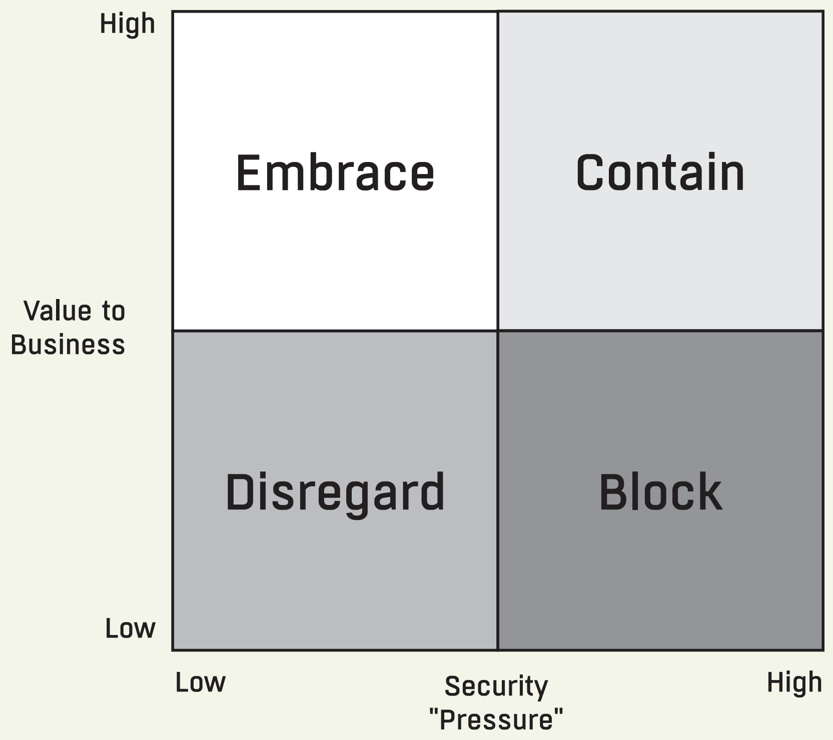
How not to B(ring) Y(our) O(wn) D(isaster)

Security vendors whip us in to a frenzy of paranoia when it comes to keeping our businesses safe. Their argument, however, has moved from prevention to enablement as a result of the BYOD trend, which crosses the boundaries of storage, security, mobility and content. With many organisations recognising the benefits of BYOD but struggling with the mindshift, we turned to BYOD expert **George Ferns,** to give us a pragmatic run-down on what we need to know about BYOD and how to manage it……



Determine your BYOD strategy. Source: Gartner 2013

Today many organisations are faced with the challenges posed by employees using their own devices on the company network. Those who I have spoken to recently feel that the issues are too complex and they are not sure how to tackle this new beast. As a consequence, they are putting BYOD (bring your own device) into the 'too hard basket', and say it is something they will address when they absolutely have to.

The BYOD trend is a new reality that will have to be faced, so what is it exactly? What are the business risks and benefits? And, most importantly, what strategy should you have in place to deal with it?

BYOD: a definition

Bring your own device is the use of personal equipment on the company network. For the most part this relates to the use of personal phones, tablets and notebooks on the wireless network, but I have seen some gamers bring in their pimped PCs and plug these into the LAN. Though BYOD predominantly uses the wireless LAN, it is more of a management issue than a wireless issue.

The risk/benefit equation

BYOD can help companies shift capital costs from company to user. Rather than supplying company-owned devices, companies can give their employees an allowance and get them to own the device and related contracts. As these devices are used for personal and company use, companies need only pay a portion of the cost. Interestingly, according to the *Good Technology State of BYOD Report*, employees are willing to pay for their own devices.

However, there are some risks that need to be taken into account when implementing a BYOD strategy. Companies may have compliance requirements under PCI DSS, HIPAA etc. Even though the employees may own their devices, their companies are still required to comply with this legislation even if company data resides on the employee's personal device. In addition to this, when an employee resigns, the company will need to make sure that they do not take any company data with them.

These and other similar challenges related to company IP, compliance requirements and appropriate use policies need to be managed under a company BYOD policy. As part of your BYOD strategy, each employee should at the very least sign one of these as part of their employment contract.

Choosing a strategy

Before you even consider the type of solution you need, it is critical that you have a strategy to deal with the risks and benefits of BYOD. Gartner uses implementation scenarios to help define what that strategy should be. *[refer to the diagram]*

Most people opt for a 'contain' or 'block' strategy, because even in the smallest networks, security is key.

Block

A 'block' strategy goes beyond just telling staff they cannot connect personal devices to the network. You would need to implement a Network Access Control (802.1x) solution to prevent people plugging notebooks, PCs or even rogue access points into the network. This would be done in conjunction with certificate services to authenticate clients. Some organisations go as far as not allowing any electronic devices in the building!

Contain

A 'contain' strategy moves from blocking these clients to managing them. Historically, this has been hard to manage, with solutions being complex and onerous to implement. Current network management solutions make this easier with Simple Network Access Control. The process works as follows: The first time a user with a new personal device connects to the WLAN network they are directed to an on-boarding/self-registration

»

Considerations and best practices for BYOD

While not every organisation has a formal bring-your-own-device program, every organisation should develop policies and processes regarding the use of personal devices for work. Citrix offers some best practices to consider when defining and implementing BYOD.

Define your BYOD policy

- **Define eligibility** – Identify who can use personal devices for work and scenarios where it is inappropriate due to data security, worker type or other factors. In enterprises that allow a BYOD device to replace a corporate endpoint, this decision is typically optional for the worker and subject to managerial discretion.

- **Determine allowed devices** – BYOD policies should allow people to use whatever type of device that best meets their needs.

- **Set service availability** – Think about the services and apps you want to make available on BYOD devices and whether they differ by work groups, user types, device types and networks used as you define your policy.

- **Clarify cost sharing** – Some organisations provide a subsidy for BYOD devices and other services, especially in cases where a corporate device is no longer provided. If considering a stipend, tax consequences and potential IT cost savings should be taken into account.

Implement BYOD in your organisation

- **Plan rollout** – Provide guidance to help people decide whether to participate, choose the right device and understand the responsibilities that come with bringing their own device, including how data can be accessed, used and stored.

- **Implement security** – Confidential business information should reside on the endpoint only in isolated, encrypted form, and only when absolutely necessary. Multi-layered security should include granular policy-based user authentication with tracking and monitoring for compliance; control over print capabilities and client-side storage; and mandated antivirus/anti-malware software. IT should consider remote wipe mechanisms if business information is allowed on the device.

- **Establish support and maintenance levels** – Spell out the type of incidents IT will support and the extent of this support. A loaner pool of devices allows uninterrupted productivity during service, especially when a BYOD device is used in place of a corporate device. Consider providing key personnel with additional, concierge-style support.

portal where they use their company login credentials to register and authenticate it. The device is at this point 'fingerprinted' to determine what it is. This is normally done using the OS version on the device, the device's MAC address and possibly information supplied upon self-registration. Based on this information, a security profile is applied to the device, including the VLAN, ACLs, parameters around when the device can connect, where it can connect, and the maximum bandwidth allocated for its use. Normally these devices would have access to the internet and email, and as a result would be placed in networks (VLANs) that do not have direct access to the company network. Access to internal applications can be made available through a firewalled VPN session and possibly using a virtual desktop infrastructure (VDI).

Some companies may want to provide direct access to internal applications for BYOD users. This of course assumes those enterprise applications can be run on the type of mobile devices that employees want to use (tablets etc). To do this they need to make sure that these devices do not introduce any malware or viruses into the network by 'posture checking' the device. This can include scans for malware and viruses. It may also include a list of banned applications such as network sniffers etc. This is normally done with a temporary client that runs on the device, does the necessary checks, and then allows/denies the connection and evaporates.

Scout it out and be prepared

While it might be tempting to simply select the best BYOD product on offer, whether that is an end-to-end solution, a wireless overlay or a point solution, preparing for BYOD actually involves partnering with a competent solution provider to design the best solution for you. For your BYOD strategy to be successful, you will also need to review your infrastructure to make sure that it can provide the necessary performance, security and scalability to cater for BYOD and refocus your IT team on the way they deliver support and services to your organisation.