hence emphasising the importance of detecting and analysing the incidents. He had also mentioned about the regulatory requirements in the context of Hong Kong from a practical point of view of handling cybersecurity issues.

4 Overview of CFI & Crest Qualifications

4.1 What is CFI?

CFI is an initiative co-organised by HKMA and The Hong Kong Institute of Bankers (HKIB). CFI consists of three pillars, namely (i) the Cyber Resilience Assessment Framework (C-RAF); (ii) the Professional Development Programme (PDP); and (iii) the Cyber Intelligence Sharing Platform (CISP).

4.2 What is CREST?

CREST is a non-profit-making organisation that represents the technical information security industry. There are more than 40 CREST Member companies and over 500 CREST qualified individuals providing technical information security services in the UK. While CREST is mainly based in the UK, it has overseas branches. Financial sectors from the UK have benefited from CREST because of market transaction services provided by a specialist professional body. CREST also supports the development and information sharing of the industry by providing in-depth guidance material and commissioning detailed research projects which are provided to the industry for free.

CREST has provided the practitioners of the information security markets with

- **Company Membership**: A demonstrable level of assurance of processes and procedures of member organisations
- **Professional qualifications:** The validation of the knowledge, skills and competence of information security professionals
- **Knowledge sharing:** The production of guidance and standards; The opportunities to share and enhance knowledge
- **Professional development:** The provision of on-going personal development

CREST provides quality penetration testing services with confidence as work will be carried out by qualified individuals with up to date knowledge, skills and competence against the latest techniques used by real attackers. All examinations for individual assessments have been reviewed and approved by The Government Communications Headquarters (GCHQ) and CESC. Additionally, the penetration testers are supported with appropriate policies processes and procedures for conducting this type of work and for the protection of client information, alongside with enforceable codes of conduct. These codes are to ensure the quality of the services provided, the integrity of the companies and individuals as well as adherence to audited policies, processes and procedures; hence offering a significant level of protection for any organisation under CREST.

For those organisations that have experienced a cyber-security related incident, or are aiming to reduce the likelihood or severity of a cyber-attack, CREST has introduced The CREST Cyber Security Incident Response scheme, offering company assessment with the support of professional qualifications endorsed by GCHQ and Centre for the Protection of National Infrastructure (CPNI). The scheme focuses on standards for incident response which is aligned to demands from all sectors of industry, the wider public sector and the academia. Companies which have undergone this scheme have demonstrated their effective policies, processes and procedures in place to help organisations plan for, manage and recover from significant cybersecurity-related incidents. In addition, professionally qualified staff in intrusion analysis and reverse engineering would be offered to aid these companies.

5 Survey Results

5.1 Questionnaire

HKIB invited 250 participants attending the 1-day conference on 25 January 2019, 200 confirmed participants attended on the date. Here are the breakdown by business sectors and by job natures of those participants:

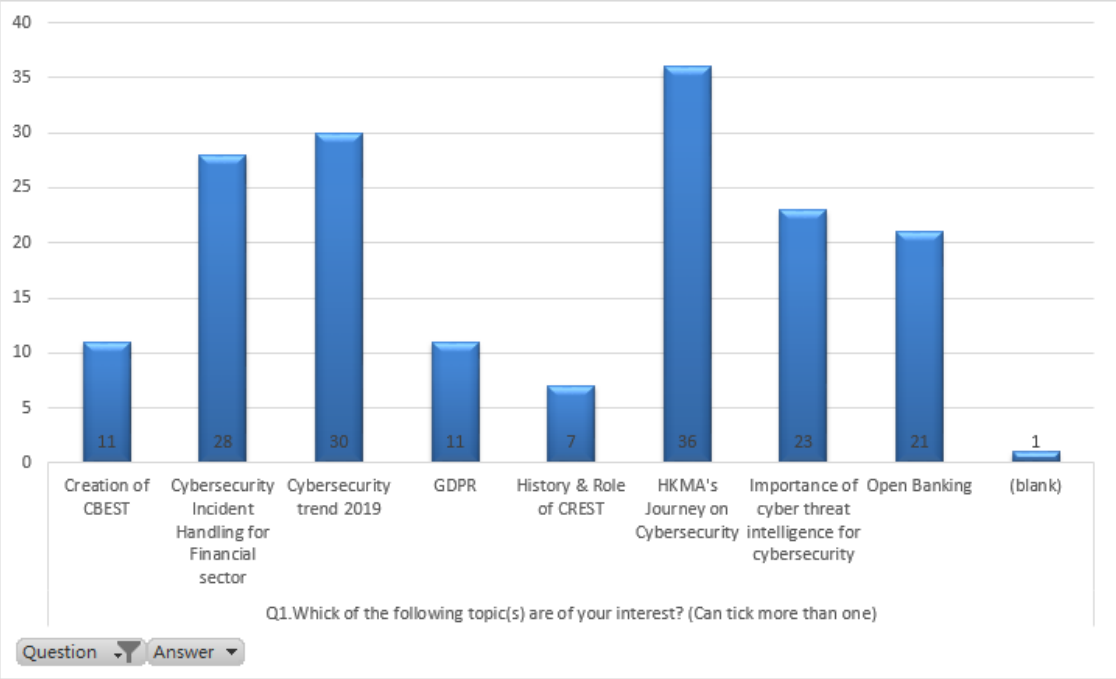
By Busines Sector	No. of people
Banking	143
Other Financial Institutions	15
IT Company and Association	30
Education Institutions	4
Regulators or Government Council	6
Others	2
Total	200

By Job Natures	No. of people
Risk Management	61
Audit	48
IT	44
Legal and Compliance	21
Management	11
Front Office	11
Others	4
Total	200

We collected back 50 questionnaires after the conference; the analysis of the survey results are as following sub-sections:

5.1.1 Conference Topics

Respondents tend to be more interested in the conference topics on related to cybersecurity and experience sharing, including "HKMA's Journey on Cybersecurity", "Cybersecurity Incident Handling for Financial sector", and "Cybersecurity trend 2019". As shown, "HKMA's Journey on Cybersecurity" was chosen as their favourable topic with 36 votes. (See the graph below.)



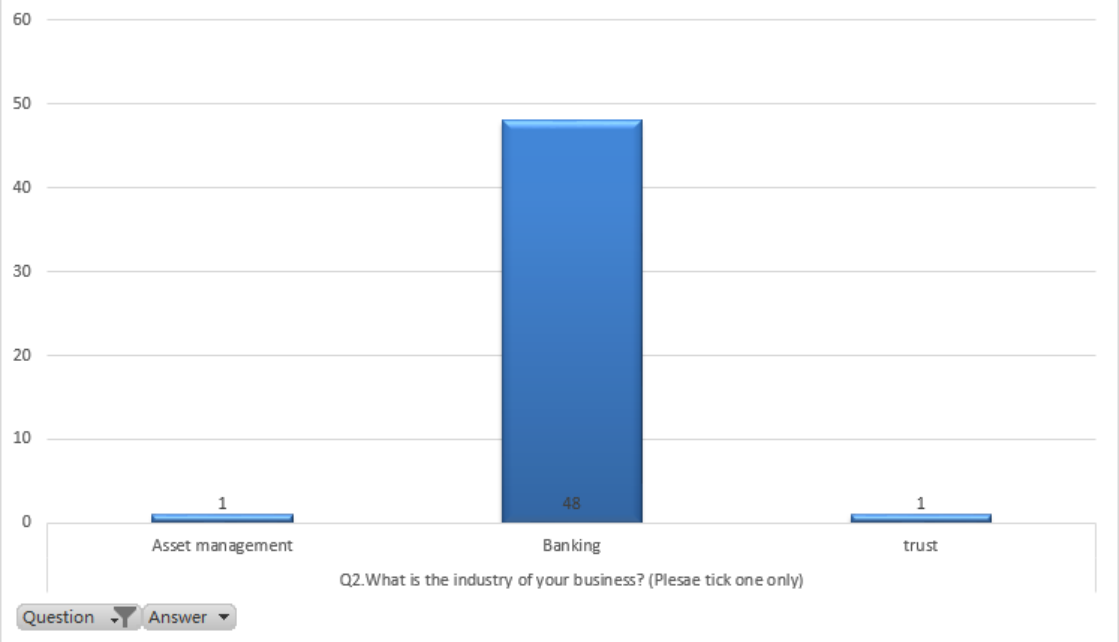
In terms of "Venue & Logistic arrangements", Most of the respondents has good feedback on the conference arrangement aspects by HKIB. A total of 16 respondents (32%) rated 8 out of 10. More than 35 respondents (70%) have given a score higher than or equal to 5.

Most respondents responded positively in "Speakers and Content" with an overall score higher than a score of 5. The session delivery was shown to match the delegates expectation, with 33 respondents (66%) gave a score of 8 of above, while the remaining 17 respondents (34%) rated lower than 8.

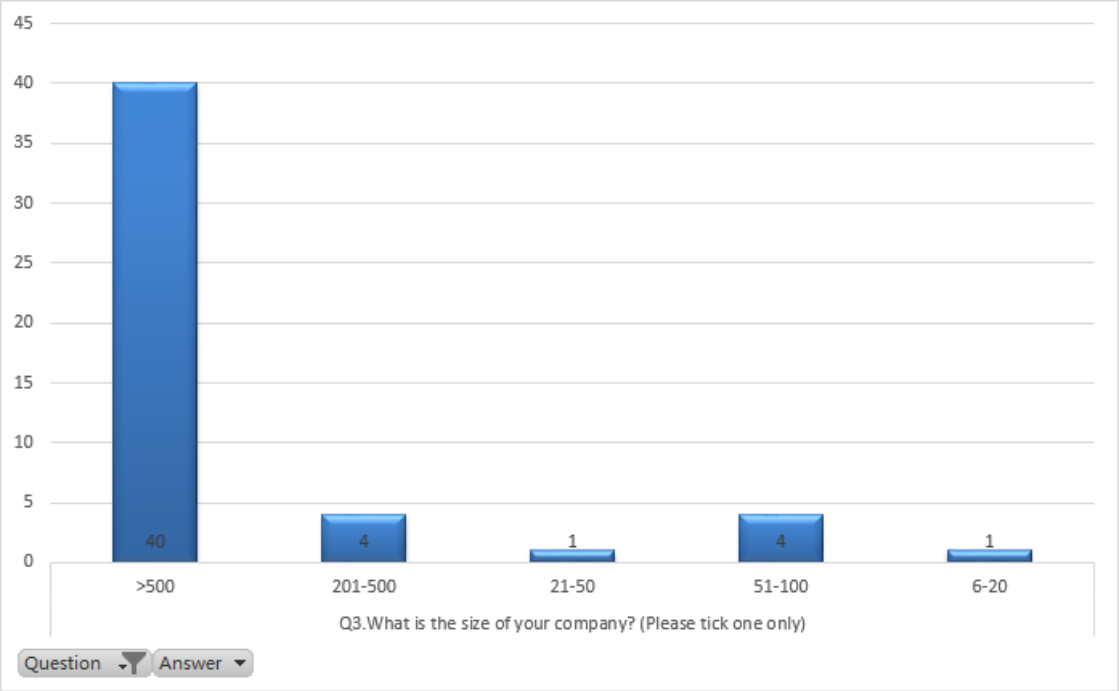
Overall speaking, likely most (98% of the respondents) rated higher than a score of 5 for the general performance of the conference. 30 respondents (60%) gave a score high than or equal to 8, whereas 20 of them gave a score lower than 8.

5.1.2 Attendees Demographics

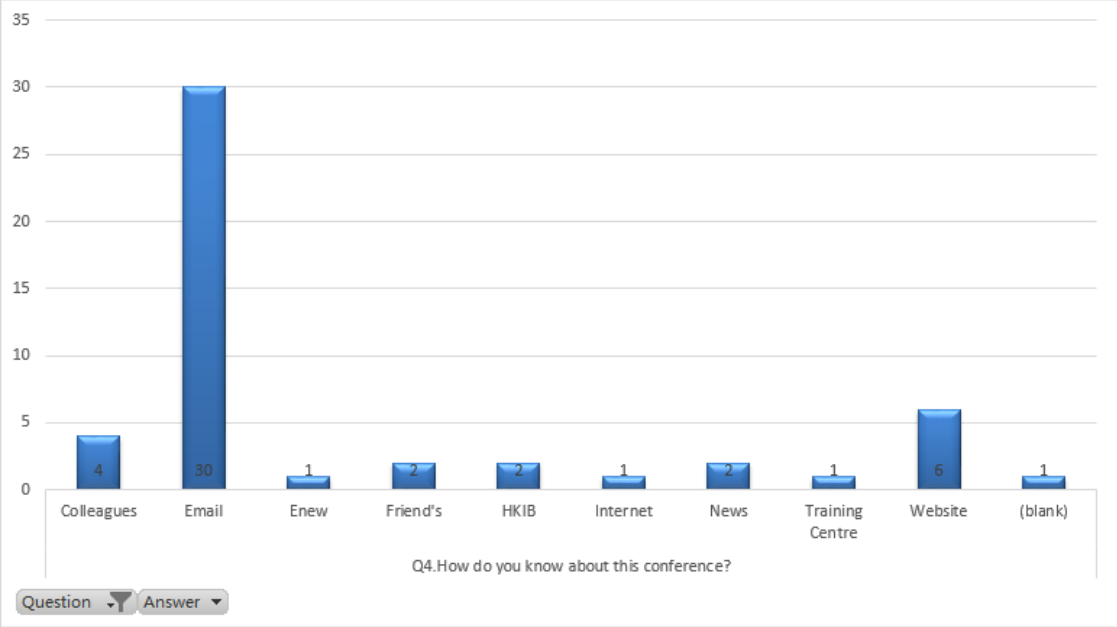
A majority of respondents are from the banking industry; with 48 out of 50 respondents (96%) indicated that they serve within the banking industry in Question 2 of the survey. (See the graph below.)



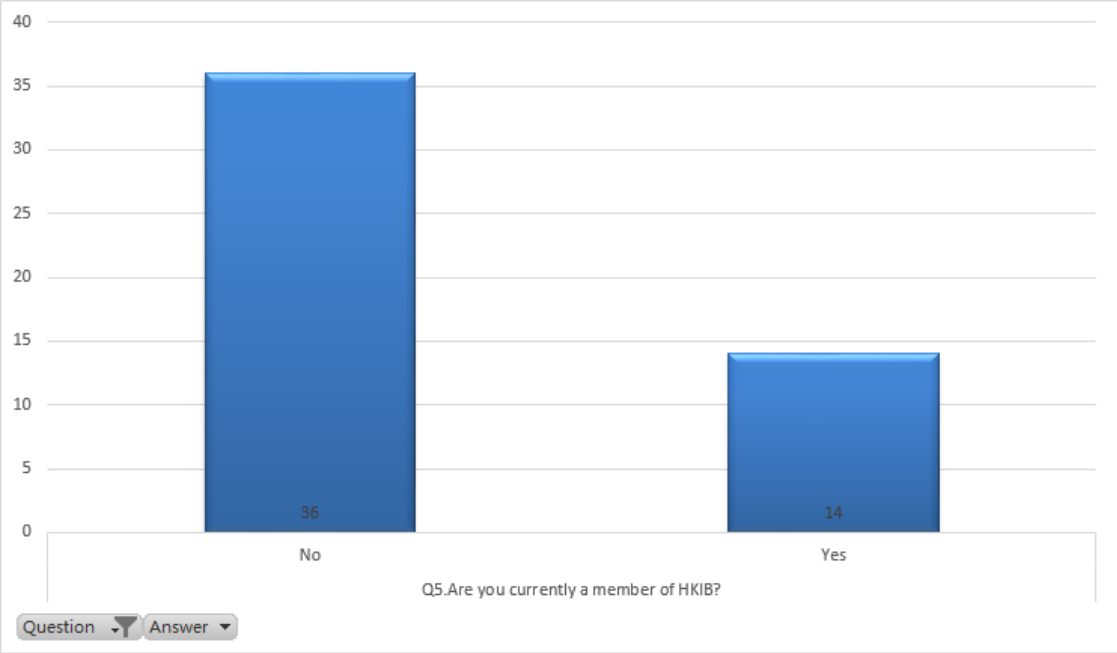
Most of the respondents are from large-scale financial institutions. In Question 3, the respondents were being asked to indicate the scale of the company they work for. It is found that 40 respondents (80%) work at financial institutions with over 500 employees.



As most of the respondents were notified of this event by email, there is a great tendency on the utilization of internet communication and information flow. Most of the respondents, 30 of them (60%), were learned about the conference via “Email”, with 6 respondents (12%) via “Website” and 6 respondents (12%) via “Colleagues” and “Friends”. While the importance of Word of Mouth shall not be neglected as part of the respondents were informed about the conference by personal network. (See the graph below.). However, 72% respondents were non-members of HKIB, only 14 respondents (28%) are HKIB Members.

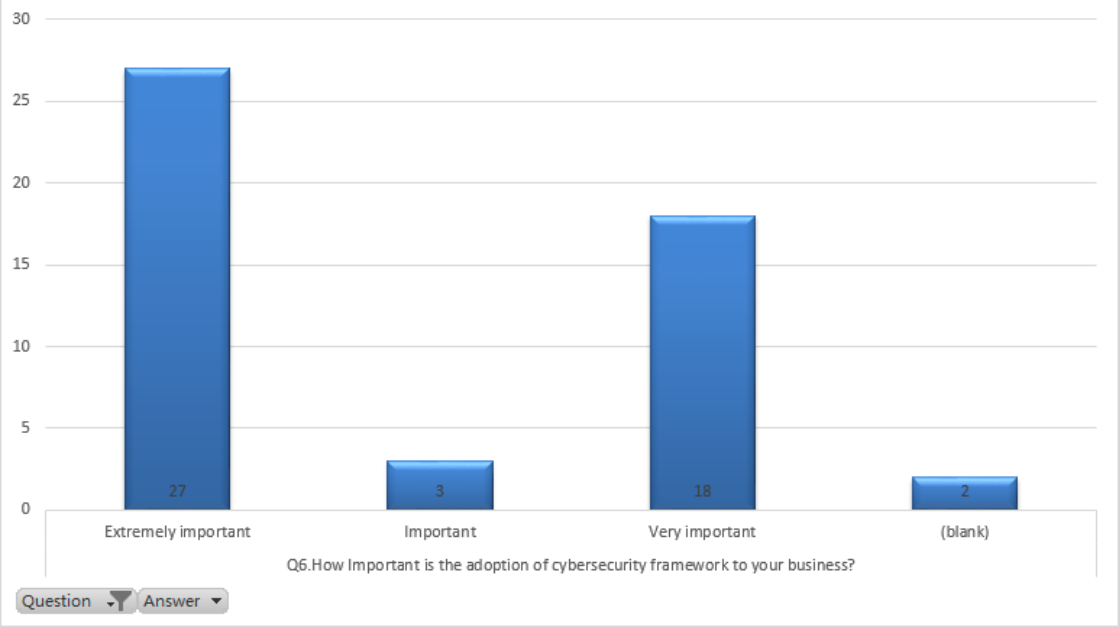


Expanding the HKIB membership database and stronger event promotion within the HKIB membership would be recommended. For this event, only 14 respondents (28%) are HKIB members, which the participation rate of these members is not high enough. HKIB should encourage its members to take part in similar events in the future. Their participation would not only brought them new industrial insights, but also help them connect with other professionals. (See the graph below.)

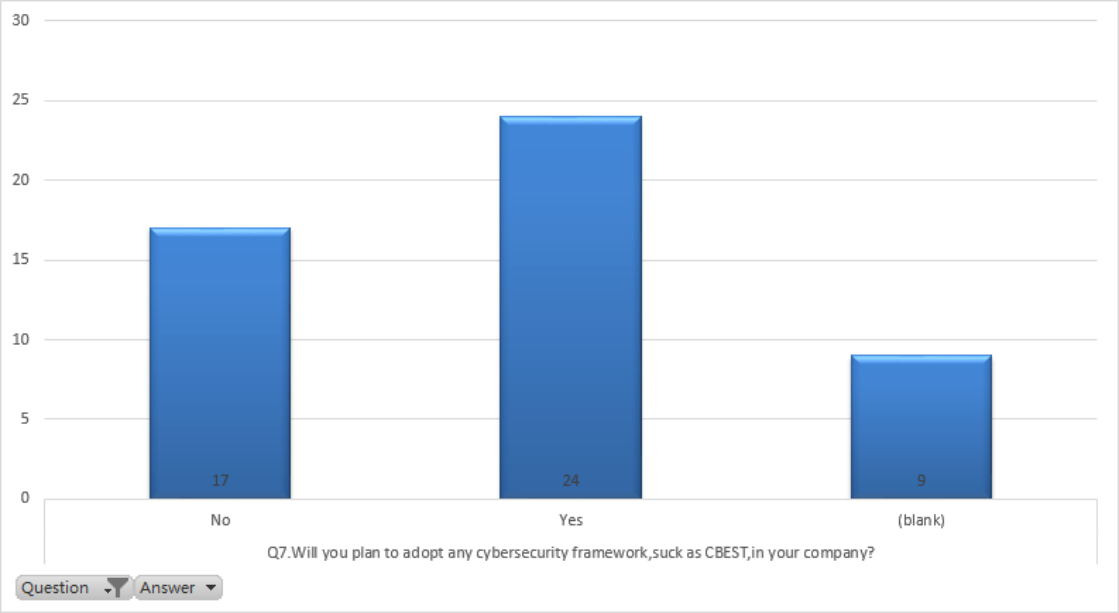


5.1.3 Cybersecurity in the Company

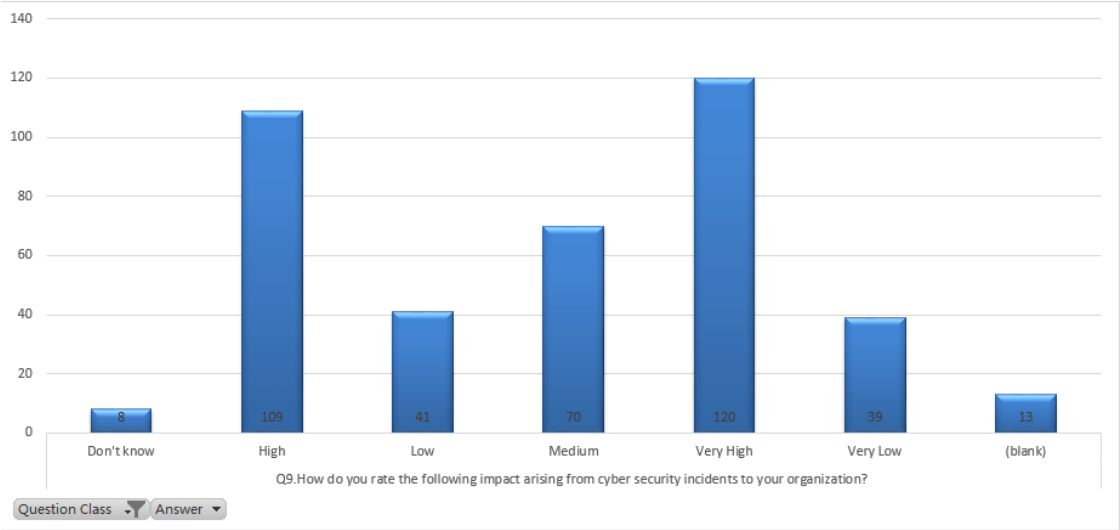
The importance of cybersecurity framework to the financial industries is highly recognized. Likely most respondents indicated their preference as "Important", "Very important", and "Extremely important", 48 out of 50 respondents. (See the graph below.)



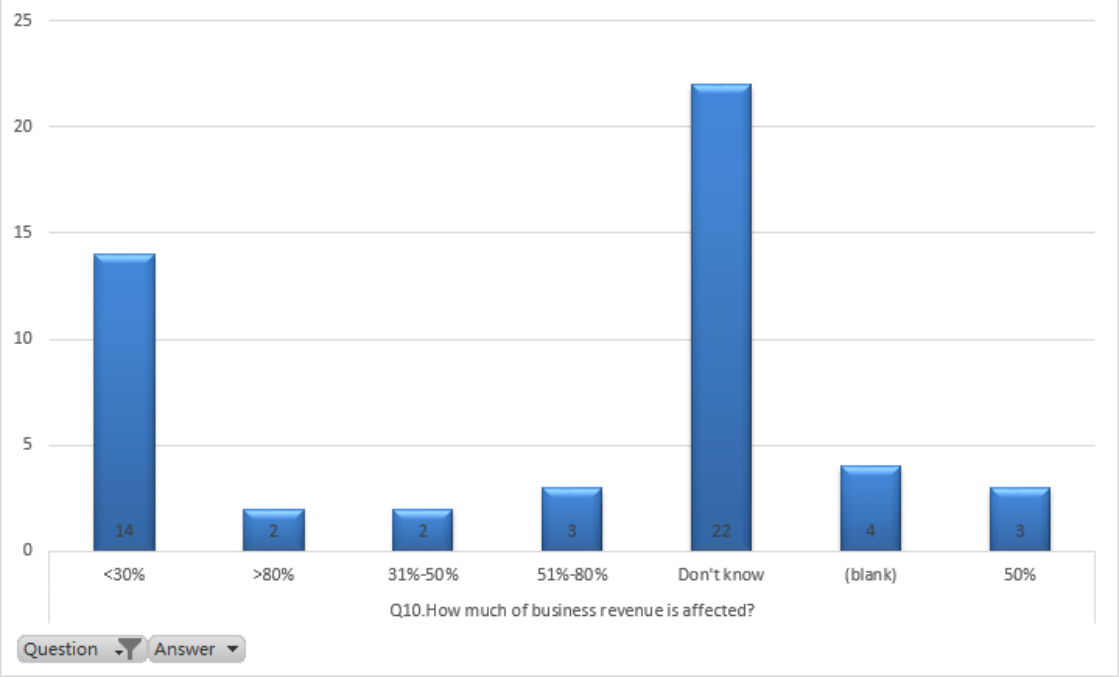
After the conference, in Question 7, only 24 respondents (48%) considered adopting cybersecurity framework such as CBEST. Further researches could be conducted to understand the underlying reason for not adopting the framework or choosing CBEST as their option. There could also be chances that the respondents did not comprehensively understand CBEST framework and more promotions may facilitate their further understanding. (See the graph below.)



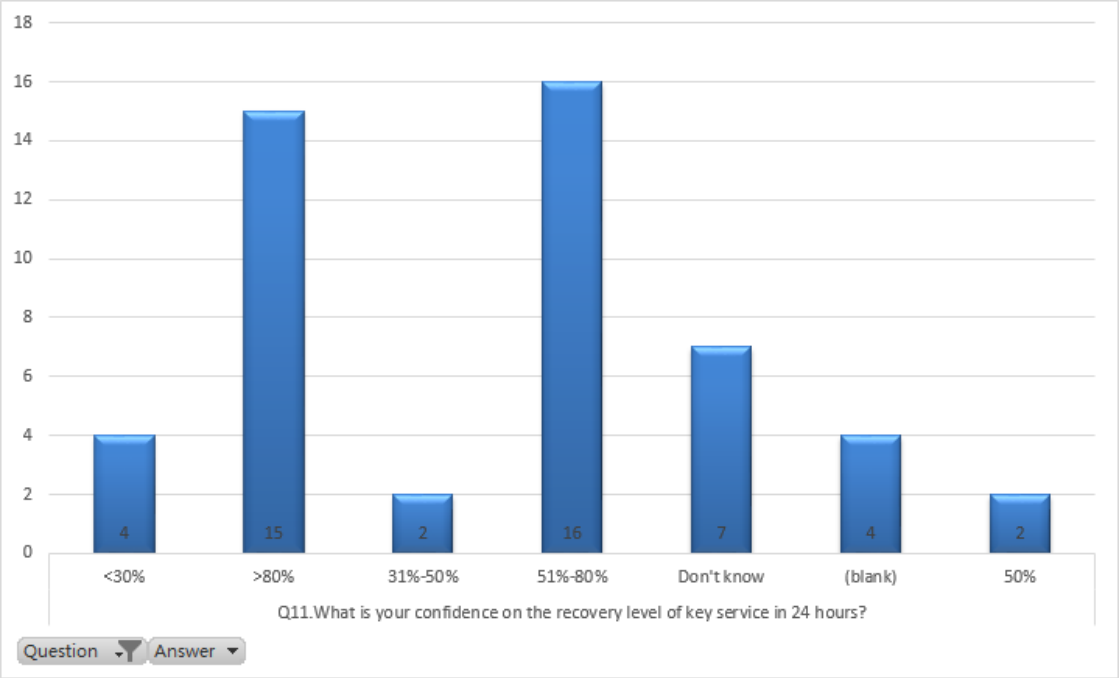
In Question 9, the respondents indicated the impact that security issues had on their organisations in eight areas, including (a) service termination, (b) the leak of information, (c) damages to intellectual property, (d) damages to the system and data, (e) reputational damage, (f) economic loss, (g) physical damage or personal injuries, and (h) the legal obligations for any liabilities. The options "High" and "Very High" has a total of 229 counts, which comprises 57% of all. (e), (a), and (b) are the areas that have the greatest number of counts in the option "Very High" with a sum of 59 counts. For the option "High", the 49 counts are added up by (d), (a), and (h). (See the graph below.)



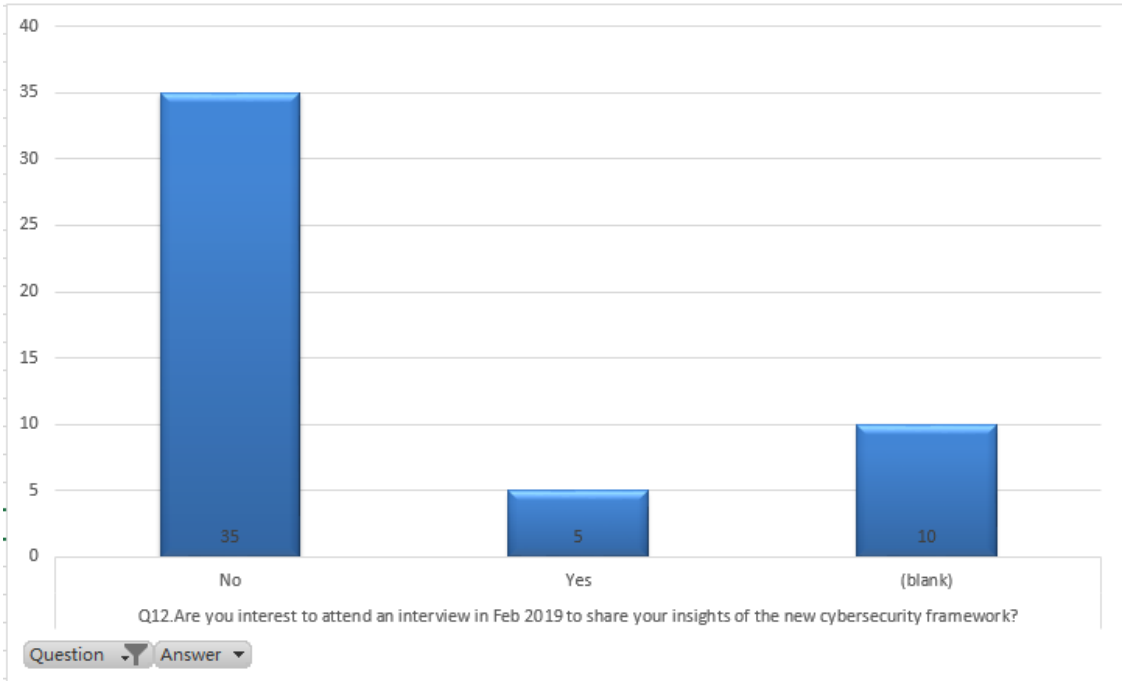
Question 10 is related to the financial impacts that cyber-attacks have on business. 22 respondents (44%) stated that they could not estimate the lost revenue after the attacks, while 14 respondents (28%) believed that less than 30% of business income would be affected. For the reason that the cyber network is crucial for the company's operations, the improvements on cybersecurity demand immediate attention. (See the graph below.)



Respondents generally have confidence in restoring the company key services in 24 hours after a cyber-attack. A total of 31 respondents (62%) chosen the options of "51%-80%" and ">80%". (See the graph below.)



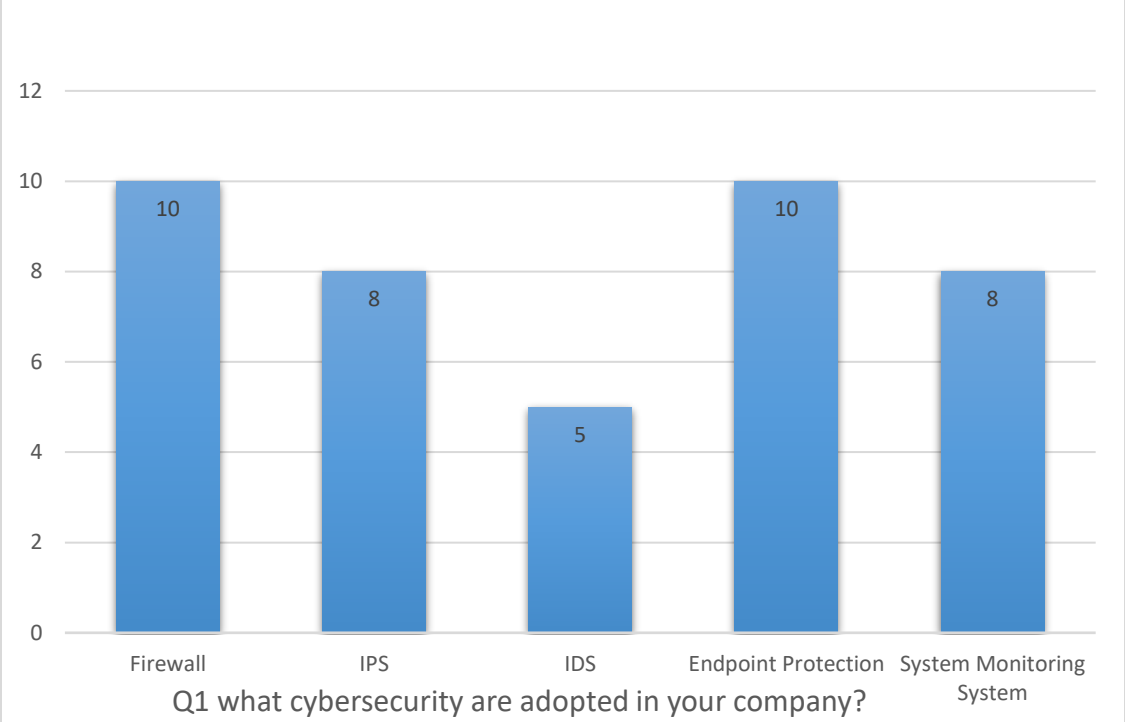
Lastly, respondents were being asked whether they will like to be interviewed about their opinions on the new cybersecurity framework in February 2019. 35 respondents (70%) indicated that they are not willing to participate in the interview potentially due to time constraints, which is not as desirable for improving cybersecurity. Only when there are enough cases and user experience for investigation could the cybersecurity be improved. (See the graph below.)



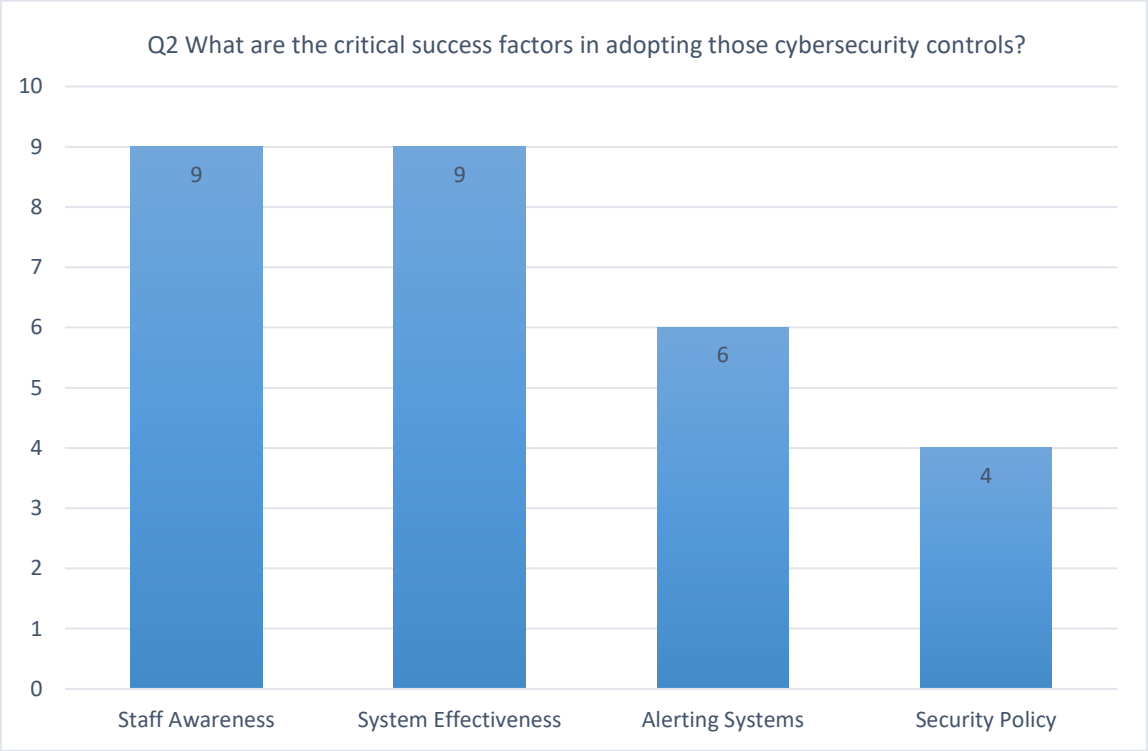
5.2 Interview

In Feb 2019, HKIB has interviewed 10 participants attending the conference on 25 January 2019, who expressed interest in sharing their insights of the new cybersecurity framework. Below are the analysis of the interview results:

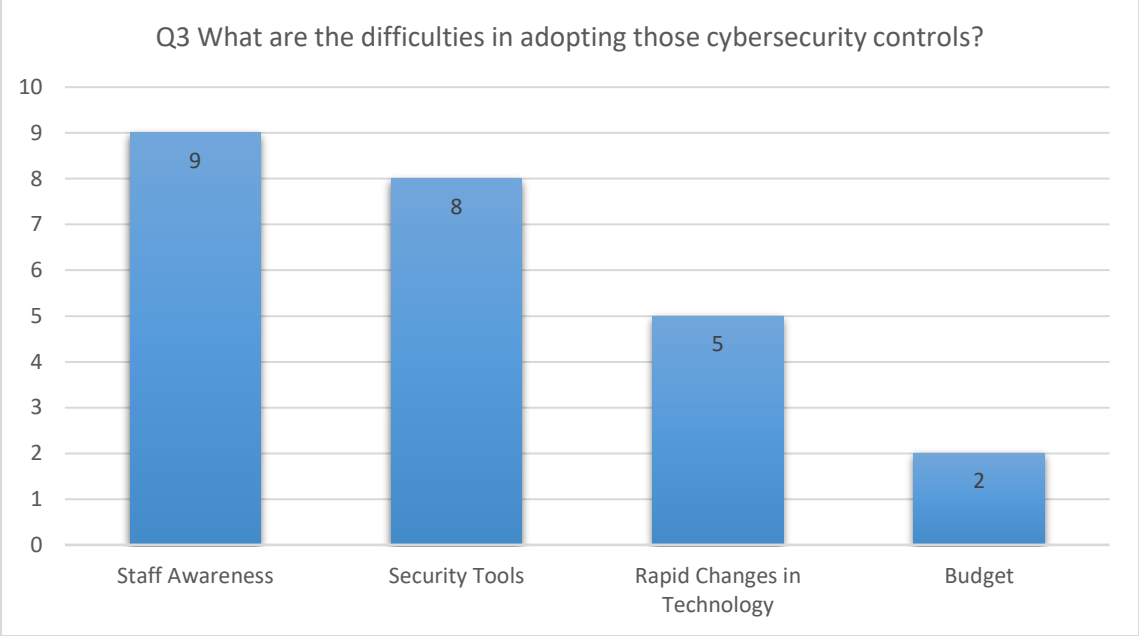
Question 1 is about the participant's company background and what cybersecurity controls (such as Firewall, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), etc.) are adopted in the company. All companies have adopted Firewall and Endpoint Protection, and most of them have adopted IPS, IDS and System Monitoring System (See the graph below.)



Question 2 is about the critical success factors in adopting those cybersecurity controls. Most of them believed that raising staff awareness of the new cybersecurity framework and having effective tools for cybersecurity are the most critical success factors. Some of them believed that alerting tools for security incidents are also important. (See the graph below.)



Question 3 is about the difficulties in adopting those cybersecurity controls. Most of them believed that raising staff awareness of cybersecurity controls and being familiar with various kinds of security tools are difficult to implement. (See the graph below.)



Question 4 is about if there is any plan to adopt cybersecurity framework in their companies. 70% of interviewees (7 of them) have already adopted cybersecurity framework and the rest of them are planning to do so in this year.

6 Conclusion

The 1-day conference of "Cybersecurity Competence Advancement Programme for Banking Industry in Hong Kong" programme was a huge success, attracting more than 200 specialists from the financial sector.

Through the event, HKIB promoted CREST to local practitioners of the financial sector. Not only will the implementation of CREST in Hong Kong equip local professionals with qualifications and skillsets, but also prevent banking institutions from potential threats. In the long run, CREST is definitely the essence of the assurance of service quality and for maintaining Hong Kong's status as an international financial centre.

Honoured speakers had introduced the CREST framework, the trends of cybersecurity, future challenges and possible improvements. Special thanks to the overseas speakers for the intellectual exchange and their support to this event. Their insightful sharing had enriched the participants' industry knowledge and had given them the latest market updates.

The survey results provided meaningful insights on how to better promote the new cybersecurity framework and what HKIB has to improve in organising activities in the future.

To conclude, this Programme had raised the awareness of the public the significance of cybersecurity controls as well as the importance of implementing CREST. While HKMA has initiated CFI for improving cybersecurity level, public recognition is also a critical factor for the accomplishing the visions.