Immediate Release

Cyberport Cybersecurity Incident Task Force Concludes Work

HONG KONG, 2 April 2024 – In response to the earlier cyberattack, Cyberport Board of Directors established a task force ("Task Force") to steer investigation and follow-up work. The Task Force has concluded relevant work and reported to the Board of Directors. Cyberport has also submitted an investigation report to the Office of the Privacy Commissioner for Personal Data (PCPD).

Cyberport has taken the incident very seriously, and soon after the incident occurrence, the Task Force was established to closely follow up on work, including swift enhancement of its defence against hacker attacks, implementation of multiple measures such as fortification of network protection barriers to strengthen capabilities of detecting network attacks and intrusions, leading to successful deterrence of subsequent cyberattacks. It has also engaged professional third-party service providers to conduct regular network security monitoring and ethical hacking, and has increased tools to monitor network security, comprehensively bolstering its defence capabilities against cyberattacks.

Meanwhile, Cyberport has proactively contacted and supported affected individuals to the best of its ability to minimise potential impact. It has promptly provided the known affected and potentially affected individuals with complimentary credit and identity monitoring services to mitigate as many potential risks as possible. The monitoring services have remained effective even after the hacker's dark web was dismantled, ensuring continued maximum protection for affected individuals.

The Task Force investigation also noted room for improvement in internal information security and data management by Cyberport, resulting in reinforcing multiple measures to enhance the calibre and awareness of information system security and data security at all operational levels. Cyberport has also reviewed and strengthened measures for personal information management to ensure compliance with personal information protection principles outlined in the Personal Data (Privacy) Ordinance. Cyberport appreciates PCPD for its valuable advice and concrete suggestions during the process, and will spare no efforts in continuously implementing and enhancing measures for system and data security.

Victor Ng, Director of Cyberport and Chairman of the Cybersecurity Incident Task Force, said,: "Since the incident took place, the Task Force and the management have proactively assessed the situation and promptly reacted by swiftly strengthening network and data protection barriers, effectively preventing subsequent network intrusions. We have also been committed to supporting affected individuals with best efforts to minimise potential impact and have fully cooperated with relevant government departments and PCPD in investigations. Cyberport will continue to enhance cybersecurity measures, strengthening its ability to counter cybersecurity threats, and ensuring that its operations comply with the Personal Data (Privacy) Ordinance. Cyberport will also fortify its internal audit, regularly examine the implementation of information security measures, and report to the Audit Committee under the Board of Directors to uplift governance levels."

Simon Chan, Chairman of Cyberport, said, "In the light of increasingly serious cyberattacks, network and data security protection are top priorities for Cyberport. We will continue to optimise the overall network system and information security strategies, proactively adopt information security measures, and enhance governance at all operational levels under the supervision of the Board of Directors to elevate the capabilities of combating network intrusions and protecting data security.

Additionally, Cyberport will collaborate with cybersecurity partner corporations and community start-ups to jointly expand the cybersecurity ecosystem. Through innovation and technology, we aim to elevate the levels of network and data security at Cyberport, within the innovator community and in Hong Kong as a whole."

For enquiries related to the cybersecurity incident, please contact our dedicated team at infosecurity.cs@cyberport.hk.

###

For media enquiries, please contact:

Cyberport
Cindy Fung
Tel: (852) 3166 3841
Email: cindyfung@cyberport.hk

FleishmanHillard Hong Kong
Silvia Wu / Carmen Yu
Tel:(852) 6773 0217 / 9012 4134
Email: silvia.wu@fleishman.com /
carmen.yu@fleishman.com

About Cyberport

Cyberport is Hong Kong's digital technology flagship and incubator for entrepreneurship with over 2,000 members including over 900 onsite and over 1,100 offsite start-ups and technology companies. It is managed by Hong Kong Cyberport Management Company Limited, wholly owned by the Hong Kong SAR Government. With a vision to be the hub for digital technology, thereby creating a new economic driver for Hong Kong, Cyberport is committed to nurturing a vibrant tech ecosystem by cultivating talent, promoting entrepreneurship among youth, supporting start-ups, fostering industry development by promoting strategic collaboration with local and international partners, and integrating new and traditional economies by accelerating digital transformation in public and private sectors.

For more information, please visit www.cyberport.hk