LEWIS SILKIN
世勤律師事務所

Auctioning off privacy

A well known auction house with operating in Hong Kong was recently hit by a major cyberattack, resulting in a shutdown of its website just days before its spring auctions began. The ransomware group, RansomHub, claimed to be behind the cyberattack and threatened to release sensitive personal information of at least 500,000 clients worldwide unless a ransom was paid. RansomHub wrote on the dark web that they had attempted to come to a reasonable resolution with the auction house, but the auction house ceased communication midway through. RansomHub added that it was clear "*…if this information is posted they will incur heavy fines from GDPR as well as ruining their reputation with their clients …*".

In response to the cyberattack, the auction house said it was notifying privacy regulators and enforcement agencies and the affected individuals. The auction house emailed its clients acknowledging that a cyberattack had took place and stated only identification data, and not financial or transaction data, were leaked. In Hong Kong, the auction house notified the privacy watchdog, the Office of the Privacy Commissioner for Personal Data, regarding the data breach. The compromised data included the name, date of birth, address, passport number, gender and nationality of around 8,400 of its clients in Hong Kong.

This incident underscores the increasing threat of cyberattacks and highlights the serious reputational damage a data breach can bring.

Threat actors launch cyberattacks for all sorts of reasons, deploying various tactics, like malware attacks, social engineering scams, and password theft, to gain unauthorised access to their target systems. Some companies may decide to negotiate with the threat actor who is extorting money and pay the ransom demanded in exchange for the return of the stolen data. It is not uncommon for the threat actor to notify their victim of the weaknesses in their systems and how they can avoid future incidents arising again.

With the growing threat of cyberattacks, there is a need to have stronger data protection measures to prevent unauthorised access and use of personal data. Companies should devise a clear contingency plan in the event a threat actor strikes which should set out the immediate steps that need to be taken. Such steps should include, how and who to notify about the data breach, who will lead the crisis communications response to a cyberattack, and what advisors are already retained or need to be engaged to support that response. Whilst there is currently no mandatory data breach notification regime in Hong Kong, data users are encouraged to adopt a proactive approach and notify the Privacy Commissioner and the affected individuals upon the discovery of a data breach. This is particularly the case when real risk of harm is reasonably foreseeable in a data breach.

If you need assistance with any data protection issues, please contact a member of our team.

Author

Jezamine Fewins
Partner and Head of Litigation

+852 2972 7114
jezamine.fewins@lewissilkin.com

Find out more