GovCERT.HK

Annual Report 2018

1. Highlights of 2018

1.1 Summary of Major Activities

To enhance the city's overall defensive capability and resilience against cyber attacks, we officially launched a Partnership Programme for Cyber Security Information Sharing named "Cybersec Infohub" and the first cross-sector cyber security information sharing and collaborative platform (Cybersechub.hk) in September 2018. Since then, we have organised numbers of seminars and workshops to promote trusted partnership of local cyber security stakeholders across prominent sectors for sharing cyber security information and providing actionable insights to the community.

Within the Government of the Hong Kong Special Administrative Region (HKSAR Government), we continued to co-organise with the Hong Kong Police Force (HKPF) to run the annual inter-departmental cyber security drill for government departments. The drill of this year not only walked through the procedures of incident response, but also provided a hands-on workshop simulating a cyber attack scenario for participants to get familiar with hands-on investigation and analysis techniques.

A keen appreciation of the threat landscape could help organisations and individuals to understand better the cyber threat environment so as to adopt early and appropriate mitigation measures. In 2018, we continued publishing threat trends, security alerts and mitigation advice through the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) web portal for reference by the general public. We further tailored specific threat awareness updates for government departments.

We are also committed to promoting information security awareness to various sectors of the community by collaborating with different organisations to regularly hold various cyber security publicity events to raise public awareness and capability development.

1.2 Achievements and Milestones

Cyber Security Information Sharing

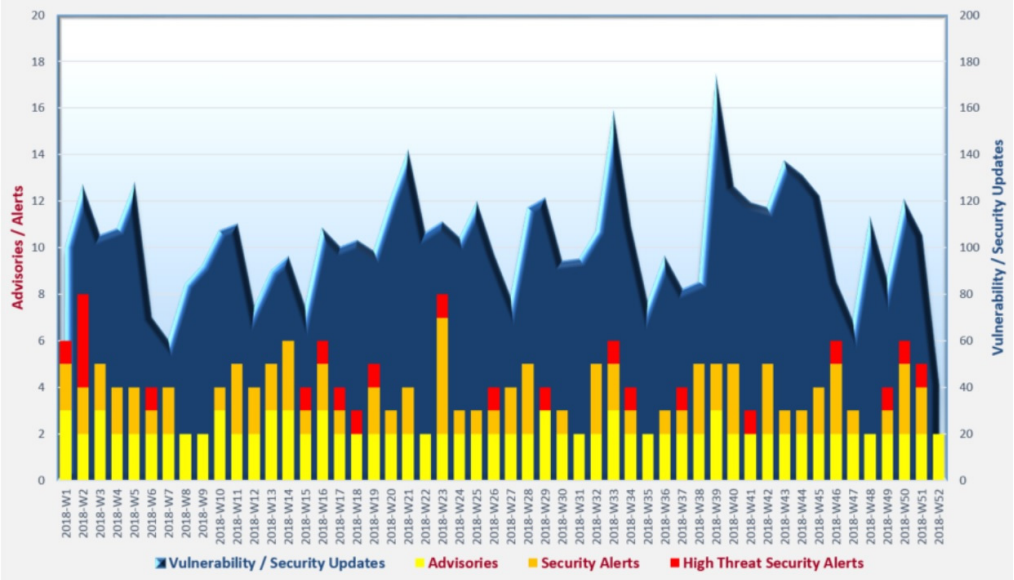
With the objective to facilitate cross-sector collaboration for a better visibility of cyber threats globally and locally, Cybersec Infohub serves well as an enabler to nurture culture in sharing cyber security information.

We are grateful to see active participation since the launch of Cybersec Infohub. As of 2018, over 100 organisations with more than 300 representatives across various sectors have joined the Programme. Many of them have taken the lead to share information on the platform. The Programme has become an essential reference for oganisations in gathering security intelligence and meeting with peers to share experiences and successes.

Cyber Threat Intelligence Management

GovCERT.HK has been monitoring cyber security threat trends and sharing relevant information with our constituents and the community for taking early precautions and together reinforcing Hong Kong's cyber security. We publish monthly Cyber Security Threat Trends Report via the GovCERT.HK web portal to highlight the observations of latest cyber security threat landscape for reference by the public to enhance their situational awareness.

Cyber Security Threat Landscape



Liaison and Collaboration

We proactively participate in the Asia Pacific Computer Emergency Response Team's (APCERT) activities and work closely with the Computer Emergency Response Team (CERT) community in handling threat information. In 2018, we delivered a presentation at the APCERT Annual General Meeting and Conference to promote partnership and collaboration in cyber security information sharing.

Capability Development

To facilitate the HKSAR Government in developing staff capabilities to tackle evolving cyber threats, we established the GovCERT.HK Technology Centre in 2018. The centre offers government departments a controlled environment with relevant facilities and equipment to enable vulnerability scanning and security testing for potential security issues of their web applications.

Awareness Building and Public Education

User awareness of information security plays a vital role in coping with cyber threats. In view of the rising trend of phishing attacks, GovCERT.HK created a series of promotional materials including educational videos and smart tips for the public to protect themselves from and defend against phishing attacks.

GovCERT.HK also devotes much attention to public education and capacity building in different business sectors and age groups. In 2018, we organised 36 school visits to reach out to some 10 000 students, parents and teachers.

2. About GovCERT.HK

2.1 Introduction

GovCERT.HK is a governmental CERT responsible for coordinating incident response for over 80 departmental Information Security Incident Response Teams of the HKSAR Government.

Since its establishment, GovCERT.HK has profoundly shaped the management framework and coordination mechanism of incident handling; and empowered close collaboration with the industry, critical Internet infrastructures, and the CERT community for timely exchange of cyber threat information and coordinated responses. GovCERT.HK also works closely with Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and local industry on cyber threat intelligence sharing, capability development, public education, and continuous promotion on cyber security and resilience through social and mass media.

GovCERT.HK also collaborates with the CERT community globally in sharing threat intelligence and incident information; participating in training events, workshops, forums and drills; and organising public awareness promotion activities and capability development initiatives.

2.2 Establishment

GovCERT.HK was established on 1 April 2015 through the consolidation of internal IT security teams within the Office of the Government Chief Information Officer (OGCIO) of the HKSAR Government.

2.3 Resources

GovCERT.HK is an establishment under OGCIO and funded by the HKSAR Government.

2.4 Mission and Constituency

Being the governmental CERT, GovCERT.HK will centrally manage incident responses within the HKSAR Government and develop CERT-related services to assist government departments in understanding the associated risks of information and cyber security, implementing appropriate security measures, monitoring potential threats and responding to security events with a view to ensuring government's information infrastructure would be well protected.

3. Activities and Operations

3.1 Scope of Services

GovCERT.HK is the computer emergency response team for the HKSAR Government, providing centrally managed incident response services and timely security advice; coordinating cyber security drills; promoting public awareness and capabilities; and engaging global CERT community with a view to enhancing information and cyber security locally and in the region.

3.2 Security News Bulletins

In 2018, GovCERT.HK published the following security bulletins to raise the awareness among government users and the general public.

- "Security Vulnerabilities and Patches" information was consolidated on every working day and disseminated to registered subscribers through emails;
- "Security Industry News" was gathered on every working day and top news with wide impact was compiled and disseminated to registered subscribers through emails; and
- "Weekly IT Security News Bulletins" was published on the first working day of each week to highlight top two to three hot security news and summarise vulnerabilities by products for easy reference by security practitioners. These Bulletins were distributed to registered subscribers through emails and posted at the GovCERT.HK website as public information. (www.govcert.gov.hk/en/reports.html#weekly-reports)

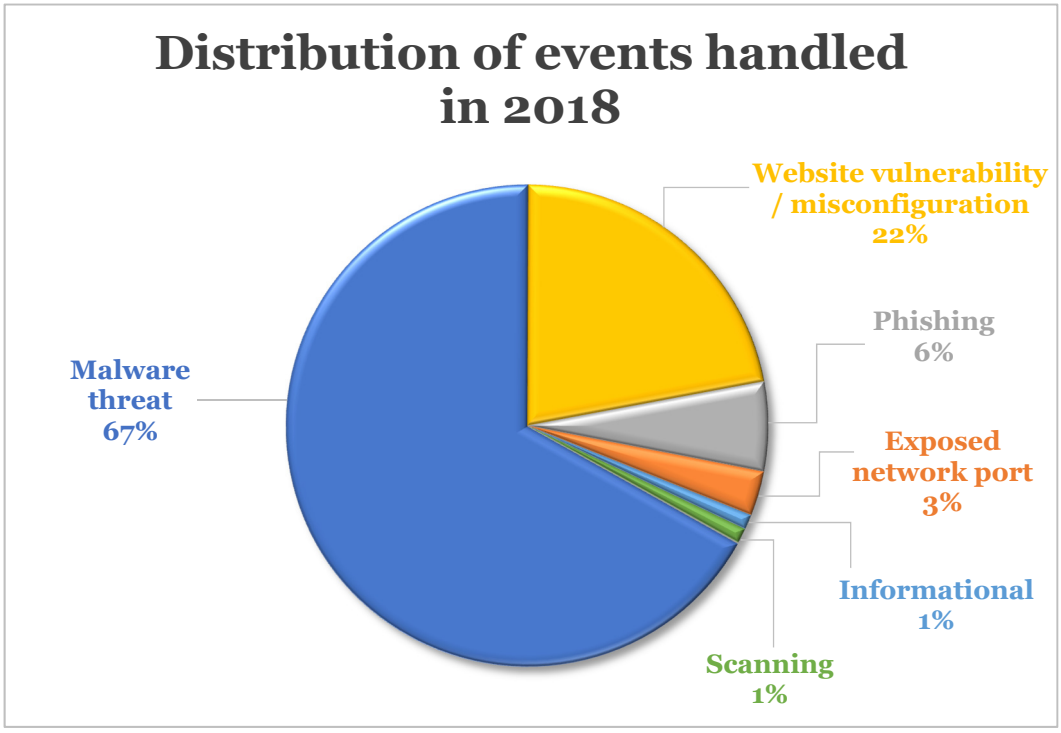
3.3 Alerts and Advisories

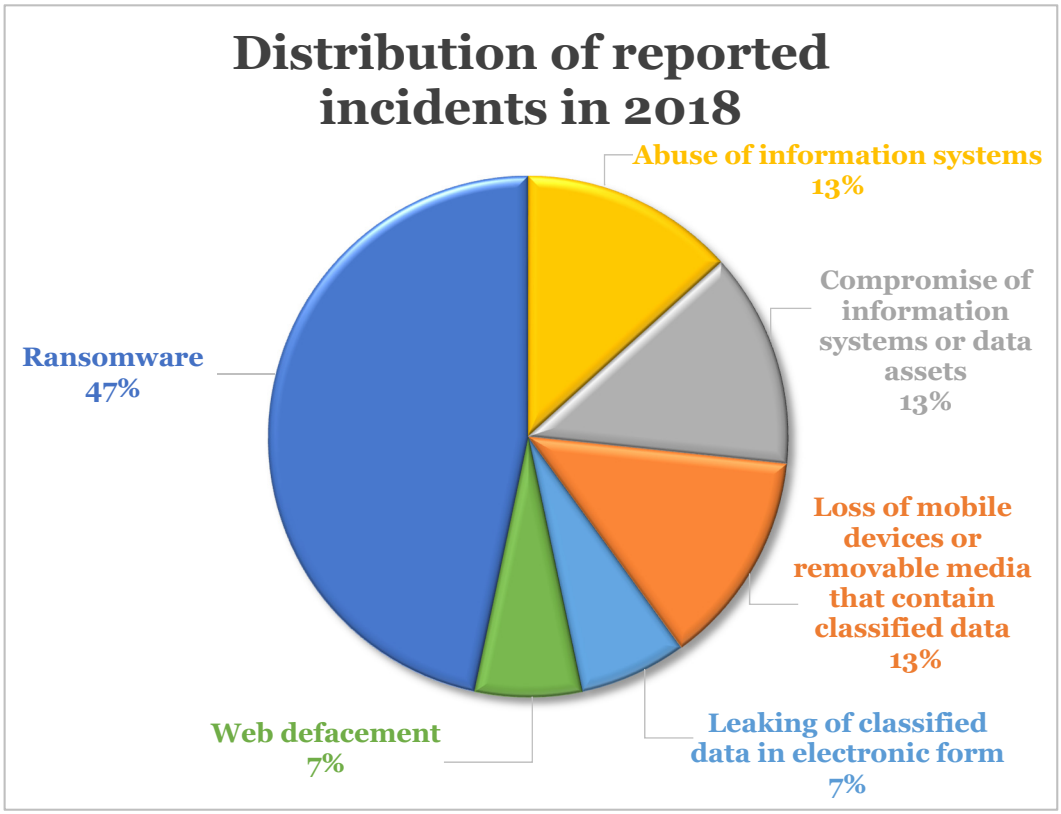
In 2018, we published 103 product security alerts associated with computing products widely deployed in government installations. We also released a security advisory for public reference highlighting the risk of the VPNFilter malware attack and recommending appropriate measures to protect their network equipment. (www.govcert.gov.hk/en/advisories.html)

In 2018, we conducted threat analysis on over 300 security events detected and received from various sources. The threat information was extracted and shared with relevant constituents for appropriate follow-ups.

3.4 Security Events and Incident Handling

Security events indicate possible breaches of information security or failure of security controls. Security incidents, however, are in relation to one or multiple events that can harm information systems and/or data assets or compromise their operations. In 2018, GovCERT.HK dealt with various cyber security events and reported incidents that were related to government installations. The following chart shows the distribution of events and reported incidents handled in 2018.



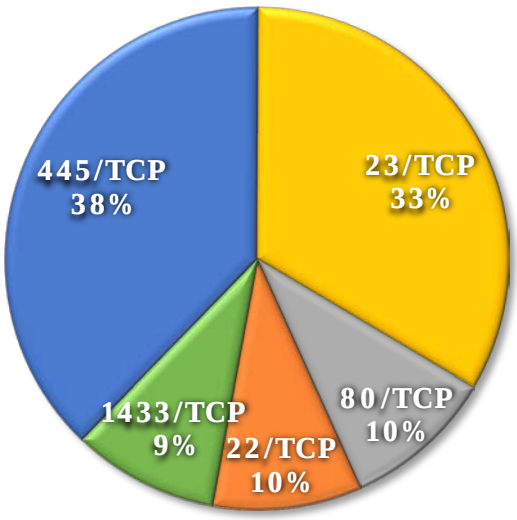


To facilitate the public to access the statistics on information security incidents in the Government, relevant data has been released to the Government's Public Sector Information Portal. (www.data.gov.hk/en-data/dataset/hk-ogcio-sec_div_01-information-security-incident)

3.5 Abuse Statistics

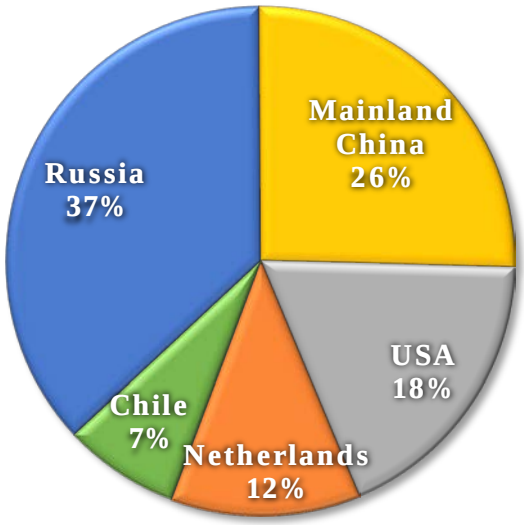
As a member of the TSUBAME project, GovCERT.HK has set up sensors to collect and analyse network scanning activities targeting Hong Kong. The following charts show the top five scanning ports and the top five source regions of scanning activities detected by the TSUBAME sensors installed in Hong Kong.

Top five scanning ports against Hong Kong in 2018



Position in 2018	Port Number	Position in 2017
1	445/TCP	4
2	23/TCP	1
3	80/TCP	-
4	22/TCP	3
5	1433/TCP	2

Top five source regions of scanning against Hong Kong in 2018

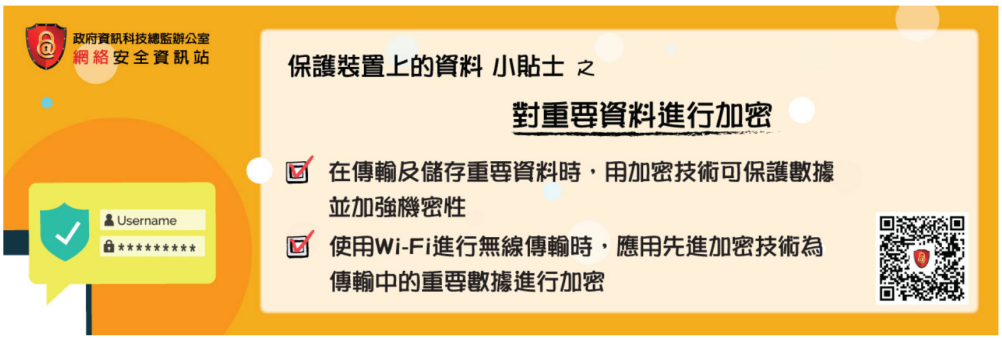


Position in 2018	Source Region	Position in 2017
1	Russia	3
2	Mainland China	1
3	USA	2
4	Netherlands	-
5	Chile	-

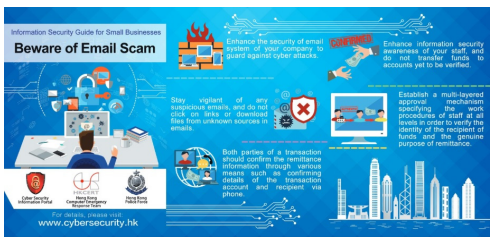
3.6 Publications and Mass Media

As cyber attacks continue to increase in number and sophistication, members of the public face cyber security risks when using different technologies, such as mobile devices, cloud services and social networking applications. We have made use of different promotion channels to reach out to our target audience and collaborated with industry players during the process.

- We broadcasted radio episodes entitled "e-World Smart Tips" to help the public understand more about information security in various aspects and raise their awareness of information security. The radio episode in each month featured a specific theme and offered associated tips on mitigating the risks of cyber threats through daily life examples and in a lively and interesting way. In 2018, we covered a wide range of topics including Wi-Fi security, data security, social networking security, endpoint security, etc.
(www.cybersecurity.hk/en/media.php#Radio)



- To provide practical tips and advice for Small and Medium Enterprise (SMEs) to defend against cyber attacks, a series of "Information Security Guide for Small Businesses" were developed to help them to secure their business.
(www.cybersecurity.hk/en/resources.php#leaflets)



- To raise public awareness on the threats of cyber scams, we organised the "Stay Smart, Keep Cyber Scams Away" video ad contest in 2018. Participants fully demonstrated their creativity to compile short video ad on how to guard against cyber security threats and promote smart tips to keep cyber scams away. The winning entries were uploaded to the InfoSec YouTube Channel for public reference as well. (www.cybersecurity.hk/en/contest-2018-prize.php)

InfoSec YouTube Channel (www.youtube.com/user/infosecgovhk)

4. Events Organised/Hosted

GovCERT.HK regularly organises awareness training and solution workshops to share latest knowledge on security measures, best practices, skills and security solutions with various levels of government users to continuously strengthen their knowledge on cyber attacks and enhance their information security skills, thereby strengthening their capabilities in guarding against cyber attacks.

4.1 Training

In 2018, we organised a total of 18 seminars, trainings and solution showcases for government IT staff and users to enhance their awareness of latest security vulnerabilities and update their knowledge in information security technologies.

- Seminars, trainings and showcases were conducted for government IT staff and users to raise their security awareness and introduce latest IT security technologies and solutions. The topics included industry best practices, phishing, DNSSEC, and security of Internet-connected devices.

- Seminars were organised for departmental IT security officers to refresh their security knowledge and update them on the Government's latest requirements and approaches in dealing with cyber security threats and adopting mitigation measures.

4.2 Drills and Exercises

Inter-departmental Cyber Security Drill of the HKSAR Government

GovCERT.HK has coordinated government departments to conduct cyber security drills to assess the participants' capabilities of incident analysis and test their incident response procedures with a view to enhancing the overall incident response capability.

With the ever-changing cyber threat landscape, it is imperative to enhance the competencies in mitigating cyber threats. We collaborated with the HKPF to conduct the inter-departmental cyber security drill with over 40 departments participated to enhance the overall information security incident response capability of the Government. The drill included a tabletop exercise and a hands-on workshop. Participants discussed how to respond to a simulated malicious attack against a website and handle media enquiries in the tabletop exercise. They also conducted incident response and investigation and applied their cyber security skills in a controlled and simulated environment during the hands-on workshop.

APCERT Drill

As the Operational Member of the APCERT, GovCERT.HK participated in the APCERT Drill with the theme of "Data Breach via Malware in Internet of Things" in March 2018. GovCERT.HK played the role of Exercise Controller in addition to Player and Observer in the drill.

4.3 Conferences and Seminars

In view of the emerging threats of cyber scams in 2018, GovCERT.HK adopted the slogan "Stay Smart, Keep Cyber Scams Away" as the theme. A series of promotional activities were organised for businesses, organisations, schools and the public to raise their awareness against cyber scams such as phishing.

- Two seminars were organised under the "Build a Secure Cyberspace" promotional campaign in May and September 2018, aiming to promote public awareness of information security and adoption of security best practices, in particular the risks of cyber scams.

- Thirty-six school visits were conducted at primary and secondary schools in 2018, reaching out to some 10 000 students, parents and teachers for raising their awareness of cyber security and encouraging the proper attitude in using the Internet.

- To promote the development of cyber security technologies and industry in Hong Kong and the Mainland, the third Hong Kong-Mainland Cyber Security Forum with the theme of "Challenges and Opportunities of Secure, Smart Connectivity" was held in April 2018. The forum attracted some 180 information security professionals from the Government, research institutions, academia, professional organisations and the information security industry to exchange views and observations on cyber security landscape and advise how to meet the challenges to be brought by smart connectivities.

5. Local and International Collaboration

GovCERT.HK has been working closely with HKCERT and other regional and global CERTs for coordinating threat information sharing and incident response.

5.1 Local collaboration

GovCERT.HK is keen on fostering exchanges and experience sharing among the local information security industry. In 2018, we launched Cybersec Infohub, a partnership programme to promote closer collaboration among local information security stakeholders of different sectors. Under the Programme, we have provided a community-driven collaborative platform (Cybersechub.hk) and organised various industry events to facilitate exchange of cyber security information. As of 2018, over 100 organisations with more than 300 representatives across various sectors have joined the Programme.
(www.cybersechub.hk)

The Internet is critical to communications, conduct of e-business and access to e-services. GovCERT.HK has been acting as a supportive role in the Internet Infrastructure Liaison Group (IILG) established and led by OGCIO. The key roles of the IILG are to maintain close liaison with Internet infrastructure stakeholders and strive in collaboration with the stakeholders for the healthy operation of the Internet infrastructure of Hong Kong. In 2018, the IILG collaboration mechanism was activated six times to strengthen monitoring of cyber security of large-scale events and provide support events to protect the local Internet infrastructure against alleged cyber attacks.

5.2 International Collaboration

To foster closer collaboration with international security experts for sharing experience in information security and strengthening the knowledge of emerging cyber threats, vulnerabilities and appropriate mitigation solutions, GovCERT.HK strives to learn from the CERT community on global trends in international standards development, global information security and data privacy policies, cyber crime initiatives and technological researches.

GovCERT.HK participated in the following events in 2018:

- Hong Kong – Mainland Cyber Security Forum
- FIRST Annual Conference
- Annual Technical Meeting for CSIRTs with National Responsibility
- CNCERT/CC Annual Conference
- 2018 China Cybersecurity Week
- APCERT Annual General Meeting and Conference
- Five APCERT on-line training sessions

6. Future Plans

6.1 Upcoming Projects

The accelerated development of emerging technologies is spurring continuous innovation, however, it could also bring along different cyber security threats. GovCERT.HK will continue to stay vigilant in defending against potential cyber attacks. In the coming year, we will launch a new round of review of the Government IT Security Policy and Guidelines by making reference to the latest international standards and industry best practices. In addition, a penetration testing platform will be set up to provide simulated network and system environments for testing web applications against potential cyber attacks.

To enhance the capability of cyber threat intelligence management, GovCERT.HK plans to operate a Malware Information Sharing Platform (MISP) instance in 2019 to enable sharing, storing and correlation of Indicators of Compromise.

6.2 Future Operations

Artificial intelligence elements will be introduced to the collaborative platform of Cybersec Infohub by making use of machine learning to build and operate the text analytics model in the first half of 2019. This move will assist members in the integration and analysis of cyber security information and facilitate easier and faster acquisition of required information by experts for timely dissemination of the information to the public.

7. Conclusion

Cyber security attacks are increasingly sophisticated, with the forms they take becoming more diversified. GovCERT.HK has been proactively collaborating with local and global CERTs, making timely response and enhancing appropriate defensive measures to the inevitable cyber security threats. GovCERT.HK will continue to foster all stakeholders to take forward communication and exchange of cyber security information so as to keep abreast of the fast-evolving cyber security landscape and enhance the cyber security resilience capability of the community.

Contact: cert@govcert.gov.hk
Websites: www.govcert.gov.hk
www.cybersecurity.hk
www.cybersechub.hk