Reacting to and managing cyber security threats

ON 1 MARCH 2017, KROLL AND PINSENT MASONS WELCOMED A GROUP OF professionals in Singapore with responsibility for managing and protecting their organisations' data to discuss the reality of cyber security threats in Asia. The discussion was conducted under Chatham House rules to facilitate openness and a candid exchange of personal experiences and opinions.

Some of the observations of the group were as follows:

1 There is a fundamental lack of awareness of the reality of the risk of cyber attack in Asia. Cyber security is viewed as a problem for the government to sort out, or something that only impacts the West. There is also a view that you will not be subject to cyber attack if you are avoiding involvement in online behaviour that might be considered "risky" (such as frequenting unsavoury websites).

In a society which has massively interlinked infrastructure and IT systems, as the majority of leading Asian cities do, this shows that many organisations are blind to the pervasive threat of cyber attack. IT security is rarely debated at the executive level by organisations in Asia, and if it is then this takes place only because of impetus from a head office based in the U.S. or Europe. CISOs are rare in Asian organisations, and many data protection policies are unsophisticated, existing only to tick a statutory or regulatory box.

2 Companies are waiting for regulators to force them to act. In the financial sector, the regulators are more proactive in compelling organisations to manage the risk of cyber attack, but regulators in other sectors have not yet forced the issue. This is coupled with a population which may not take data privacy as seriously as counterparts in other jurisdictions, with individuals often willingly sharing ID details or passport numbers in exchange for a promotional offer or other trinket. Again, there is a perception that cyber attacks happen to other people and rarely target Asian companies. This is of course not true.

3 Where cyber attacks are occurring, organisations are either unaware they have suffered a data breach or, worse still, are aware of the breach but choosing not to disclose it to customers. This "sweeping under the carpet" of cyber issues means that many if not the majority of cyber attacks in Asia are undetected or unreported.

4 Cyber readiness is viewed as another item on the balance sheet to be avoided or reduced. Small companies would rather not increase their IT spend to deal with cyber security concerns. Unless companies operate in a regulated environment, a cyber risk assessment is seen as an unnecessary cost. Outside of the IT sector the understanding of the nature and type of various cyber attacks is very low indeed.

5 Asia is a mishmash of jurisdictions and rules: different countries take different approaches to cyber security. Whilst some jurisdictions take the issue more seriously (such as South Korea), in other jurisdictions (such as China, Hong Kong, and Singapore) the general attitude towards cyber security outside of a regulated environment is one of complacency.

6 The majority of organisations have a health and safety policy and conduct regular fire drills. So why not look after the health and safety of your systems and data and conduct regular cyber drills. The corporate spend on ineffective antivirus software could be repurposed to deal with a more up-to-date cyber risk policy. Prevention of and readiness for cyber attack should be as important as any other organisation's policies for the protection of their businesses.

7 Ignorance of cyber security issues is rife, so education (for all employees) is key. We have a duty to safeguard the data of our customers and employees, and that duty can only be discharged by ensuring that everyone is aware of the risk and how to mitigate it. Education is key.

SELF-CHECK QUESTIONS

- ☐ Do we have a response team and plan?
- ☐ Have we set up key relationships?
- ☐ What type of data are we keeping?
- ☐ How do we secure our data?
- ☐ Are we testing ourselves?
- ☐ Do we have cyber insurance?

Jonathan Fairtlough
Managing Director, Kroll

M: +1 213 598 4181
jfairtlough@kroll.com

Paul Haswell
Partner, Pinsent Masons

D: +852 2294 3315
M: +852 5964 2050
paul.haswell@pinsentmasons.com

Gregory Michaels
Associate Managing Director, Kroll

T: +1 201 978 1546
gregory.michaels@kroll.com

Arwen Berry
Senior Associate,
Pinsent Masons MPillay

D: +65 6305 8494
arwen.berry@pinsentmasons.com

Tam Huynh
Senior Director, Kroll

T: +65 6645 4526
tam.huynh@kroll.com

CONTACT

For more information, email or visit us online:
asia@kroll.com | T: +65 6645 4947

kroll.com

Kroll

RPT KCS APAC_REACTING TO CYBER SECURITY THREATS_APR 2017