

ANNUAL REPORT

2025

GovCERT.HK
www.govcert.gov.hk



HIGHLIGHTS OF 2025

1.1 Summary of Major Activities

The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) persistently collaborated with relevant stakeholders to deliver a wide range of initiatives to strengthen cybersecurity resilience, enhance defensive capabilities and promote cybersecurity awareness amid an increasingly complex threat landscape. In view of several major events in 2025, including the 15th National Games and the eighth Legislative Council General Election, we reinforced safeguards for digital infrastructure and government information systems, enhanced monitoring and threat intelligence, and strengthened operational readiness through regular drills and collaboration to ensure safe and stable operation of Hong Kong's digital infrastructure and government information systems.

1.2 Achievements and Milestones

Cyber Security Assurance and Resilience

To strengthen government-wide cyber resilience, we organised attack-and-defence training and tournament activities in collaboration with the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF) and the Hong Kong Internet Registration Corporation Limited (HKIRC) to enhance the professional skills and incident response capabilities of cybersecurity personnel. We also partnered closely with the CSTCB of HKPF, HKIRC and the Hong Kong Institute of Information Technology (HKIIT) to continuously enhance operational readiness through inter-departmental cybersecurity drill exercises and the Hong Kong Cybersecurity Attack and Defence Drill, enabling participants to validate incident response procedures, sharpen technical skills and improve coordination under simulated scenarios.

HIGHLIGHTS OF 2025

Furthermore, we conducted a comprehensive review of government information security policies and guidelines, carried out regular compliance audits for bureaux and departments (B/Ds) to assess adherence to relevant security requirements, and enhanced monitoring and intelligence-gathering mechanisms to improve detection and response, thereby strengthening resilience against evolving threats and challenges.

Awareness and Capability Building

To enhance public awareness of information security and strengthen the cybersecurity capabilities of IT practitioners, we collaborated with industry stakeholders to deliver the Cybersecurity Awareness Campaign 2025 under the theme “Let’s Secure as we Digitalise”, comprising contests, a prize campaign, seminars and forums that promoted practical cyber hygiene and secure digital practices. The Cybersecurity Symposium 2025 was a key highlight, convening industry leaders and experts to exchange views on emerging threats and effective defence strategies. In parallel, we organised thematic seminars, technical workshops and certificate training on information security and cybersecurity incident response to uplift professional competencies and operational readiness, and worked with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and HKIRC to launch the “Cybersecurity Service Providers Connect Programme” and “Cybersec One” programme respectively, to strengthen organisational resilience.



HIGHLIGHTS OF 2025

Liaison and Collaboration

We maintained close liaison and collaboration with local partners such as HKIRC and HKCERT, relevant stakeholder groups, and Greater Bay Area counterparts, while also actively participating in international CERT community activities, exchanges, training and drill exercises in Asia Pacific Computer Emergency Response Team (APCERT) and the Forum of Incident Response and Security Teams (FIRST), with the aim of strengthening coordination, intelligence exchange and collective preparedness.

ABOUT GOVCERT.HK

2.1 Introduction

GovCERT.HK is a governmental CERT responsible for coordinating incident responses for over 80 departmental Information Security Incident Response Teams (ISIRTs) of the Government of the Hong Kong Special Administrative Region of the People's Republic of China (“the Government”).

GovCERT.HK works closely with HKCERT and HKIRC, local industries and critical Internet infrastructure stakeholders on cyber threat intelligence sharing, capability development, public education and continuous promotion on cyber security. 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, with a view to enhancing information and cybersecurity in the region.

2.2 Establishment

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

2.3 Resources

GovCERT.HK is an establishment under DPO (formerly 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 robust protection of government's information infrastructure.

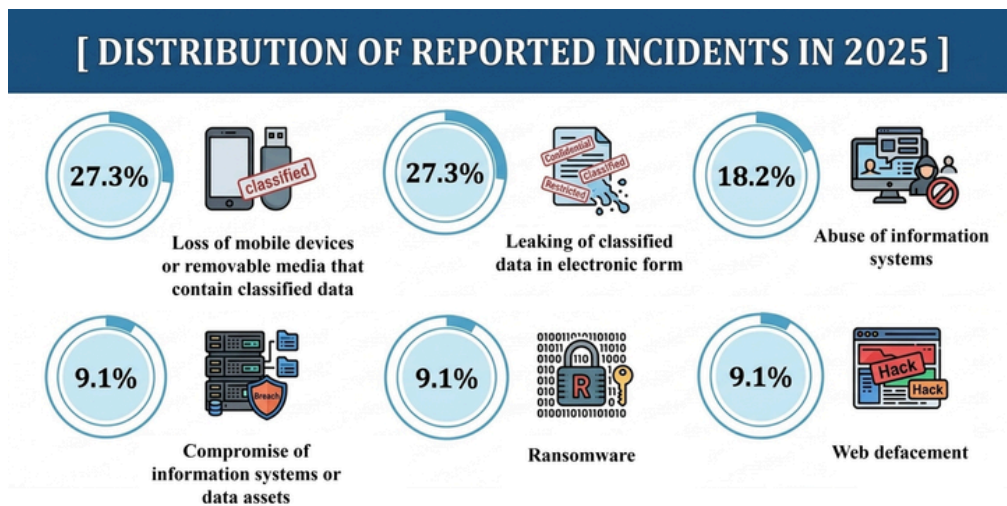
ACTIVITIES AND OPERATIONS

3.1 Alerts and Advisories

In 2025, GovCERT.HK issued 263 security alerts on known vulnerabilities in common products. We proactively requested government departments to implement prompt and appropriate preventive measures for all reported vulnerabilities, with particular emphasis on those assessed at higher severity levels to mitigate potential information security risks.

3.2 Incident Handling Reports

GovCERT.HK handled 11 reported incidents related to government installations, with the incident types shown below:

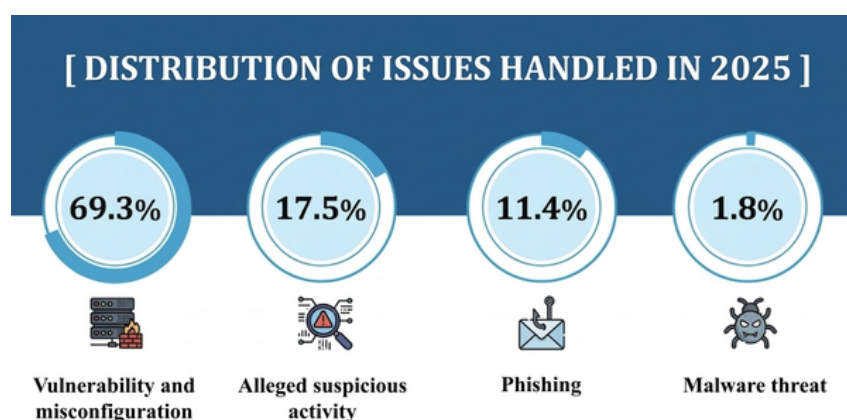


Relevant statistics on information security incidents in the Government are also available on the Government's Public Sector Information Portal for public access.

(http://www.data.gov.hk/en-data/dataset/hk-dpo-pgc_div_01-information-security-incident)

3.3 Abuse Statistics

GovCERT.HK assisted government departments to take effective and prompt measures to prevent and reduce the risks and impacts of cyberattacks on their information systems, with the types of security issues shown below:



3.4 Publications and Mass Media

To proactively reach out to the public, we continued to share tips and best practices against cyber threats through multiple channels.

- We partnered with Radio Television Hong Kong (RTHK) to broadcast radio episodes “e-World Smart Tips”, covering a wide range of topics such as tips for safe online sharing, secure online shopping, Wi-Fi security, mobile payments, netiquette, data loss prevention, digital identity protection, password hygiene, and the safe use of instant messaging and AI, in a lively and interesting way. (www.cybersecurity.hk/en/media.php#Radio)

- We published practical leaflets and infographics on themes such as digital signage security, online shopping security tips, phishing awareness and guidance on identifying and responding to deepfakes, to raise public awareness and encourage protective measures against cyber threats.

(www.cybersecurity.hk/en/resources.php)



- We organised the “Let's Secure as we Digitalise” Instant Messaging Apps Stickers Design Contest, which attracted many creative and impactful submissions. The designs effectively raised public awareness of cybersecurity through artistic expression and were well received. They also served as timely reminders for the public to stay vigilant against online scams, strengthening city-wide cyber resilience and collective defence against cyberattacks.



Winning Entries



- We provided timely updates and practical tips on the latest cybersecurity news and events on the DPO Facebook page, including guidance on the safe use of cloud services and AI to enhance public awareness.

(<http://www.facebook.com/digitalpolicyhk>)

3.5 Government-wide Health Check

GovCERT.HK has implemented a centralised cyber security health check platform since December 2024 to perform regular and continuous health checks on government public-facing information systems and websites. This initiative aims to enhance the detection of potential security vulnerabilities, thereby strengthening the prevention of information and cyber security incidents. For government information systems and websites with relatively higher risk, GovCERT.HK adopts a risk-based approach, selecting government information systems for manual penetration testing to identify application-level security vulnerabilities.

EVENTS ORGANISED/HOSTED

4.1 Training

Seminars/Webinars

In 2025, we organised a range of seminars, webinars, and training sessions covering the latest IT security technologies and solutions, emerging cybersecurity threats, and response strategies. More than 6 900 government staff participated in these events, which addressed topics including phishing prevention, AI and social media security, safe browsing practices, network security, and credential-based threats.

In collaboration with the Civil Service College, we delivered an Innovation and Technology (I&T) leadership series of thematic seminars to strengthen government senior management's understanding and capabilities in information systems management, cybersecurity, and data security.



Certificate in Cybersecurity for the Public Sector

To enhance government staff's information security competencies, we commissioned the Hong Kong Institute of Information Technology (HKIIT) to design and deliver the Certificate in Cybersecurity for the Public Sector, an accredited programme recognised under the Hong Kong Qualifications Framework (HKQF). The programme comprises three levels: Foundation, Intermediate, and Advanced to comprehensively enhance the information security skills of government staff.

4.2 Audit, Drills and Exercises

Government-wide information security compliance audit

A new round of government-wide information security compliance audits was launched in late 2024, and audits covering all B/Ds were completed in 2025. In addition, nine major government IT systems were identified under a risk-based approach for in-depth compliance audits, to ensure B/Ds' adherence to government information security requirements.

Inter-departmental Cyber Security Drill

GovCERT.HK partnered with the CSTCB of HKPF to organise the annual Inter-departmental Cyber Security Drill, with a view to strengthening the preparedness and overall defensive capabilities of B/Ds against cyberattacks since 2017. In 2025, the exercise reached new milestones in both scale and participation, over 280 government officers from 71 B/Ds, together with industry experts from six professional and academic institutions, participated in this drill and an online training workshop to share the latest strategies and techniques for handling cyber incidents.

Hong Kong Cybersecurity Attack and Defence Drill

Following the success of the first Hong Kong Cybersecurity Attack and Defence Drill (the Drill) organised last year, we spearheaded to organise the Drill again in collaboration with the CSTCB of HKPF, HKIRC, Cyberport, and HKIIT in 2025, to enhance the technical skills, strategy, experience, and overall defence capabilities of participants in identifying and responding to cyberattacks. The scale of this year's drill has been expanded to include the participation of 25 government departments and 9 public organisations forming the defensive teams, and 15 red teams formed by cyber security enterprises and post-secondary colleges, thereby enhancing the drill effectiveness. Experienced teams from the Mainland were also invited to participate in the red teams this year to promote technical exchanges between the two places. Moreover, over 250 representatives from more than 60 government departments and organisations took part in the drill on-site as observers to monitor the operation and progress of the exercise and learn more about the latest trends in cybersecurity threats from the Drill.



Government-wide Phishing Drill Campaign

A new round of the Government-wide Phishing Drill Campaign was completed in 2025. The campaign leveraged new technologies, including AI, to simulate realistic phishing emails, thereby strengthening government staff's awareness and ability to identify and report phishing attempts.

4.3 Conferences and Seminars

Build a Secure Cyberspace Promotional Campaign

A series of promotional activities under the theme "Let's Secure as we Digitalise" were organised for organisations, schools and the public to raise their cyber security awareness and strengthen their cyber security postures. The prize campaign integrates the creative outcomes from the earlier Instant Messaging Apps Stickers Design Contest with social media activities, enabling the public to learn proper cybersecurity knowledge in a fun and relaxed atmosphere, and apply it to daily life. Webinars and seminars were also organised under the campaign to further deepen cybersecurity knowledge of the participants.



School visits and security talks for non-governmental organisations (NGOs)

To promote cyber security awareness and cyber etiquette, we organised a total of 35 visits to primary and secondary schools, tertiary institutions, and NGOs to deliver information security talks to students, teachers, parents, service recipients and staff of NGOs.

InfoSec Tours with RTHK Radio 2

We continued to partner with the RTHK to conduct three InfoSec Tours with topics of “Essential Cybersecurity Awareness and Digital Literacy in the Age of AI”, “Safe Internet Surfing with Netiquette” and “The Pitfalls in Cyberspace”, which delivered information security messages in a relaxing way while promoting the importance of online safety and security.



Cybersec Infohub engagement activities

To encourage the engagement and effective discussion among public and private organisations on cybersecurity, various activities such as sector-specific meeting and networking, technical professional workshops, webinars and seminars were arranged under the Cybersec Infohub partnership programme with affirmative feedback.



Cybersecurity & Diverse Innovation Symposium

We co-organised the “Cybersecurity & Diverse Innovation Symposium 2025” with the CSTCB of HKPF. The Symposium examined a range of topics, including emerging cybersecurity challenges, cross-sector collaboration, and innovation-led defence strategies. It attracted over 600 experts from Hong Kong and the Mainland, representing multiple sectors.



China Cybersecurity Week Hong Kong Sub-forum

We, along with the CSTCB of HKPF, the HKIRC and the Hong Kong Cybersecurity Professional Association (HKCSPA), jointly organised the "China Cybersecurity Week Hong Kong Sub-forum 2025". It brought together over 400 experts and business leaders from the Guangdong-Hong Kong-Macao Greater Bay Area (GBA), who exchanged views on various topics such as emerging threats in cybersecurity and the latest cybersecurity defence technologies, jointly exploring Hong Kong's cybersecurity trends.



Cybersecurity Symposium

We organised the Cybersecurity Symposium in collaboration with the CSTCB of HKPF, the HKIRC and the HKCSPA, aiming at fostering collaboration between public and private organisations and supporting Hong Kong's development as a leading digital economy, thereby strengthening Hong Kong's overall cybersecurity defence and resilience capabilities. Several insightful keynote speeches and panel discussion sessions were held during the symposium. More than 30 experts from the Government, academia, technology, telecommunications, finance, and insurance sectors were invited as speakers and over 1 000 cybersecurity professionals and industry leaders from various sectors attended.



LOCAL AND INTERNATIONAL COLLABORATION

5.1 Local Collaboration

Promoting Cyber Security Information Sharing and Collaboration

We continued to promote and operate the Cybersec Infohub with HKIRC for establishing closer connections among local information security stakeholders. The programme attracted over 3 130 organisations and more than 4 470 representatives from various local sectors as of the end of 2025.

In response to the increasing frequency of cybersecurity threats affecting public and private organisations in Hong Kong and to prepare for the major events held in Hong Kong, we convened special meetings in July, October and November with the Internet Infrastructure Liaison Group and representatives of the cybersecurity industry to discuss enhancements to technical protection measures and risk management strategies.



Nurturing Cyber Security Talents

We continued to support our working partners to organise various programmes and campaigns to groom cybersecurity talents with the latest cybersecurity skills and knowledge, thereby attracting and retaining talents in the cybersecurity industry in a long run, including the following events:

- “Capture the Flag Challenge 2025” by HKCERT
- “Cyber Attack and Defence Elite Training cum Tournament” by HKIRC
- “Cyber Youth Programme 2025” including training courses, competition and a game-aided learning platform by HKIRC

Enhancing Overall Cyber Security Resilience

We also supported our working partners to organise various programmes and campaigns to provide free services and resources for promoting cybersecurity awareness and enhancing defence capabilities among SMEs and public to address emerging threats. GovCERT.HK supported the following initiatives:

- “Cybersecurity Service Providers Connect Programme” co-organised with HKCERT
- “Cyber Security Summit Hong Kong 2025” by HKCERT
- “Cybersec One Programme” by HKIRC
- “Healthy Web” with free web screening service by HKIRC
- “Cybersec Training Hub” with free training resources online by HKIRC
- “Cyber Security Staff Awareness Recognition Scheme 2025” by HKIRC

5.2 Chinese Mainland and International Collaboration

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

GovCERT.HK participated in the following events in 2025::

- 2025 China Cybersecurity Week
- 2025 China Cybersecurity Week Macau Sub-forum
- APCERT Annual General Meeting and Conference
- APCERT Drill with the theme of “When Ransomware Meets Generative AI”
- APCERT on-line training sessions
- NatCSIRT Meeting 2025 and 37th FIRST Annual Conference
- 2025 World Internet Conference Asia-Pacific Summit
- 2025 World Internet Conference Wuzhen Summit

To promote cybersecurity exchange and collaboration in the Guangdong–Hong Kong–Macao Greater Bay Area (GBA), we signed a memorandum of understanding (MoU) last year. We have held regular experience-sharing meetings with the Cyberspace Administration of Guangdong Province and the Cybersecurity Incident Alert and Response Centre of Macao to exchange updates on the latest cybersecurity developments and initiatives, and to discuss priority areas for cybersecurity cooperation among Guangdong, Hong Kong, and Macao.

FUTURE PLANS

GovCERT.HK will continue to enhance cybersecurity awareness, preparedness and resilience among government, industry and public through various initiatives:

- Enhance technical skills, strategies and defensive readiness across government and the public sector via training and attack-and-defence drills to effectively address emerging threats;
- Strengthen collaboration with local, regional, and international cybersecurity partners to support cross-boundary incident coordination and regular information exchange;
- Deepen engagement with stakeholders to deliver programmes supporting the education sector, public organisations, and SMEs in strengthening cybersecurity readiness and resilience, nurturing talent, and promoting cybersecurity awareness across different sectors; and
- Promote the responsible and secure use of AI at work, fostering a sustainable culture of AI safety and cybersecurity readiness across the community.

CONCLUSION

To maintain a secure and resilient cyber environment that supports the Government's digital services and Hong Kong's continued development, GovCERT.HK will continue to strengthen cybersecurity governance, operational preparedness, technical defence capabilities, and community awareness. We will also deepen collaboration with local, regional, and international partners to enhance information sharing, coordination, and collective readiness in response to an evolving cyber threat landscape.



cert@govcert.gov.hk



www.govcert.gov.hk
www.cybersechub.hk
www.cybersecurity.hk
www.infosec.gov.hk