To BYOD or not to BYOD, that is the Question...

spectralink

Introduction

A lot of the miscommunication in Shakespeare's tragedies could have been spared by a smartphone or two, but it would have made for far less engaging stories!

Today, however, over 80% of the world population owns a smartphone, and there are roughly 10.47 billion Internet of Things connections worldwide[1]. We've become used to being connected to each other and to being able to access information wherever we are, at the tap of an app. We have access to one-click purchasing, endless information and each other via video calls and Instant Messaging (IM), in addition to regular telephone calls. So why is the professional world so slow to catch up? Is bringing consumer devices into work really the answer?

The risk of BYOD

1. Do you need to provide coverage for a large, distributed business?
2. Do you need to meet strict data protection regulation, such as GDPR or HIPAA?
3. Are you required to use secure and reliable networks?
4. Do you need durable, rugged devices?

If you answered yes to any of these questions, then consumer grade devices are not for you!

Keep reading to find out more about the risks of Bring Your Own Device (BYOD) policies and avoid making fruitless mobility investments.

What is mobility to you?

Mobility for consumers and mobility within the enterprise are actually two very different things.

Consumer-grade devices with internet access allow users to download a few apps and open documents. This means that consumers can pay bills, IM a babysitter or order take-away while on the bus.

Enterprise mobility needs to be able to offer the same services and then some. It needs to make workers more productive and efficient, to make it easy to contact colleagues and ask for information or to call for help if in a hazardous environment. A mobility solution needs to receive and manage all types of data -including voice and video - all without the need for lengthy custom application development and extensive training, and all from one single mobile device.

Enterprise mobility is the outcome of a comprehensive strategy and goes way beyond simply placing a handset in the hands of your workers.

Achieving your business goals

Productivity

Businesses typically introduce enterprise mobility with one main objective in mind: improving productivity[2]. Being able to rapidly get in touch with staff, suppliers and management also critically helps improve customer service while enabling workers to access and input information from anywhere, without having to visit a fixed desk location. Furthermore, it helps keep more accurate records and manage supply or operation chains more efficiently.

Businesses typically use enterprise mobility solutions to:

- automate processes
- reduce audit time and increase transparency of operations
- streamline operations
- ensure seamless, crystal clear voice availability
- provide workers with voice, data and video communications
- add presence indicators, collaborative tools and call forwarding all on a single handset

Consumer devices cannot accommodate all these apps and tools on a single device without seriously compromising it (shortening battery life and freezing). Only enterprise devices have been purpose-built to support this type of seamless, always-on communication.

Connectivity

Why is consistent connectivity to a network for both data and voice critical?

- Staff need to be able to reach each other with information wherever they are, whether it is kitchen staff or housekeeping communicating with reception in a busy restaurant or resort, or nurses connecting with the pharmacy to check drugs are available and in the right dosage;
- Security staff and other lone workers (who often find themselves isolated) need to be able to access their colleagues or the central emergency unit immediately from anywhere;
- Lone workers can also become exposed to danger due to their isolation, so professional mobility devices should offer one-touch panic buttons, worker location capabilities and full coverage that ensures there are no black-spot areas.

Consumer devices can't guarantee this level of connectivity and rely on external networks over which your business has no control. Enterprise-wide connectivity cannot be limited to providing devices but needs to encompass company-wide networking and connectivity.

Don’t commit a BYOD Blunder

BYOD policies ask workers to bring in their personal, consumer-grade devices to work and to use them to carry out professional tasks. A variation of BYOD is a policy commonly shortened to COPE (Corporate-Owned, Personally Used) which sees organizations purchase devices to be used both personally and professionally. They both expose businesses to a number of dangers.

Security

The range of different handsets and operating systems used makes it hard to keep systems up to date and secure, meaning users often end up flouting security controls and using unmanaged devices to access corporate networks, apps and data.

Possible solutions:

Mobile Device Management (MDM) will allow you to manage devices centrally, giving power to IT over personal or mixed-personal-professional-use devices which includes the ability to wipe and lock handsets in case of a suspected breach.

Cons

- Consumer devices typically do not support enterprise-class MDM solutions, so either users or IT will have to resort to a time-consuming, manual do-it-yourself approach
- IT will have to deal with and train staff on as many different devices as they bring in
- This will result in frustration and loss of productivity; not something to look forward to!
- Employees often have to give control of their devices over to their company, allowing them permission to remotely wipe devices if they believe security has been compromised; this means an employee no longer has autonomy over their personal device and could lose their personal data, photos, music, etc.

MAM (Mobile Application Management) enables IT to control and secure specific apps without managing the rest of the device. These systems allow users to log on to multiple types of corporate applications via a single set of credentials. This approach simplifies the management of multiple user accounts per employee, which typically pose security risks.

Cons

- once an employee has universal access, they can download potentially sensitive information (medical records or payment details) on to any device without authorization.

Enterprise devices can be managed remotely to update, monitor, troubleshoot, lock and wipe devices as necessary. This centralized approach allows businesses to retain control and keep a higher functionality level within all devices and applications across the business. Workers remain free to use their personal devices as they see fit without putting company systems or data at risk and without worry that their device will be wiped if any security protocols are accidentally breached.

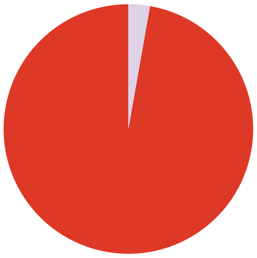
Data Protection

Legislation everywhere, to different degrees, requires businesses ensure that security protocols and procedures are in place so that data trails are clearly auditable and accessible.

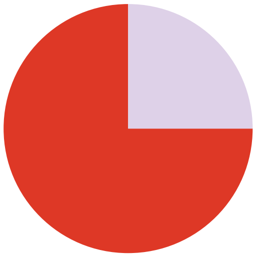
Add to this that BYOD policies increase the possibility of devices being accessed, stolen, or even simply lost and it is clear that protecting sensitive data within a BYOD environment is extremely difficult.

Tools to prevent or limit a data breach

- centralized management
- geolocalization
- geofences alerting the IT system when the device is leaving the premises
- encryption on a media card (within the device or over the wireless LAN)
- remote lock & wipe for lost or stolen devices
- application permissions to stop users from downloading unauthorised applications or uploading data to unauthorised servers
- ability to stop automatic updates
- restrict user access to hardware and features that access external servers



97% of employee's devices are reported to contain privacy issues[3]



75% of employee's devices lacked adequate data encryption[4]

Made to different standards

Unlike enterprise devices, consumer devices are not made to last, and they are not designed to have the same breadth of capabilities as enterprise devices which can include:

- **Barcode scanning:** a tool that is critical in retail, warehousing, logistics and also in medical environments as UDI (Unique Device Identifiers) ranging from the GUDIDs introduced by the FDA in the US, to the GS1 codes in the UK.

  In retail settings, customer devices are often unable to process loyalty cards or to read codes that are under shrinkwrap or have been damaged, while enterprise devices can and save staff having to decipher codes – a manual effort that wastes time and introduces an element of human error.
- **Push-to-talk:** can be critical in hazardous environments where workers may find themselves isolated. Many consumer devices require a multi-step process to call emergency services.
- **Rugged design:** ensures that your mobility investment pays off. In warehouses, manufacturing plants, factories, labs, hospitals and refineries it is critical that devices are robust and can resist tough environments where accidental dropping, exposure to chemicals, sterilization or being crushed are daily risks.

An important issue that is too often overlooked is charging and the lack of insertion ratings on consumer devices which state the number of insertions a cradle can handle before contacts wear out. When devices are used around the clock and on different shifts, new insertions can be very frequent leading to devices needing to be changed much more often or to new cradles and chargers needing to be purchased regularly.

Device Life Expectancy

The peace of mind that devices will keep running efficiently throughout one or more shifts also means increased productivity. Workers do not have to stop what they are doing and look for a power source when battery runs out, nor are they obliged to swap devices at the end of a shift but instead can pick up seamlessly where their colleague left off.

BYOD	ENTERPRISE
The worker has to find the specific service to provide repairs + difficult to locate parts	Single central repair agreement covers normal wear and tear and accidental breakage + replacements can be delivered with all the required software applications and device settings out of the box
Battery drains easily + requires one charger per device and a single power outlet	Last through multiple shifts + has multi-slot chargers with the option for replaceable batteries
The worker needs to sterilize the device after use or expose it to chemicals, dust and risk of droppage	Ruggedized devices are designed for tough environments and can resist exposure to chemicals, dirt and droppage.

Enterprise-grade devices can support your business

Do you want workers to be more productive, efficient and satisfied?

Then you should stay clear of BYOD or COPE policies, as the apparent savings comes with a whole set of risks, problems and difficulties. You might find that not only is it not possible to realize the benefits you were hoping for, but you will end up saddled with frequent replacements and upgrade costs, more admin and IT department hours, as well as potentially very expensive remediation in case security is breached.

To make your business truly mobile, introducing a device per worker is not enough; you will need to define a mobility strategy comprehensive of networks and infrastructures and to understand which devices and functions are the most beneficial for you and your specific business.

To find out more about the pros and cons of consumer versus enterprise and how Spectralink solutions can support your unique objectives talk to sales

SOURCES

[1] Bank my cell, How many phones are in the world? https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

[2] Digital Thoughts, Top 7 Benefits of Enterprise Mobility Solutions, https://blog.thedigitalgroup.com/top-7-benefits-of-enterprise-mobility-solutions

[3] CIO article; Mobile Security – Study finds most mobile apps put your security and privacy at risk

[4] CIO article; Mobile Security – Study finds most mobile apps put your security and privacy at risk

About Spectralink

As an award winner in mobile technology, Spectralink has been transforming the way our customers work and communicate for 30+ years. Through our determination to do extraordinary things, we enable mobile workforces and empower our customers and partners to explore what's next, what's possible. With our enterprise grade, best-in-class mobile solutions, we are with our customers wherever they work, however they need us. Our people, commitment to innovation and our passion are our foundation for success.

spectralink.com
info@spectralink.com
+1 800-775-5330 North America
+45 7560 2850 EMEA