Version: 1130 25 January 2022

Cybersecurity Incident – FAQ

Common questions from members

1. What happened?

We suffered a cyber incident disrupting access to the Institute's server infrastructure in late December 2021.

Some of the electronic files saved on the server were encrypted without our permission. We have been unable to open, read or edit the encrypted files, but have been working with relevant parties to resolve this.

We are treating this incident as a potential data breach as members' personal information may have been compromised, and we have notified all members of this matter via email and reported to the Hong Kong Police and the Hong Kong Privacy Commissioner for Personal Data.

2. Have you reported this incident to the Police? What have they found?

The incident has been reported to the Hong Kong Police and other authorities, including the Hong Kong Monetary Authority, the Hong Kong Privacy Commissioner for Personal Data, and the Hong Kong Computer Emergency Response Team.

Investigation is still underway.

3. Any signs of our data being stolen and used in unauthorised activities? What types of personal data may have been compromised?

We are treating this incident as a potential data breach as members' personal information may have been compromised, and we have notified all members of this matter via email.

As of now, there is no evidence of any unauthorised use of members' personal information. No related suspicious activities or data leakage incidents have been identified or reported to us so far.

We have engaged a cybersecurity consultant to monitor threat actors' websites as well as other common websites in the dark web. At this point, there has been no reported instances of the Institute's documents or its members' personal information being released in the public domain.

The personal information involved may include members' names, HKID numbers and other information that they have previously submitted to the Institute for course enrolment or activity registration.

This incident is still being investigated by the Institute and the bodies involved and we shall keep our members updated on the latest findings.

4. How come you can let this happen? Didn't you have strong cybersecurity measures in place?

We take cybersecurity very seriously.

We sincerely apologise for the inconvenience and concerns caused to our members.

We have engaged a cybersecurity consultant to investigate this incident. Although the breach has already been contained, we are still looking to mitigate the impact as far as possible.

We remain committed to stepping up our cybersecurity measures and enhancing our IT infrastructure to mitigate risks.

5. Which services have been suspended due to this incident?

To safeguard our members' information security when using our online system, we have suspended some of the member-only services and online activities until further notice.

These suspended services include online registrations and MyHKIB membership services.

The operation of the HKIB office and FLEX Learning remains normal. Public access to the HKIB public website is not affected.

In order to reduce the impact of the incident on members, we will continue to provide services through offline channels.

We sincerely apologise for the inconvenience caused to our members.

6. If I am asked to submit or change my personal information on the HKIB platform, how can I tell the request is authentic?

Members are reminded to beware of phishing emails and fraudulent websites purporting to be from HKIB. We will never send you emails with an embedded link asking you to share your personal information. Data update is always carried out via HKIB official website www.hkib.org, where members are allowed to access MyHKIB.

If you're ever contacted by anyone asking you to share your personal information, or notice suspicious activity related to your HKIB membership or activities, please contact us on (852) 2153 7800 or cs@hkib.org immediately.

7. How long will it take to resume all the suspended services? When can I use MyHKIB again?

Although the breach has already been contained and the system vulnerabilities have been addressed, our cybersecurity consultant has reported that it will take more time to achieve any data recovery.

We will inform our Members and resume MyHKIB as soon as we are certain of the security safeguarding members' information when using our online system.

We shall keep our members updated as soon as any development happens relating to this.

8. I work in one of the banks in Hong Kong. Have I been affected by this incident? Will I be informed of further development? How would I know whether my employees/ colleagues have been affected by this incident?

We are not in the position to comment on any individual case.

We have informed all our individual and corporate members of this incident via email communication in early January.

As of now, there is no evidence of any unauthorised use of members' personal information. No related suspicious activities or data leakage incidents have been identified or reported to us so far.

We have engaged a cybersecurity consultant to monitor threat actors' websites as well as other common websites in the dark web. At this point, there has been no reported instances of the Institute's documents or its members' personal information being released in the public domain.

9. I suspect my personal data has been stolen due to this incident. Who should I contact about my situation?

Please contact us on (852) 2153 7800 or cs@hkib.org about your situation.