RISK INSIGHTS Technology

Crendon Insurance Brokers

Is BYOD Right for Your Company?

More and more staff—especially the young, technologically-savvy—are no longer satisfied with company-issued tools to get the job done. Known as Bring Your Own Device (BYOD), businesses are finding that employees want to swap company equipment in favour of personally owned devices, such as laptops, tablets or smartphones that they are more comfortable using.

This is largely a reversal from the past, when businesses were generally the first to adopt cutting-edge technology, and consumers followed. Consumerisation of information technology, another name for BYOD, is all part of the increasing influence of consumer technology in the workplace. To determine if a BYOD approach is right for your company, first familiarise yourself with the advantages and risks of BYOD.

BYOD Advantages

BYOD can be a money-saver for companies, reducing the amount spent on hardware and software purchases, maintenance and the cost of training employees to use the equipment. Allowing personally owned devices could save thousands of pounds in up-front IT hardware costs for new employees, especially for rapidly expanding companies, because employees buy and maintain their own equipment. Companies can choose to compensate them by subsidising or reimbursing their purchases, or by offering flexible work schedules and the ability to work remotely.

In addition to saving money, BYOD can be effective for recruiting and retaining staff. With freedom to choose the technology they are comfortable with, employees are more productive and satisfied with their jobs.

BYOD Risks

While BYOD saves some companies money, others could end up spending a lot more. Businesses that require the standardisation of their applications, hardware and operating systems—meaning that some equipment must be integrated with others—could actually increase IT management costs if personally owned devices were added to the mix.

Adopting BYOD exposes companies to two major risks: IT security risks and data loss. This alone may be enough to compel a company to ban BYOD altogether. Are these risks worth the benefits?

Employees are allowed to use their own devices for business purposes at 75 per cent of companies.

Risks to Network Security

Personally owned devices usually don't have the same bulletproof security technology that your company computers have. One risk is authentication, which is how you allow users to access your network. Since your IT department doesn't control the employee's device, you must find a way to authenticate the user. Not to mention, if the personal device doesn't have malware protection, Trojans, spyware and other malware attacks can be introduced to your network.

The content of this Risk Insights is of general interest and is not intended to apply to specific circumstances. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.

Is BYOD Right for Your Company?

Mitigating the IT Security Risk

Security threats are serious, but that doesn't mean you should forgo adopting BYOD. Your IT department can help mitigate the risks with the following:

- Keeping track of which devices are corporate-issued and which are employee-owned.
- Installing digital certificates on each personal device so it can be authenticated before the employee uses it to log in to your network.
- Ensuring that the company Wi-Fi network is able to handle the increased number of Wi-Fi devices that access it so that it won't negatively affect the network's performance.
- Creating an Acceptable Use Policy, defining the rules for what employees should and should not do when they access your network, regardless of whether they use company computers or personally owned devices.

Risks to Company Data

In addition to IT security, a data breach due to lost, stolen or insecure devices is a threat that should not be ignored. Saving money and keeping employees happy are important, but losing confidential or proprietary company data could result in a tarnished reputation, lost customers and costly fines and legal actions. Especially if employees work with sensitive customer data, such as personally identifiable information, BYOD could increase the risk of a data breach.

Can you trust that your employees will protect your data? Inform them that while the device is their own, the data belongs to the company. The line between separating company files from personal files on personal devices can get blurry, increasing the chances that company data could be mixed up with personal data. Be aware that employees who save company data on personal cloud storage sites, such as Google Docs®, Facebook® and YouTube®, increase the risk of sharing or streaming content to unauthorised viewers.

How focused is your staff? Keep in mind BYOD could also result in decreased productivity, as employees are more likely to distract themselves with surfing the Web or taking care of personal business on their own devices than they are on company devices.

Mitigating the Risk of Data Loss

In deciding whether or not to adopt BYOD, focus on protecting your data and mitigating the risk of a data breach. Work with your IT department to create a BYOD policy that includes:

- Installing remote wiping software on the employee's personal device in case the device is lost or stolen. Inform employees that remote wiping may cause their personal data, such as pictures and contacts, to also be erased.
- Educating and training employees on how to safeguard company data when they access it from their own devices.
- Informing employees about the protocol to follow in case their devices are lost or stolen.

Smart Risk Management: Create a BYOD Policy

Balancing the risks while keeping employees happy is a challenge. Many companies make the mistake of adopting BYOD without putting a formal policy in place, increasing the chances of BYOD abuse.

Work with your IT department to incorporate the security and data loss risk mitigation into your policy. You may also want to consult your legal department about adding disclaimers, such as confiscating employee-owned devices in case of litigation.

Once the policy is in place, inform your employees about which personal devices your company will and will not support. Educate them about the importance of IT security and protecting company data on their devices. Working on a personal device should be no different from working on a company computer.

Contact **Crendon Insurance Brokers Ltd** for more information on managing BYOD risks.