Toying with cyber security

VTech and Hong Kong's cyber laws

VTech is a multi-billion-dollar global supplier of electronic toys and learning products for children, and reportedly the world's biggest manufacturer of cordless telephones. In short, it is a giant company producing high-tech electronic goods – surely, you might think, capable of fending off a cyber-attack.

However, in November 2015, the company's learning products store was hacked, leading to a massive data breach in which millions of customers' personal information, including children's profiles, was compromised[1]. On 1 December 2015, the Office of the Privacy Commissioner for Personal Data in Hong Kong (Privacy Commissioner) announced that it had launched an investigation[2]. A 21-year-old man has been arrested in the UK in connection with the incident[3].

Unfortunately, VTech is not an isolated case – reports of cyber-crime in Hong Kong are increasingly regular. Recent incidents include:

- In May 2015, Bank of China (Hong Kong) and the Bank of East Asia were reportedly hit by distributed denial of service (DDoS) attacks demanding bitcoin ransoms[4].
- In July 2015, it emerged that Mandarin Oriental's Hong Kong hotels had suffered an eight-month-long cyber-attack targeting customers' credit cards[5].
- In August 2015, a "spear phishing" campaign was reportedly carried out on Hong Kong media organisations, apparently focusing on those publishing pro-democracy material[6].

Figures released by the Hong Kong Police confirm that cyber-crime is rising dramatically. In 2014, reported financial losses arising from cyber-crime in Hong Kong were HK$1.2bn[7], up from HK$917m in 2013. The figure for 2009 was only HK$45.1m.

The problem is likely to be even worse than these statistics suggest. Since Hong Kong law does not generally require that data breaches be reported, it is likely that many Hong Kong businesses are suffering data breaches but, mindful of potential reputational damage, are choosing not to disclose them.

The reasons for this sharp increase are hard to pin down. Perhaps, the simplest explanation is that adoption and use of computer technologies – including convenient and cost-effective developments such as cloud computing and "bring your own device" initiatives – have been increasing more quickly than awareness and understanding of

Any comments or queries?

Jonathan Cary
Partner
+852 2216 7173
jonathan.cary@rpc.com.hk

Ben Yates
Senior Associate
+852 2216 7169
ben.yates@rpc.com.hk

1. vtech.com.
2. pcpd.org.hk.
3. thetimes.co.uk.
4. thestandard.com.hk.
5. themandarinoriental.com.
6. fireeye.com.
7. infosec.gov.hk.

the risks involved in using them. At the same time, readily-available, easy-to-use, hacking "kits" are making simple but effective hacking techniques available to anyone in the world with a basic level of IT knowledge and access to the internet.

Hong Kong's cyber regime

Recognising the need to do something to address the rapid growth in cyber-crime, in December 2012, The Hong Kong Police established a dedicated Cyber Security and Technology Crime Bureau[8]. However, although significant resources have been thrown into the Bureau, the Police face a very steep challenge in attempting to keep up with constantly-evolving, and often borderless, technology crime.

In addition, the Hong Kong Police's powers of investigation into cyber-crime are constrained by a relatively restrictive and outdated set of legal provisions, including the Telecommunications Ordinance[9] (sections 24, 27 and 27A in particular), the Crimes Ordinance[10] (section 161) and the Interception of Communications and Surveillance Ordinance[11]. The Hong Kong Government's reluctance to expand the Police's powers reflects the fact that Hong Kong, along with many jurisdictions across the world, is grappling with the potential clash between on the one hand, Police powers of surveillance and investigation, and on the other, core principles such as freedom of speech and privacy.

For the time being at least, the emphasis in tackling cyber-crime is on ensuring that those handling sensitive data legally do so with adequate care. In this regulatory environment, obtaining the necessary legal and practical advice is a must.

The Personal Data (Privacy) Ordinance (PD(P)O) and the Privacy Commissioner – cornerstones of Hong Kong's cyber regime

The PD(P)O[12] does not directly address cyber-criminals, but rather holds those handling others' "personal data" accountable for any failure to take adequate security measures to prevent data breaches. The Privacy Commissioner, as VTech will be aware, has broad powers to enforce the PD(P)O's personal data protection regime. In practice, this makes the PD(P)O one of Hong Kong's most effective regulatory tools for preventing cyber-crime. Recent amendments to the PD(P)O have introduced new offences, along with stiffer penalties for breaches of existing provisions[13].

Under the PD(P)O, "personal data" is defined very broadly. It includes any data relating directly or indirectly to a living individual (a data subject) in a form in which access to or processing of the data is practicable that can be used directly or indirectly to ascertain the identity of that person (PD(P)O, s. 2). Any entity that collects or controls the collection of personal data (a data user) must comply with the six "Data Protection Principles" (DPPs) set out in Schedule 1 to the PD(P)O.

Under DPP 4 (security of personal data), "[a]ll [reasonably] practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use ...". The steps required to be taken depend on "the kind of data and the harm that could result if any of those things should occur".

The Privacy Commissioner has published a number of guidance notes to put some flesh on the bones of the PD(P)O and the DPPs. In particular, the "Guidance on data Breach Handling and the Giving of Breach Notifications", issued in 2010 and revised in October 2015[14], provides guidance on how the risk of harm should be assessed and when "data users" should make data breach notifications. The "Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry", published in October 2014, provides financial institutions with practical guidance on how the PD(P)O applies to the

8. police.gov.hk.
9. legislation.gov.hk.
10. legislation.gov.hk.
11. legislation.gov.hk.
12. legislation.gov.hk.
13. pcpd.org.hk.
14. pcpd.org.hk.

collection, holding, processing and use of customer data[15].

Investigating potential breaches
Although the Privacy Commissioner has published guidance on when data breach notifications should be made, there is in fact no legal obligation on a data user to report a data breach to the Commissioner. Most cases, therefore, end up in the hands of the Privacy Commissioner as a result of complaints made by data subjects. In 2014-2105, the Privacy Commissioner received 1,690 complaint cases. Of these, 193 related to data security, and a record 223 complaints were made relating to the use of information and communication technology – a dramatic 89% year-on-year increase[16].

When the Privacy Commissioner receives a complaint about a potential breach of the PD(P)O, he is obliged (except in certain circumstances) to carry out an investigation (PD(P)O, s. 38(i)). The Privacy Commissioner may also carry out an investigation where he has reasonable grounds to believe that a breach has occurred (PD(P)O, s. 38(ii)).

In carrying out his investigations, the Commissioner has the power to enter premises forcibly (with a warrant) to carry out an inspection (PD(P)O, s. 42). Obstructing or knowingly misleading the Commissioner is a criminal offence with a maximum penalty of six months in jail and HK$10K fine (PD(P)O, s. 50B).

Once his investigation has concluded, the Privacy Commissioner may issue recommendations to the data user to promote compliance with the PD(P)O, serve an enforcement notice on the data user requiring remedial measures to be taken by a specified date and/or issue a public report on the investigation (PD(P)O, ss. 47 & 48).

Taking action for breaches of the PD(P)O
Breach of the DPPs is not in itself an offence under the PD(P)O. However, if an enforcement notice issued by the Privacy Commissioner is not complied with, this will constitute a criminal offence, with a maximum penalty on first conviction of two years' imprisonment, a fine of HK$50,000 and a daily fine of HK$1K for continued contravention. For a second or subsequent conviction, the maximum fine increases to HK$100K and HK$2K per day of continued contravention (PD(P)O, s. 50A). The Privacy Commissioner may refer cases to the Hong Kong Police for prosecution. In 2014-2015, 18 cases were transferred or reported to the Police or other authorities[17].

Apart from criminal sanctions, the PD(P)O also provides data subjects with a right to bring civil court proceedings for damages, including injury to feelings, by reason of contravention of the PD(P)O (PD(P)O, s. 66). The Privacy Commissioner has the power to grant legal assistance to any person who intends to institute proceedings to seek compensation, although he is unlikely to do so unless the case raises a particular "question of principle" or if he considers that it is "unreasonable, having regard to the complexity of the case and your position in relation to the relevant data user, to expect you to deal with the case unaided" (PD(P)O, s. 66B). In most cases, it would be advisable to hire a lawyer to handle the civil proceedings on your behalf.

Data breach in the finance industry – the Securities and Futures Commission (SFC) and the Hong Kong Monetary Authority (HKMA)
The SFC has wide-ranging powers to investigate licensed and registered persons where it has information suggesting that they are not "fit and proper" to remain licensed or registered. A failure to maintain adequate IT systems and controls could constitute a breach of the SFC's Code of Conduct and lead to an SFC investigation. This is a very real risk. On 27 January 2014, the SFC issued a circular urging licensed corporations to "review and, where appropriate, enhance their IT security controls and other preventive and detective measures to reduce internet hacking risks and the potential damage arising from an

15. pcpd.org.hk.
16. pcpd.org.hk.
17. pcpd.org.hk.

internet attack"[18]. Another circular followed on 27 November 2014, in which the SFC highlighted the cyber-security risks facing the financial industry[19]. A failure to give heed to the SFC's warnings may well lead to stiff penalties for licensed corporations.

In tandem with the SFC and the Privacy Commissioner, the Hong Kong Monetary Authority (HKMA) has also released circulars on data security. On 14 October 2014, the HKMA issued a circular to Authorised Institutions setting out recommended controls for preventing and detecting the loss or leakage of customer data[20]. In its 15 September 2015 entitled "Cyber Security Risk Management"[21], the HKMA made clear its expectations that the board and senior management of Authorised Institutions should take measures to ensure that adequate security systems were in place. The HKMA has also published a number of press releases warning the public of the dangers of technology fraud[22].

In practice, both the SFC and the HKMA operate in cooperation with the Privacy Commissioner in identifying and investigating data security failings. In 2014-2015, the Commissioner received 314 complaints in relation to the banking and financial sector[23].

Taking measures to guard against cyber-crime

The VTech data breach should serve as a warning to all Hong Kong businesses. The international nature of the breach, and the negative press arising from it, demonstrate the serious consequences that can flow from the activities of hackers and cyber-criminals. With the now almost-total computerisation of personal information, and the widespread practice of storing and sharing such information online, the risks have never been greater.

It is not surprising that Hong Kong's regulators are becoming increasingly vocal regarding the steps that should be taken to address cyber-crime. The guidance notes published by the Privacy Commissioner, the SFC and the HKMA are valuable sources of reference for all organisations, including those outside the financial sector. That guidance will, however, need to be adapted to a business's specific needs, and the measures taken will need to be targeted and affordable.

For a business handling sensitive data – and that means almost any business – a range of measures should be taken to guard against cyber-crime. Those measures may include:

- Put in place a privacy policy that complies with the PD(P)O (as amended). Many organisations either have no privacy policy at all or the policy is inadequate. Privacy policies and procedures should be updated to take into account the recent amendments to the PD(P)O – failing which there could be serious consequences, including criminal sanctions.
- Ensure that your staff are adequately trained in data security. Many cyber-attacks, such as phishing and wire fraud, can be prevented through staff training and the adoption of stringent security procedures for dealing with external parties.
- Put in place measures to restrict access to data to those employees who require it. Although much publicity has been given to cyber security threats emanating from terrorist organisations, hostile foreign governments, organised criminals and "hacktivists", the reality is that a large proportion of those criminals are much closer to home. In particular, disgruntled employees pose a huge security risk, particularly for organisations that have not put in place adequate information barriers.
- Ensure that your website and IT systems are (and remain) up-to-date and that any vulnerabilities are addressed. Many hacking techniques exploit basic structural flaws found in old websites that have not been updated.
- Consider obtaining insurance cover for cyber-related risks. Such policies are becoming increasingly popular as a result of the uncertain risks posed by cyber-crime

18. sfc.hk.
19. sfc.hk.
20. hkma.gov.hk.
21. hkma.gov.hk.
22. hkma.gov.hk.
23. pcpd.org.hk.

and the clear signal from Hong Kong's regulators that adequate measures must be taken to keep data secure.

- Licensed corporations should follow the SFC's recommendations as set out in its circulars dated 27 January 2014 and 27 November 2014.
- Authorised Institutions should adopt the HKMA's guidance set out in its circulars dated 14 October 2014 and 15 September 2015.

Even with all the right measures in place, however, a data breach could still occur. In those circumstances, it is absolutely crucial that quick and effective action be taken to identify what has happened and to limit the damage arising from the incident.

Without the necessary professional guidance, putting in place the right measures for your business can be a difficult and costly process. RPC can conduct a thorough review of your policies and procedures to ensure that they comply with the PD(P)O. In the event of a data breach or other cyber-attack, we can provide you with the emergency legal advice you need to minimise the financial, commercial and reputational damage. If you find yourself facing investigation by the Privacy Commissioner or the SFC, or civil action in the Hong Kong courts, our experience in dealing with such matters can assist.

For regulatory reasons, RPC operates as a registered foreign law firm in Hong Kong and in association with Smyth & Co.

About RPC

RPC is a modern, progressive and commercially focused international law firm. We have 78 partners and over 600 employees based in London, Hong Kong, Singapore and Bristol.

"... the client-centred modern legal services business."

At RPC we put our clients and our people at the heart of what we do:

- **Best Legal Adviser status every year since 2009**
- **Best Legal Employer status every year since 2009**
- **Shortlisted for Law Firm of the Year for two consecutive years**

We have also been shortlisted and won a number of industry awards, including:

- **Winner – Law Firm of the Year – The British Legal Awards 2015**
- **Winner – Competition and Regulatory Team of the Year – The British Legal Awards 2015**
- **Winner – Law Firm of the Year – The Lawyer Awards 2014**
- **Winner – Law Firm of the Year – Halsbury Legal Awards 2014**
- **Winner – Insurance and Reinsurance Law Firm of the Year, Hong Kong – Finance Monthly Law Awards 2015**
- **Winner – Hong Kong – Leading Litigation Lawyer of the Year – ACQ Global Awards 2015**
- **Nominated – Maritime and Shipping Law Firm of the Year – Hong Kong – Lawyer Monthly Legal Awards 2015**
- **Winner – Commercial Team of the Year – The British Legal Awards 2014**
- **Winner – Competition Team of the Year – Legal Business Awards 2014**

"... they are my firm of choice in Asia." **Chambers Asia Pacific 2015**

Areas of specialism

- Banking
- Commercial
- Commercial Litigation
- Competition
- Construction
- Corporate
- Employment
- Insurance
- Intellectual Property
- Marine and International Trade
- Media
- Outsourcing
- Private Equity
- Real Estate
- Regulatory
- Reinsurance
- Tax
- Technology

15587

Tower Bridge House
St Katharine's Way
London E1W 1AA
T +44 20 3060 6000

Temple Circus
Temple Way
Bristol BS1 6LW
T +44 20 3060 6000

11/F Three Exchange Square
8 Connaught Place
Central Hong Kong
T +852 2216 7000

8 Marina View #34-02A
Asia Square Tower 1
Singapore 018960
T +65 6818 5695