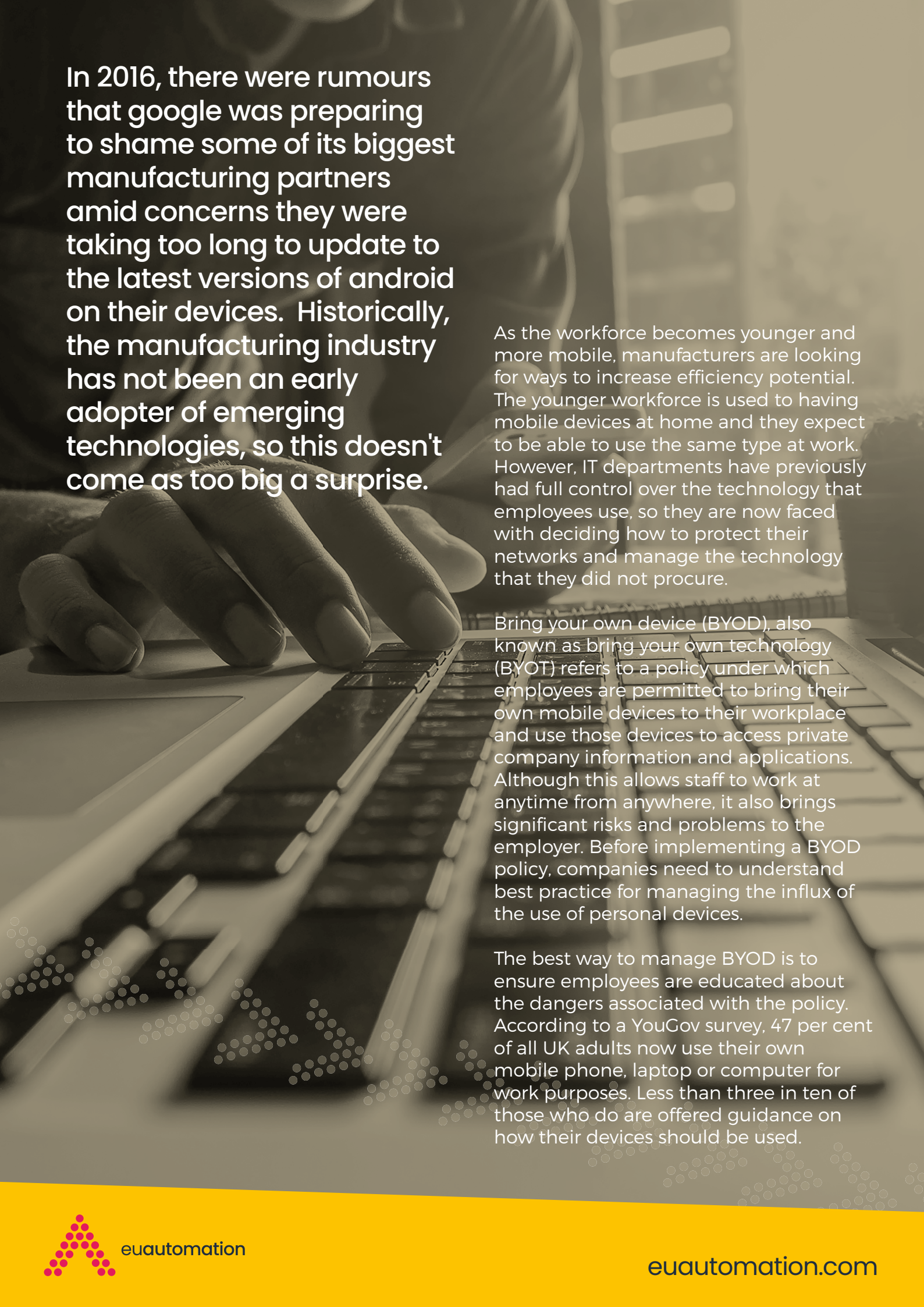


Mobile devices in industrial automation



euautomation



In 2016, there were rumours that google was preparing to shame some of its biggest manufacturing partners amid concerns they were taking too long to update to the latest versions of android on their devices. Historically, the manufacturing industry has not been an early adopter of emerging technologies, so this doesn't come as too big a surprise.

As the workforce becomes younger and more mobile, manufacturers are looking for ways to increase efficiency potential. The younger workforce is used to having mobile devices at home and they expect to be able to use the same type at work. However, IT departments have previously had full control over the technology that employees use, so they are now faced with deciding how to protect their networks and manage the technology that they did not procure.

Bring your own device (BYOD), also known as bring your own technology (BYOT) refers to a policy under which employees are permitted to bring their own mobile devices to their workplace and use those devices to access private company information and applications. Although this allows staff to work at anytime from anywhere, it also brings significant risks and problems to the employer. Before implementing a BYOD policy, companies need to understand best practice for managing the influx of the use of personal devices.

The best way to manage BYOD is to ensure employees are educated about the dangers associated with the policy. According to a YouGov survey, 47 per cent of all UK adults now use their own mobile phone, laptop or computer for work purposes. Less than three in ten of those who do are offered guidance on how their devices should be used.



Considerations

There are several things to consider before implementing a BYOD policy, including which operating platforms to use, the device enrolment process and what steps to follow if a device is lost or stolen.

Mobile devices need to be equipped with all of the features that employees require. Compiling a list of tasks that employees are likely to use their devices for will help financial and IT officers decide which operating platform is most suitable for the business and which applications and programmes need to be installed.

Devices should be registered and authenticated before being used by employees. It's extremely important that managers know at all times which device belongs to which employee as it allows network administrators to quickly detect any unauthorised devices on the network.

If employees are likely to store sensitive data on their devices, businesses need to think about what they will do if a device is lost or stolen. We are increasingly seeing news stories about USB sticks left on public transport and laptops being stolen from cars. If the IT department is notified of a loss immediately, a device wipe can be performed before it becomes a greater problem. Employees should be aware that they are required to notify IT when a device is lost. They should also be made aware of the processes surrounding employee departure — will their device have to be wiped when they leave?

Access to business information on employee-owned devices can lead to data and connectivity issues. Security is further compounded by the fragmentation of the mobile operating systems market. When employees bring their own devices to work, it's impossible to ensure that each one operates identically, opening some devices up to security issues more than others.

New versions of operating systems are measured in months, rather than the average three-year refresh cycle of Windows in a desktop PC. This pace of change and the fragmented market complicate things for an IT department looking to establish a consistent standard for security and support without putting rules into place about what devices an employee can bring to work.

When it comes to smart phones, there are also issues regarding whose responsibility it is to ensure the device is charged throughout an employee's shift. Coverage can also be problematic in a large manufacturing plant as some facilities can have unreliable service and coverage, especially with machines creating electrical interference.



Legislation

Without the correct guidelines in place, a BYOD policy can result in fines, lawsuits and data breaches for an organisation. Companies in the UK must ensure compliance with the Data Protection Act of 1998, regardless of industry, sector or size. This imposes obligations on data controllers to process their data fairly and transparently and to take all appropriate security measures to prevent unauthorised access. Failure to protect data can result in fines of up to £500,000.

Legal responsibility for protecting data lies with the company, rather than the individual owner of the device. Therefore, employers must ensure that a robust security infrastructure is in place, without impeding the employee's use of their own device.



Cloud

Using cloud systems removes the need to download company documents onto a personal device, limiting the degree of security an employer might need to use. With cloud computing, all storage and data processing occurs outside the personal mobile devices, so corporate documents have greater security.

Lack of antivirus and malware protection can also be remedied with cloud computing. Mobile device management tools help secure devices from outside threats using a cloud computing environment from a central location. Personal devices that access business infrastructure are sometimes seen as easy access points for hackers. Mobile device management tools are an integral part of minimising the risk of data breaches.

Research shows that US and UK companies using cloud computing systems reduced their infrastructure costs by 23 per cent. These systems eliminate the need to make and distribute paper copies of documents, as employees can find digital versions online. The cost of running a server is also much more than using the cloud.



euautomation

euautomation.com

On the factory floor

BYOD is no longer limited to office-based staff. Many manufacturing companies have implemented a BYOD policy on the factory floor for more efficient operations. Companies that have already implemented BYOD found that it increased mobility and optimised response time for engineers. It also brought economic advantages, as the majority of employees already own a smart phone or tablet and know how to operate their device.

While BYOD works for many manufacturers, some worry that they are not designed to sustain the harsh conditions of an industrial factory. In response to this, British phone retailer, Tuffphones has unveiled a new range of hard-wearing handsets aimed at industrial and construction workers. The Android device is extra durable and designed to cope with water and dust ingress, along with being dropped from significant heights. This could pave the way for more accepted mobile device use across the industry.

Manufacturers can take advantage of BYOD to connect in real-time to supply warehouses, production facilities and the field. Integration with enterprise resource planning (ERP), manufacturing executions systems (MES) and customer relationship management (CRM) applications enables a faster response to critical issues across operations. This results in a more agile and flexible supply chain that adapts to the changes in market conditions and customer demands.

BYOD also allows manufacturers to universally monitor and control the day-to-day functions of multiple business lines. On the factory floor, it's common for engineers to use their own devices to receive machine alerts and alarms to signify that there is something that needs their attention. Receiving this alert on a mobile device means that the factory doesn't need to rely on an engineer checking desktop computers or IT systems, as they can receive the notification wherever they are.

Manufacturers can also use mobile devices to message each other during times when it's not appropriate to call or if the conditions inside the factory are too noisy.



CYOD

While the use of mobile devices on the factory floor improves efficiency, communication and reaction times, asking staff to use their personal devices for work purposes might not be the best way to bring technology to the floor.

An alternative that has been rising in popularity over recent years is the choose your own device (CYOD) model. This allows employees to choose the device that they will use for work purposes, but the organisation still owns the contract. Under a CYOD scheme, IT departments can support a limited set of devices without feeling overburdened by the multitude of devices that are currently available to the public.

The negative impacts of BYOD, including security issues and troubleshooting can be drastically reduced with CYOD. Employees can still work from remote locations and access information about equipment from anywhere in the factory, but the company's IT department still maintains order over the influx of mobile devices and applications. Having a limited number of devices, all of which the IT department are familiar with, reduces time spent on troubleshooting.

Because the devices are bought and owned by the company when following a CYOD policy, it means that they can be installed with the correct security software and set up with the appropriate administrator, firewall and network settings. Research suggests that 43 per cent of employees have accessed sensitive data on their personal device while using an unsecured public network, such as those in airports and restaurants. With CYOD, employers can have peace of mind that mobile devices are protected in these situations.



Policies

Whichever method companies choose, there should be a mobile policy in place to govern usage and access to sensitive company data and gateways. The policy needs to define what is considered acceptable use, whether the company or the employee owns the device. It should highlight what the employee is allowed to store on the device, in terms of protected data and also what is deemed acceptable use, if the device does not belong to the employee.

Employees need to be aware of the device support available to them — which department should they contact if they are having connectivity problems, for instance? Employees should also know if they are entitled to any reimbursements, if they have purchased the device themselves, or if they are required to contribute anything towards their service plan for a company-owned device.



Don't get left behind

With the majority of employees expected to use technology to improve productivity in the workplace, what happens to those that aren't as familiar with today's mobile devices? While most employees will only need minimum training when using mobile devices on the factory floor, older less technically-skilled employees will need ongoing support. For new tablet or mobile implementation, show all employees how to set up their email on the new hardware, how to load files onto the device and how to connect it to Wi-Fi. By making the learning process as simple as possible, they should quickly get used to using mobile technology regularly.

It's also important for all employees to understand why mobile technology will be beneficial to them in the workplace. Some might find it useful to have access to important files from anywhere in the factory and some might want to use their tablet as a second monitor when operating equipment. After realising how much time and energy they will save, they will be more receptive to the idea of incorporating these devices into their daily work routines.

Despite popular belief, manufacturers shouldn't be too worried about workers operating mobile devices in the workplace. A recent survey by London-based market research firm, Ipsos Mori, sponsored by Dropbox, found that older workers are less likely to find using technology in the workplace stressful and experience less trouble working with multiple devices than the younger cohort.

With an entire workplace on board and an in-depth policy in place, employers should have no problem implementing mobile devices into everyday factory floor procedures. While manufacturers haven't always got on board with upcoming technologies, mobile devices have been proven to improve efficiency and productivity on the factory floor. To avoid getting left behind, employers should start planning its implementation of technology now, before employees and customers find another company that embraces it with both hands.

