Photo: Thinkstock

BYOD – Understanding and Dealing with Data Security Risks

By Chris Davis

- **Bring Your Own Device, or BYOD, is a growing practice which allows employees to connect their personal devices, such as a smartphone, laptop or tablet, to the corporate network so that they can access business and collaborative applications.**

- **By allowing employees to access corporate data on their personal devices, IT departments are grappling with the issue of security. This can put a company's business systems and reputation at risk and the process requires properly implemented and managed BYOD guidelines and user policies.**

As the lines between work-related IT and personal technology continue to blur in the age of the "anytime, anywhere" workplace, BYOD practices provide convenience for both employees and employers. However, the sheer range and complexity of devices that can be connected to company networks increases the risk of misuse, loss, or unauthorised disclosure of organisation-collected data, whether through employees losing devices or by compromising cybersecurity.

According to a recent *Cyber-security –Defending your future* report by HR consulting firm Robert Half, one in three Hong Kong Chief Information Officers believes that a lack of employee knowledge and skills regarding data security is the most significant security risk their organisation will face in the next five years. With nearly three-quarters (74%) of local CIOs allowing employees to access corporate data on their personal devices, the security risks of BYOD have become a top priority. The research shows that nearly all (99%) CIOs are taking steps to protect their company from potential data breaches in light of the threat posed by BYOD. In addition, 57% have deployed mobile device management technologies to enforce enhanced protection on employee mobile devices; 56% require

workers to sign an acceptable use policy; 51% are providing training to their staff on maintaining security while using their mobile devices and 45% are using authentication software. The growing focus on security is meanwhile generating an increased demand for IT security specialists with the niche skills needed to protect companies against data security risks. But 98% of Hong Kong CIOs say it is challenging to source technology professionals, with 23% stating that professionals with mobile security skills are in top demand.

Managing the risks

Annie Cheung, general manager with information technology and telecommunication (IT&T) resourcing company Peoplebank, says that, as BYOD becomes an increasingly common practice in Hong Kong, as it is elsewhere in the world, different industry sectors are adopting different solutions to protect their network safety. For example, Cheung says business sectors including banking, government, legal and retail, which work with a lot of sensitive or personal data, tend to have policies in place aimed at reducing the risk to IT systems. In contrast, Cheung notes, start-ups and smaller businesses – typically enterprises with fewer than 10 employees and an open culture and flat organisational structure – are inclined to be less stringent about BYOD security. Meanwhile, manufacturing organisations are starting to focus more on improving their BYOD polices. Breach of security and loss of sensitive/ confidential information are the most risky components of adopting BYOD practices, Cheung says.

One solution employers with perceived high-risk network security are implementing is to provide employees with a company smartphone, rather than allow them to use their own personal devices. Cheung says the approach makes it easier to detect unusual activities and potential threats, although this approach can potentially conflict with the employee's personal privacy protection rights. Mobile device management (MDM) delivered as a cloud-based service is another solution that broadens the scope of BYOD risk mitigation. According to Cheung however, MDM solutions may not cover all areas of IT security. For example, companies may effectively disable confidential data if a phone is lost or stolen, but might not have the necessary technology capabilities to prevent hacking.

Implementing solutions

Cheung recommends having a formal BYOD policy in place which should include a set of practices and requirements in the form of a manual clearly stating user guidelines and technical requirements for using mobile devices and what course of action to take if a device is lost or stolen. "Communication is key," Cheung says. "Regardless of the BYOD security implementations put in place, they must be transparent to the employee and employees must be made aware of their own rights and obligations," she stresses. This requires clear statements that explain consequences and regular training programmes to address BYOD.

To ensure BYOD practices are aligned with company-wide interests, policies should be constructed through multiple-department collaboration, encompassing IT, HR, security and legal. The programme should also meet the needs of employees, not just the preferences of IT personnel. Otherwise, says Cheung, employees may circumvent data-protection safeguards in order to be more productive or streamline their own user experience. For companies thinking of devising a BYOD policy, Cheung

says it is important to be clear who is responsible for securing the device and educating employees about the risks and responsibilities that BYOD practices involve. Because the BYOD policy is an important part of an employee's engagement with an employer, Cheung says HR needs to play a key role in the education process. For instance, HR should take responsibility for explaining policies and what precautions to take. But in the event of a security breach, it should be the IT department that provides the technical solutions.

If BYOD solutions are implemented by an external IT provider, Cheung says, the provider needs to conduct training sessions for employees. In addition, training sessions need to be supported by a regular BYOD policy and practices review to make sure all procedures are outlined and clearly defined to match the demands of the business and possible changes of risks.

With many younger members of the Hong Kong workforce attached to their personal devices and using them as a matter of habit, they can be unaware of the potential hazards associated with their BYOD activities. Cheung recommends that even if employers have not formally specified that employees can use their own devices or software for work, companies should be aware that this may still be happening and they should protect themselves. "By having clear BYOD strategies in place, staff can work flexibly, which enhances satisfaction and boosts productivity and mayeven reduce attrition," notes Cheung. Moreover, Cheung says, a well-implemented BYOD strategy can also benefit the bottom line through cost-saving on hardware/software and spending on device maintenance.

Protecting personal privacy

In allowing BYOD practices, Stephen Wong Kai-yi, Hong Kong's Privacy Commissioner for Personal Data, notes that a company is effectively transferring organisation-collected personal data from a secured corporate system to what is likely to be an employee's less secure device, over which the organisation has far less effective control. "Lack of control may lead to data privacy risks such as over-retention of personal data, unauthorised change of data use and transfer, security breaches or non-fulfilment of data access requests," says Wong, who cautions that even though the personal data is stored on a device owned by the employee, the organisation remains fully responsible for compliance with the Personal Data (Privacy) Ordinance and the requirements of the Data Protection Principles (DPPs) with respect to personal data.

The Privacy Commissioner recommends employers establish controls as to how organisation-collected personal data is accessed and used by its employees. "It is important for an organisation to note that BYOD equipment contains private information about employees, their family members or other individuals," Wong says. Any protection measures implemented by the organisation should respect private information. To strengthen compliance and protection levels, Wong suggests employers implement a combination of measures. These should include using a dedicated username and password in addition to screen locks; data encryption methods appropriate to the sensitivity of the personal data; criteria by which an organisation decides what information and apps can be accessible by BYOD equipment; mechanisms by which an organisation may monitor the compliance of the BYOD policy and practice; and the consequence of non-compliance. A mechanism for assessing the integrity of a device, especially detecting if the device has been compromised at the platform level, is also recommended. Wong believes that communicating an organisation's BYOD policy through employee training is particularly important. "It is important that employees and management understand their respective rights and obligations when using their own devices for business purposes," says Wong. iHRM

What makes an effective BYOD policy

1. **A manual of practices and requirements for using mobile devices.**
2. **Regular training programmes to address BYOD.**
3. **Inter-department collaboration to meet the needs of employees.**
4. **HR should explain to employees the company's policy and what precautions to take.**
5. **IT department should provide technical solutions.**
6. **A regular policy-and-practices review to match the demands of the business and possible changes of risks.**