Annual Report 2020

GovCERT.HK

www.govcert.gov.hk

Highlights of 2020

1.1 Summary of Major Activities

2020 has been an extraordinarily challenging year for all of us to adapt swiftly to the rapidly changing global conditions. Under the "new normal" amid the Coronavirus Disease 2019 (COVID-19) epidemic, the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) has maintained its smooth operation and contributed in fighting this battle by offering assistance including conducting security risk assessment and vulnerability scanning in time to safeguard newly developed systems and applications of the Government of the Hong Kong Special Administrative Region of the People's Republic of China (the Government) in combating the epidemic. We have also monitored and provided information security advice on the work-from-home arrangement and usage of video conferencing solutions to government users. In response to arising cyber attacks using COVID-19 related themes, we have worked closely with stakeholders to provide security advice in a timely manner. All these measures have been proven to be vital for Hong Kong's integral effort in maintaining a secure cyberspace under the ever-changing global digital environment.

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 2020, we continued publishing threat trends, security alerts and mitigation

Highlights of 2020

advice through the GovCERT.HK web portal for the general public's reference. We further tailored specific threat awareness updates for government departments.

To enhance the city's overall defensive capability and resilience against cyber attacks, we continued to leverage the local cross-sector Partnership Programme for Cyber Security Information Sharing (Cybersec Infohub), to promote trusted partnership between local cyber security stakeholders across different sectors for sharing cyber security information and providing actionable insights to the community. We regularised the programme to encourage more participation of organisations from various industries.

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.

Highlights of 2020

1.2 Achievements and Milestones

Operation under the "New Normal"

In response to the workforce transformation sparked by the COVID-19 epidemic, GovCERT.HK has adopted various initiatives, such as releasing educational videos on cyber conference security and guidelines for remote access and corporate VPN security, to remind organisations and the public to stay alert of cyber threats arose from the epidemic. We have also paid close attention to epidemic-themed cyber risks and collaborated with stakeholders to provide security alerts and advice. In addition, GovCERT.HK has rendered its support to various COVID-19 epidemic related programmes and systems in order to timely launch various government services to combat the COVID-19 epidemic.

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 to nurture a culture of sharing cyber security information. Given the positive response from participating public and private organisations of Cybersec Infohub operating for over two years, we regularised the programme and partnered with the Hong Kong Internet Registration Corporation Limited (HKIRC) to encourage more participation from various industries including the small and medium enterprises (SMEs). In 2020, we gathered industry experts to form a new supporting alliance, Cybersec Connect, to offer support and advice on cyber security related problems for the members. The programme has become an

essential reference for organisations to obtain cyber security information and meet with various stakeholders to exchange the latest security trends and best practices.

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. We have published monthly Cyber Security Threat Trends Report via the GovCERT.HK web portal to highlight observations on the latest cyber security threat landscape for the public's reference. To enhance the capacity and capability of cyber threat intelligence management, we integrated Malware Information Sharing Platform (MISP) instances into the Cyber Risk Information Sharing Platform (CRisP) to enable collection, sharing, storing and correlation of Indicators of Compromise and facilitate collaboration on handling security events with related parties in the Government.

Government IT Security Policy and Guidelines

To ensure that the policy and guidelines tie in with security trends as well as technology advancement, the Government reviewed the "Government IT Security Policy and Guidelines" to cover the latest areas of information and cyber security with reference to international standards and industry best practices. Requirements were strengthened in various security areas including protection of mission critical systems and common applications, remote access control, protection of personal data and adoption of emerging technologies such as Internet of things (IoT) and public cloud. The updated government IT security policy and guidelines were uploaded onto GovCERT.HK's website for reference by the public.

Liaison and Collaboration

We actively participated in the Asia Pacific Computer Emergency Response Team's (APCERT) activities and worked closely with the Computer Emergency Response Team (CERT) community in handling threat information. We have been supporting the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) to produce a series of animations to raise public awareness of cyber security with themes including remote working and video conference, cloud security, phishing and malware, and IoT security.

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 scams and data breaches during the COVID-19 epidemic, GovCERT.HK produced a series of promotional materials including educational animations and smart tips for the public to protect themselves from and defend against cyber threats.

GovCERT.HK also devoted much attention to public education and capacity building in different business sectors and age groups, with some 20 face-to-face and online school visits conducted in 2019/20 and 2020/21 school years. We revamped our Information Security (InfoSec) website to provide a more lively design for better user experience and disseminate security related tips and advice to the public.

About GovCERT.HK

2.1 Introduction

The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) is a governmental Computer Emergency Response Team (CERT) responsible for coordinating incident response for over 80 departmental Information Security Incident Response Teams (ISIRTs) of the 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 infrastructure stakeholders, and the CERT community for timely exchange of cyber threat information and coordinated responses. GovCERT.HK also works closely with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and local industries on cyber threat intelligence sharing, capability development, public education, and continuous promotion on cyber security through social and mass media.

GovCERT.HK also actively collaborates with other governmental and regional CERTs, and international organisations in sharing cyber threat intelligence and incident information; participating in training events, workshops, forums and drills; and organising activities for public awareness promotion and capability development.

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 Government.

2.3 Resources

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

2.4 Mission and Constituency

Being the governmental CERT, GovCERT.HK centrally manages incident responses within the Government and develops 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 that the government's information infrastructure is well protected.

Activities and Operations

3.1 Scope of Services

GovCERT.HK is the CERT for the 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 in the region.

3.2 Security News Bulletins

In 2020, 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 summarise selected recent security news and product vulnerabilities for security practitioners' easy reference. The Bulletins were distributed to registered government subscribers through emails and posted at the GovCERT.HK website as public information. (www.govcert.gov.hk/en/secbulletins.html)

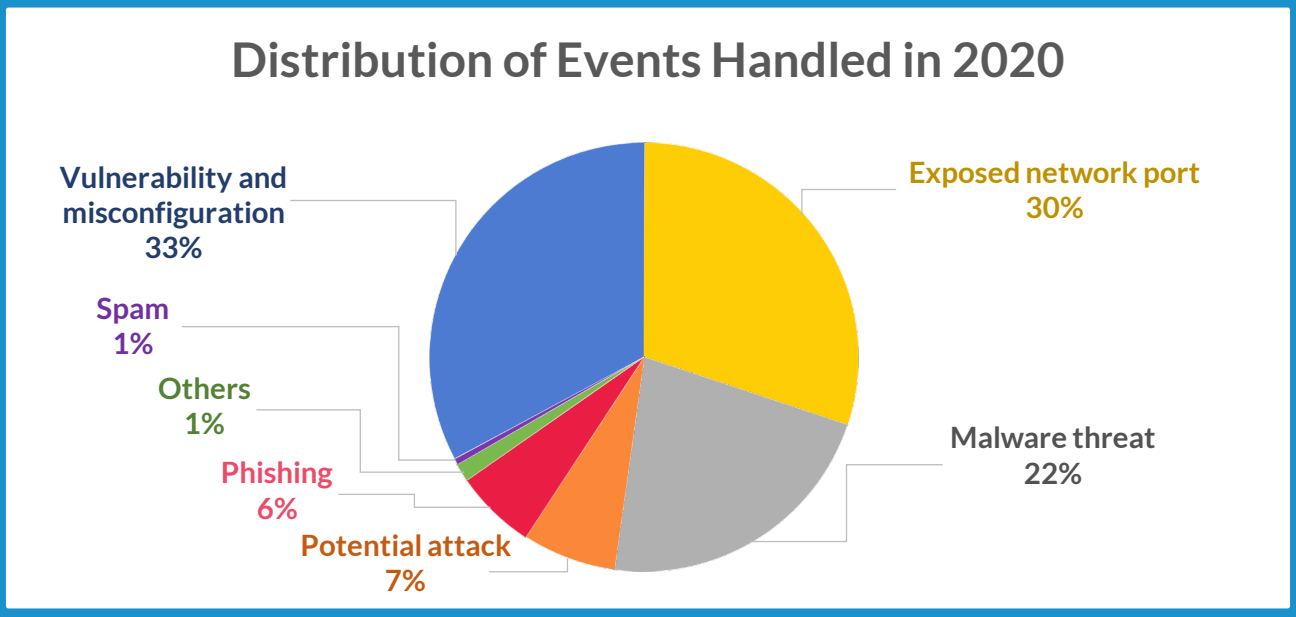
3.3 Alerts and Advisories

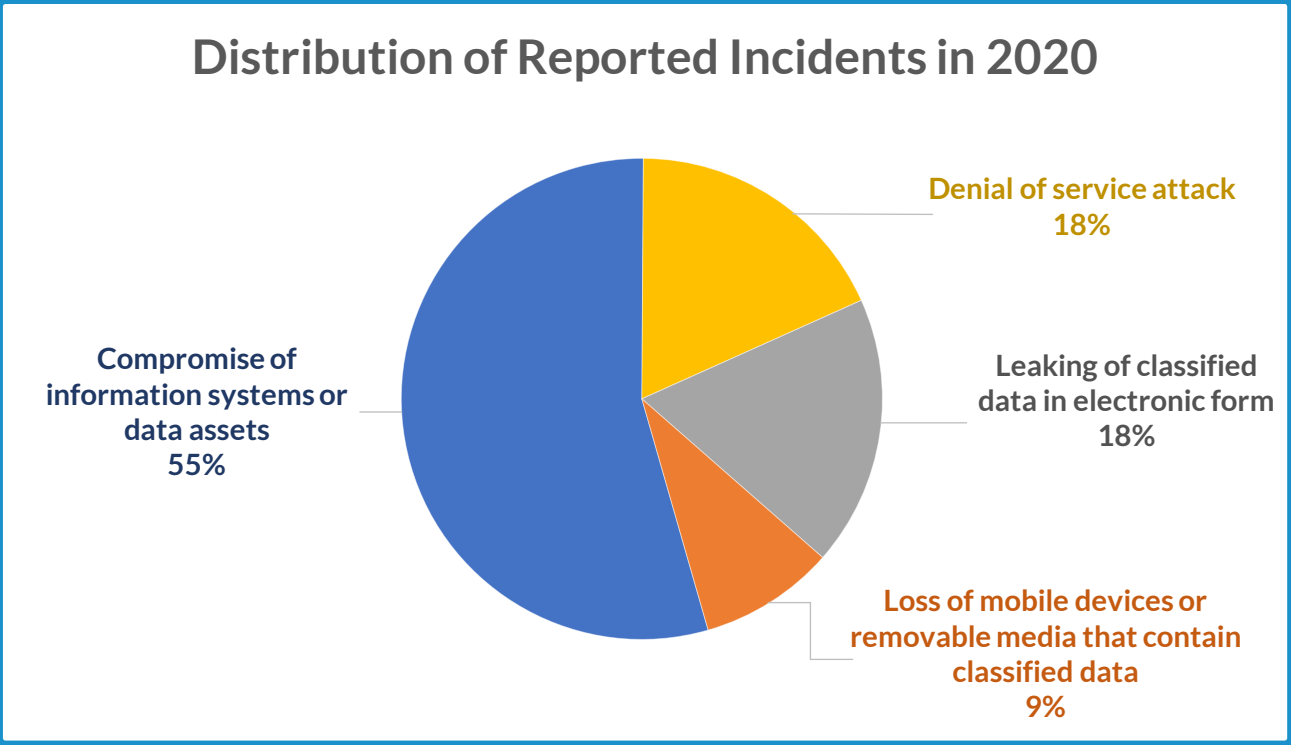
In 2020, GovCERT.HK issued over 90 security alerts associated with computing products widely deployed in government installations. For those security vulnerabilities which were considered highly risky to the Government, we proactively requested government departments to take prompt and appropriate preventive measures against potential information security risks.

We also conducted threat analysis on over 210 security events detected and received from various sources. The threat assessment results and security advice were promptly shared with relevant parties 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 2020, GovCERT.HK dealt with various cyber security events and reported incidents that were related to government installations. The following charts show the distribution of events and reported incidents handled in 2020.



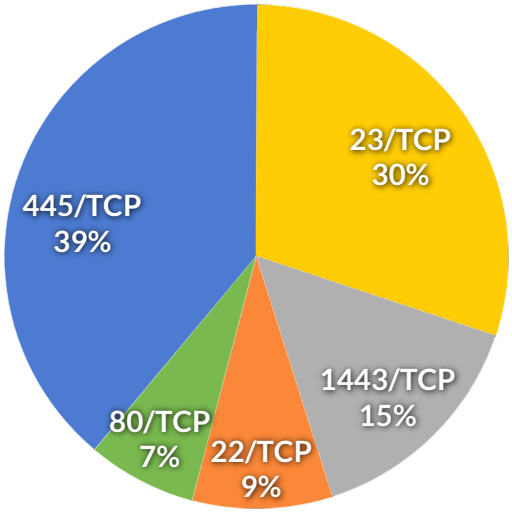


To facilitate public access to the statistics on information security incidents in the Government, relevant data has been made available on the Government's Public Sector Information Portal. (www.data.gov.hk/en-data/dataset/hk-ogcio-sec_div_01-information-security-incident).

3.5 Abuse Statistics

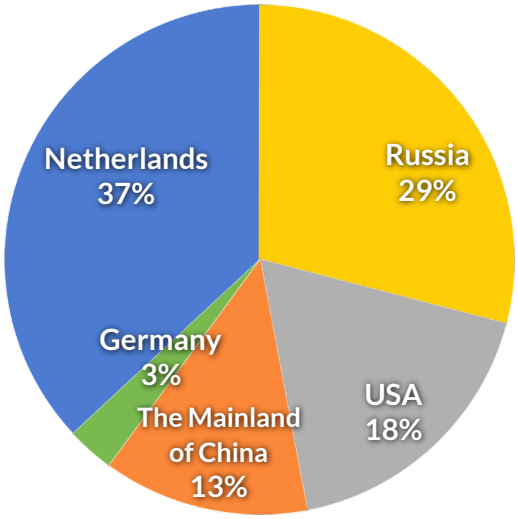
As a member of the TSUBAME project under APCERT, GovCERT.HK has set up sensors to collect and analyse network scanning activities targeting at Hong Kong. The following charts show the top five scanning ports (contributed 13% of all the scanning activities) and the top five source regions (contributed 76% of all the scanning activities) detected by the TSUBAME sensors installed in Hong Kong in 2020.

Top Five Scanning Ports against Hong Kong in 2020



Position in 2020	Port Number	Position in 2019
1	445/TCP	1
2	23/TCP	2
3	1443/TCP	5
4	22/TCP	4
5	80/TCP	-

Top Five Source Regions of Scanning against Hong Kong in 2020

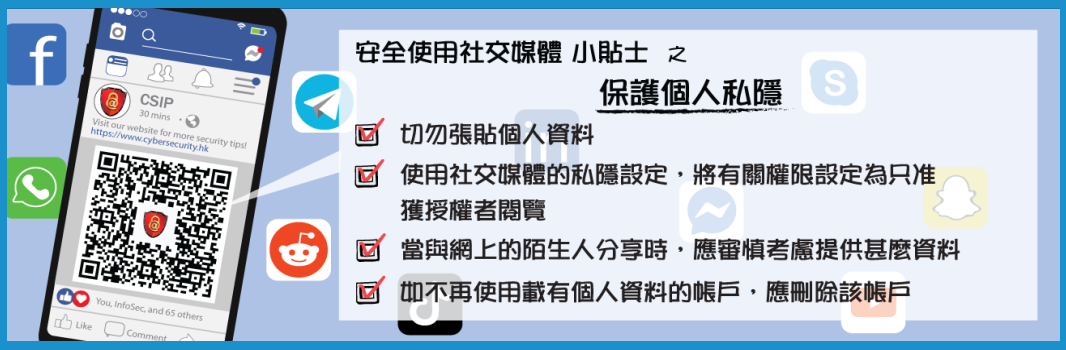


Position in 2020	Source Region	Position in 2019
1	Netherlands	3
2	Russia	1
3	USA	4
4	The Mainland of China	2
5	Germany	-

3.6 Publications and Mass Media

The COVID-19 epidemic has created new challenges in adapting the digitally transformed living. To actively reach out to the general public, various promotion channels including radio broadcast, YouTube, Facebook, Twitter, webinars, and school visits were used to share tips and best practices on using different technologies, such as mobile devices, cloud services, social networking applications and remote working applications under the new normal.

- 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 the issue. 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 2020, we covered a wide range of topics including data security, phishing attacks, social networking security, IoT devices security, and more. (www.cybersecurity.hk/en/media.php#Radio)



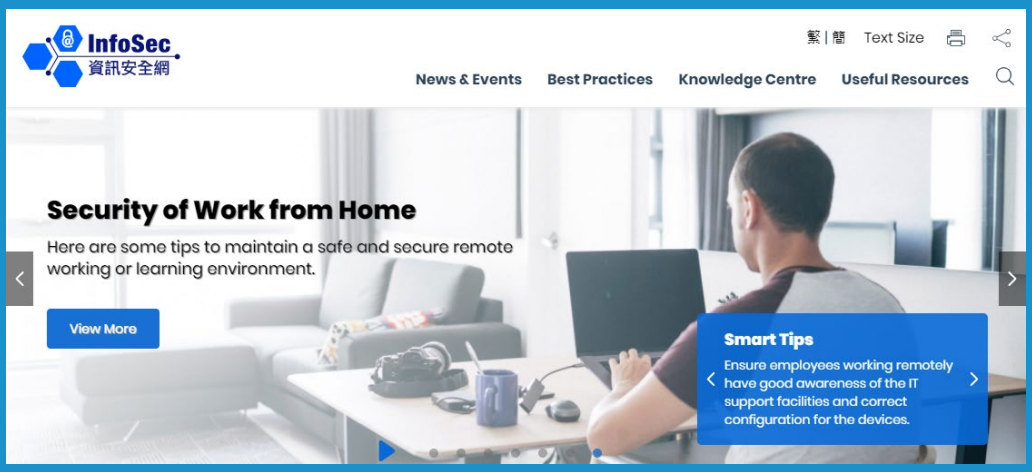
- A series of handy guidelines with different themes were developed to provide practical tips and advice for SMEs to guard against cyber attacks. (www.cybersecurity.hk/en/resources.php#leaflets)

- To encourage the public to exercise care when using mobile devices and raise their awareness of mobile device security, we organised the "Secure Use of Mobile Devices" sticker design contest in 2020. Participants fully demonstrated their creativity to design a set of stickers for instant messaging applications to convey the message of taking precautions to protect mobile devices. The winning entries are now available at www.cybersecurity.hk/en/contest-2020.php. Download now and share with your family and friends!

Winning Entries

- Leveraging the OGCIO Facebook page, we have shared a series of posts with timely updates and tips on cyber security topics such as precaution of phishing attacks and safe use of remote working applications. The posts were made in a light-hearted manner with eye-catching infographics and animations to strengthen our communications with the public. (www.facebook.com/OGCIOHK)

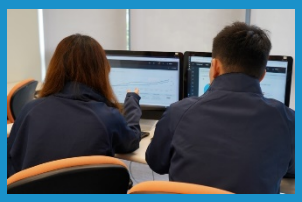
- In 2020, we have also revamped our InfoSec Website to provide a more lively design for disseminating security related tips and advice useful for all members of the public.
(www.infosec.gov.hk)



3.7 GovCERT.HK Technology Centre

To facilitate the Government in developing staff capabilities on more specialised knowledge and skills to tackle evolving cyber threats, our GovCERT.HK Technology Centre offers government departments a controlled environment with relevant facilities and equipment to enable vulnerability scanning, dynamic application security testing, penetration testing and malware analysis for potential security issues of their web applications. The overall security of government web applications and services is enhanced by making use of the tools to identify web vulnerabilities, misconfigurations, compromised passwords, etc.

Web vulnerability scan & dynamic application security testing



Penetration testing platform

Malware analysis corner

Password checker

GovCERT.HK Technology Centre

Events Organised / Hosted

GovCERT.HK regularly organises awareness training and solution workshops to share the 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 2020, we organised more than 10 seminars, webinars and trainings for government IT staff and users to raise their information security awareness and update their knowledge on the latest IT security technologies and solutions. More than 1 400 government staff participated in these events to understand the latest cyber security trends and preventive measures. Topics included information security management, IT governance, protection of personal data, security measures and best practices for remote working, defence against phishing, operating system security, promotion of various security solutions, etc.

4.2 Drills and Exercises

Inter-departmental Cyber Security Drill of the Government

To enhance the overall incident response capability of the Government, GovCERT.HK has actively coordinated government departments to conduct cyber security drills to enhance the participants' incident handling capabilities and test their familiarity with the predefined incident response procedures.

This year, we continued to organise the annual inter-departmental cyber security drill to strengthen the cyber security incident response capability of the Government. The drill was held in online mode due to the COVID-19 epidemic. We provided a simulated cyber attack scenario for participants to discuss and propose response actions based on the background information given. An incident response workshop was also organised to enhance the capabilities of participants in handling, investigating and analysing cyber attacks.

Government-wide Phishing Drill Campaign

To further strengthen government users' awareness and capabilities in defending against phishing attack, we have successfully completed the "Government-wide Phishing Drill Campaign" in 2020. More than 1.7 million of pseudo-phishing emails were sent out to all Government Internet email users and a general improvement on awareness of phishing emails was observed upon completion of the exercise. Apart from the drill, we organised a number of webinars to share the common findings and lesson learnt from the drills. We also launched a set of interactive phishing quizzes to continue promoting awareness of the issue in the government.

APCERT Drill

As an Operational Member of the APCERT, GovCERT.HK participated in the APCERT Drill with the theme of "Banker doubles down on Mining" in March 2020. GovCERT.HK played the role of Exercise Controller in addition to Player and Observer in the drill.

4.3 Conferences and Seminars

Build a Secure Cyberspace Promotional Campaign

To promote public awareness of mobile device security, GovCERT.HK adopted "Secure Use of Mobile Devices" as the theme in 2020. A series of promotional activities were organised for businesses, organisations, schools and the public to raise their awareness of adopting security measures proactively to better protect their mobile devices.

- Two webinars were organised under the "Build a Secure Cyberspace" promotional campaign in May 2020 and February 2021, aiming to promote public awareness of cyber security challenges in remote working and online learning during the epidemic, and taking precautions to protect mobile devices.

School Visits and InfoSec Tours

To promote cyber security awareness and cyber etiquette to our community, GovCERT.HK organised visits to primary, secondary schools and tertiary institutions to deliver information security talks to students, teachers and parents. GovCERT.HK also partnered with the Radio Television Hong Kong (RTHK) to conduct InfoSec Tours, aiming to deliver information security message in a relaxing way by visiting schools and conducting a variety of activities.

- More than 20 face-to-face and online school visits were conducted in the 2019/20 and 2020/21 school years, reaching out to more than 5 000 students and parents for raising their awareness of cyber security and encouraging the proper attitude in using the Internet.
- In response to the increasing adoption of digital technology by the elderly in their daily lives, the OGCIO also conducted seminars for them to raise their cyber security awareness.
- One InfoSec Tour was conducted at a primary school in 2020. In view of the epidemic situation, we produced two InfoSec Tours videos with topics of "Study at home safely" and "Responding to the temptation of the online world" for broadcasting remotely.

Cybersec Infohub Engagement Activities

To encourage trust building, facilitate exchange of cyber security information and promote closer collaboration among different sectors under the Cybersec Infohub partnership programme, sector-specific events, professional workshops and webinars were arranged in 2020 with positive response from participants.

Local and International Collaboration

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

5.1 Local Collaboration

Cybersec Infohub

GovCERT.HK continued to promote closer collaboration among local information security stakeholders of different sectors to share cyber security information through the Cybersec Infohub programme (www.cybersechub.hk), with over 320 organisations and more than 1 000 representatives from various sectors joined the programme as of 2020. In particular, we have encouraged exchanges of cyber security information within key industries with higher risks to cyber attacks, such as banking and healthcare sectors. We have helped members from these sectors to form private groups for closer collaboration on specific topics of common interest.

The Cybersec Infohub started a new chapter in September 2020 through partnership with HKIRC in running the formalised programme to further encourage more organisations, including SMEs, to join and collaborate so as to bring Hong Kong's cyber security to a new level. A launching ceremony cum members professional workshop was held in September 2020 to embrace the

bright future of the Cybersec Infohub and enlighten members on the salience of information sharing.

A cyber security supporting alliance of industry experts gathered, named Cybersec Connect, was also set up under the programme to answer cyber security-related questions from members, especially SMEs, and offer appropriate advice.

Internet Infrastructure Liaison Group (IILG)

To help maintain the healthy operation of the Internet infrastructure of Hong Kong, GovCERT.HK continued to support the IILG which was established and led by the OGCIO to foster closer liaison with the Internet infrastructure stakeholders, aiming to collaborate with the stakeholders for the smooth operation of the local Internet infrastructure. In 2020, the IILG collaboration mechanism was activated five times to support major events and take precautions against cyber threats, such as issuance of reminder to local Internet infrastructure stakeholders to stay vigilant against Distributed Denial-of-Service (DDoS) Extortion Attacks in September 2020.

HKCERT

Building cyber security awareness is one of the keys to defence against cyber attacks. To raise public awareness of cyber threats, we have been working with HKCERT for the new project "HKCERT Digital Campaign for Security Awareness Promotion" to produce and disseminate a series of animations covering topics on remote working and video conference, cloud security, phishing and malware, and IoT security via social media.

(www.youtube.com/watch?v=FH7zWAb4-GQ)
(www.youtube.com/watch?v=Jhzpcr7CeZw)

To nurture more talents to join the information security industry, and to enhance the cyber security awareness of local students, we supported HKCERT in organising a Capture the Flag (CTF) Challenge that provided students the opportunity to compete in cyber security tasks to gain real life experience in computer security.

HKIRC

We have also supported HKIRC to provide a free website scanning service to SMEs to help them identify and mitigate potential information security issues, as SMEs are generally with fewer resources devoted to cyber security and hence more vulnerable to 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 strived 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 2020:

- FIRST Annual Conference
- Annual Technical Meeting for CSIRTs with National Responsibility
- CNCERT/CC Annual Conference
- CNCERT/CC Online Conference for International Partnership
- 2020 China Cybersecurity Week
- APCERT Annual General Meeting and Conference
- APCERT Drill
- APCERT Online Training Sessions
- APISC Security Training

Future Plans

6.1 Upcoming Projects

To meet the challenges of evolving security threats posed by emerging technologies and keep pace with the development of international standards and industry practices in information security management, we have conducted regular reviews to assess the latest cyber security trends and provide recommendations of necessary updates to the government IT security related regulations, policies and guidelines. We will continue to develop new practice guides on different technology areas for reference by government departments, and share these practice guides with the public where appropriate.

We will also collaborate with HKCERT to organise another CTF competition to nurture the next generation of information security talents and raise their interests in joining the cyber security workforce of the future. The competition will be divided into three groups, including secondary schools, tertiary institutions, and open group to make it more exciting.

6.2 Future Operations

Considering the continual growth of a wider spectrum of organisations in the membership base of Cybersec Infohub, information sharing via the collaborative platform will be further enhanced by integrating external threat intelligence feeds and enabling machine-to-machine sharing via Application Programming Interfaces (APIs). It will facilitate the members to integrate the invaluable cyber security information automatically with their information security systems for more timely response in safeguarding against potential cyber threats.

Conclusion

Cyber security attacks are increasingly targeted and sophisticated, with the forms they take becoming more diversified. GovCERT.HK has been proactively collaborating with local and global CERTs to take forward communication and make timely responses in facing the transboundary cyber security threats. In facilitating Hong Kong to become a secure smart city, GovCERT.HK will continue to encourage effective exchange of cyber security information and raise situational awareness of community stakeholders to stay keen of the fast evolving cyber security landscape, with unceasing efforts to enhance the cyber security resilience capability of the community.

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