WHEN BYOD IS A BAD IDEA

Corporations are increasingly allowing their employees to purchase their own smartphones, tablets and other communications devices in efforts to cut costs. But is this strategy safe for all industries? For companies operating in hazardous environments where the risk of explosion or other disasters is high, BYOD is not only a bad business decision – it can be a deadly one.

November 2014

By Thomas P. Ventulett
Airo Wireless, LLC
1545 Peachtree ST NE
Suite 300
Atlanta, GA 30305 USA
www.airowireless.com

Introduction

To maintain costs and keep employees happy, companies are aggressively jumping on the Bring Your Own Device (BYOD) bandwagon in which employees purchase their own mobile phones, tablets or computers, thereby avoiding company purchasing requirements. Clever BYOD programs can help manage costs while giving personnel the freedom to choose their preferred communications devices. Corporations can control these devices through a litany of Mobile Device Management (MDM) applications and platforms.

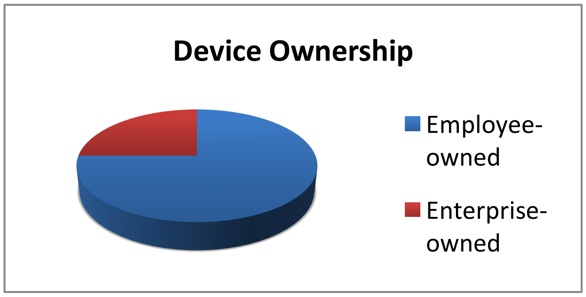
This liberal approach to corporate infrastructure relies on a third-party MDM solution that sits on the application layer of the device to presumably make it safe and compliant with company policies. Unfortunately, this does not address very serious underlying dangers associated with the use of mobile devices in certain industries - namely, hazardous industries - thereby introducing new risk into these organizations and jeopardizing company assets and capitalization.

Oil and gas companies, as well as businesses in 18 other global infrastructure verticals that operate in mission-critical and hazardous locations, are good examples. The revenue of the top 10 oil and gas companies in 2014 exceeded $3.04 trillion[1], and national oil company revenues worldwide surpass this figure. These companies, however profitable, function in risky environments where every business decision puts lives and property on the line. Personnel working under these circumstances are not equipped, nor inclined, to make the best decisions for the enterprises' safe and effective communications platforms. Information loss carries a significant price; facility loss (e.g., a refinery) or, especially, loss of life, can be even costlier.

The Current Mobility Situation

The global economy relies on the ever-increasing need for efficiency and big data analytics, while reducing risks and liabilities. Mobile devices and solutions increase functional efficiencies, deliver real-time access to information and can reduce operational risks. With the evolution of technologies over the last 20 years, from feature phones, to email-enabled handsets, to smartphones running enterprise applications, global industry has benefited from this exponential power of individual computing and data access.

Moreover, recent market research shows a trend in employee-owned mobile devices, estimating that only one-quarter of enterprise devices will be owned by companies, as opposed to employees, by 2017.[2]



This trend has profound significance for nearly some of the largest industries in the global economy that operate locations where the concentration of gases or the density of particulates

[1] (http://www.statista.com/statistics/272710/top-10-oil-and-gas-companies-worldwide-based-on-revenue/
[2] http://www.fiercemobileit.com/story/4-tips-ensure-smooth-byod-program-roll-out/2014-10-10

in the air creates a volatile and explosive environment. These volatile environments almost always lie at the front edge of revenue generation, where the risk of explosion can be the most costly. Unfortunately, a typical circuit board found in any modern electronic device, such as a smartphone or tablet, can create enough heat or spark to ignite a hazardous operating environment.

A typical circuit board found in any modern electronic device, such as a smartphone or tablet, can create enough heat or spark to ignite a hazardous operating environment.

Global standards for the use and operation of electronic equipment in hazardous locations have been established. These standards are written for large-scale equipment used in places such as refineries and are based on designs of simple circuits. A typical smartphone may have more than 500 distinct circuits with stored capacitance nearly 10 times the allowable limits for safe operation in a gas-rich environment. Application of these standards to complex circuits can be difficult at best. As a result, a significant sector of the modern economy – the hazardous industry space - does not have access to modern communications and computing.

However, with the advent of safe and appropriate devices that enable voice and data communications for true mission-critical environments, the promise of mobility can now be realized for hazardous industries. Once they establish an application-rich environment, these enterprises can employ subsequent technologies of the Internet of Things, where the highest return on investment exists - and the greatest risk to economic destabilization can occur without them.

When BYOD is BAD

The underlying premise of BYOD is simply cost savings. Secondarily, there is a general assumption that if employees have access to their own handsets, they will react more positively to the work environment than if a device is pushed upon them by their employer. Lowering costs and simultaneously improving workforce satisfaction would naturally be considered a win-win situation. The question, though, is whether this is truly appropriate for an enterprise, or whether it is simply another short-term strategy promoted by consultants and solution providers whose goals may not be aligned with the long-term risk profile of a corporation.

To carry the “latest and greatest” handsets, employees are often willing to use their own money to buy them. As soon as this purchasing strategy becomes a reality, companies can slough off the responsibility of corporate infrastructure onto employees and presumably save loads of cash. The financial reality has turned out to be somewhat different.

Research done by analysts, including the Aberdeen Group[3], have shown that there are plenty of hidden costs in a BYOD program, not in the least, MDM services that are intended to provide high levels of control over the devices through software. Software, however, does not replace employee responsibility for safety and security.

Information technology (IT) professionals are very adept at understanding information and network security. But this only represents part of the picture. Corporate security extends to physical locations, where consumer electronics simply have no place and would be considered inappropriate or illegal to carry. In nearly 20 of the largest industries in the developed world, almost 15% of the workforce operates in hazardous locations - areas that are prone to an explosion due to the concentration of gases or particulates in the air. These hazardous locations (e.g., refinery, mine, pharmaceutical plant or chemical plant) represent the heart of operations for these organizations. Relying on third-party software to protect email and data does not ensure that an employee is operating appropriate electronics in appropriate locations.

Table 1: Industries Operating in Hazardous Explosive Environments

Oil & Gas Drilling	Power Generation	Granaries
Petrochemical Refining/Processing	Pharmaceuticals	Mining
Fuel Storage/Transport	Distilleries	Water/Sewage Treatment
Polymers	Food Manufacturing/CPG	Car Manufacturing/Painting
Chemical Manufacturing	Aviation/Military Flight Lines	Textiles
Printing		

BYOD programs can be considered a bad idea for sensitive industries when weighing the very high cost of failure compared with the benefit of a having an employee pay for a few-hundred-dollar phone. The risk/reward calculation is hard to imagine. Consumer devices are not engineered, nor can be altered, to meet the safety requirements of a hazardous location. Additionally, personal handsets are designed to meet consumer needs, tastes and personal preferences and are never designed to limit user distraction when job site hazards are present. Lastly, a BYOD program does not make up for necessary internal infrastructure improvements. Combined, these limitations imposed by a BYOD program make for not only a bad business strategy, they can also be dangerous to an enterprise.

1. Some BYOD Devices are Physically a Bad Idea

A typical mobile phone or tablet carries 6 to 8 times the allowable limits of stored capacitance to operate in a hazardous location. That means that such devices have 6 to 8 times the energy necessary to ignite a volatile environment. Given this data point alone, it would be irresponsible for an IT department to rely on a BYOD program in a company that operates in such locations. The cost of risk would far outweigh the cost savings on mobile devices.

[3] http://www.aberdeen.com/research/9699/MA-BYOD-increasing-costs.aspx/content.aspx

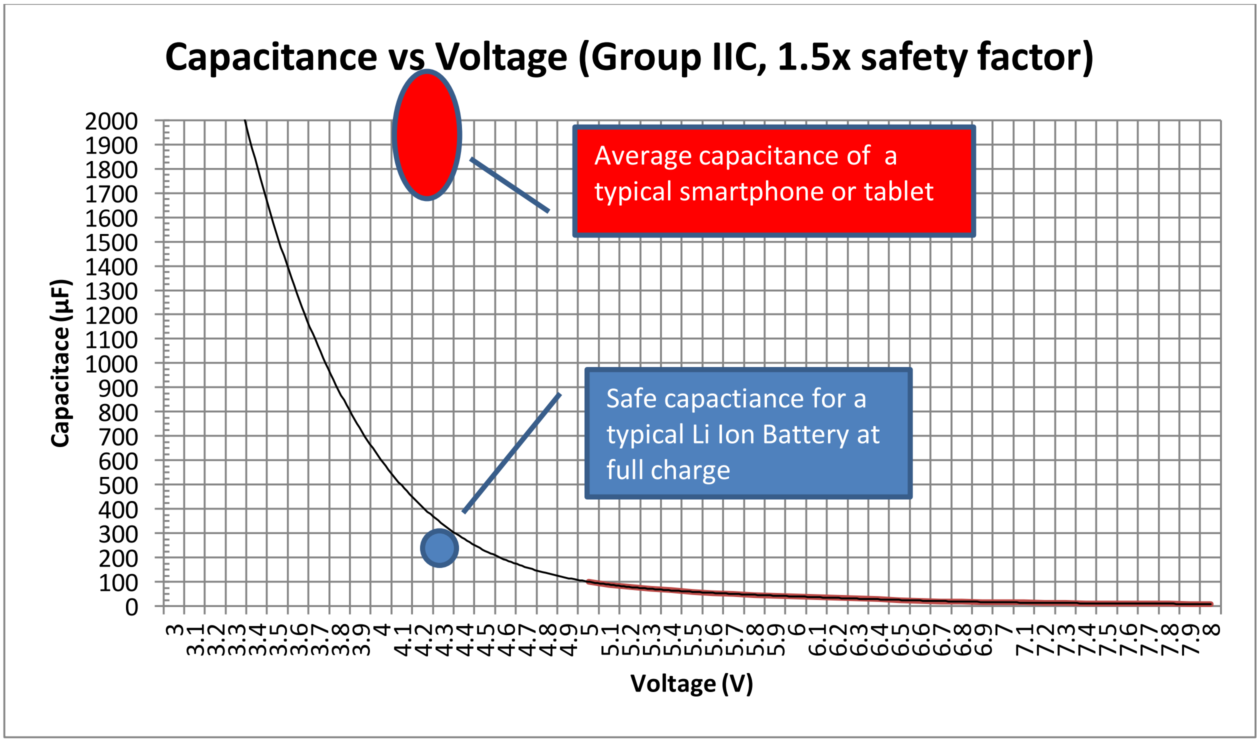


Table 2 Safe Capacitance/Voltage
in electronic devices

An MDM solution does not prevent an employee from carrying an unsafe personal device onto company property. Further, an MDM solution does not control the stored capacitance on a mobile device. Lastly, an MDM solution does not prohibit an employee from believing Internet gimmicks that claim an "engineered case" or "protective cover" can make a standard mobile phone intrinsically safe.[4] The risks associated with allowing personal handhelds in hazardous environments can be hard to calculate, but they have enterprise-wide – and potentially fatal - implications.

2. Some BYOD Devices Don't Match the Use Case

Handsets must be designed from the outset to be deemed safe for operation in a volatile location. Safety and risk prevention encompass much more than just the physical device and an MDM solution controlling it. In a hazardous duty job, employees must remain vigilant and focused on their tasks at hand. Fast-moving equipment, heavy machinery and, of course, explosive environments all require employees to wear protective gear, operate without distraction and identify risks and hazards. Posting a Facebook update to share the view from an offshore rig, for example, can introduce new risk to not only the individual but to the organization as a whole.

[4] Equipment and wiring that is incapable of releasing sufficient electrical or thermal energy to cause ignition of a specific hazardous atmospheric mixture in its most easily ignited concentration. (ISA-RP12.6)

In addition, the culture of BYOD has pushed potential risks even further. Since an employee purchased the device, there is an assumption that the employee “has the right” to determine when, where and how it is used. Corporate policies have tried to keep pace with defining access rights to information, but the research proves otherwise. In a recent survey by Centrify[5], almost half of the employees in large North American corporations have more than six third-party applications installed on their smartphones, including cloud storage solutions that are not controlled by a company MDM solution. If users can be easily distracted by various personal inputs, then who is responsible for protecting the business?

3. BYOD Devices are a Bad Idea for Infrastructure Evolution

Since 1933 when the first two-way radio was installed in a police car, organizations have relied on this formidable technology for communications. Although reliable, this technology has only marginally upgraded to digital, with 12.5KHz of bandwidth per channel. With modern smartphones running LTE, Bluetooth and Wi-Fi across a vast array of bands, there is little comparison in the modern age. A two-way radio simply is not designed to meet the high-bandwidth needs of a vast enterprise.

Obviously, a two-way radio would never be qualified as a BYOD! The point, though, remains the same. A great deal of time, money and effort goes into selecting company Enterprise Resource Planning (ERP) systems, mail servers, back-up servers, disaster recovery plans and, of course, information security. Even in the realm of the less exotic, Microsoft Office and Microsoft Exchange are the staples for business operations worldwide. While IT managers interview, qualify, test and validate these systems and their subsequent upgrades, pervasive access and the choice of equipment used is suddenly left to the end user without regard to current or future compatibility.

In the specific case of two-way radios that remain on job sites today, organizations cannot entrust infrastructure improvement decisions to the employee. When carbon paper became a thing of the past due to the introduction of the personal computer in the 1980’s, corporations did not look to employees to bring solutions from home to solve the problem. Yet this type of strategy is prevalent today in many of the hazardous industries listed in Table 1. Relying on a BYOD program as a method to bypass corporate responsibility injects risk into the organization and can lead to long-term infrastructure failure for companies operating in hazardous environments.

Conclusion

Although BYOD strategies are increasingly popular among large enterprises to realize cost savings, these plans are dangerous for corporations in the hazardous industries space. Personnel cannot be held responsible for choosing or controlling communications devices that are safe for explosive environs, nor can device management systems prevent user distraction caused by personal use of corporate devices. With BYOD, organizations can lose control over

[5] http://www.centrify.com/news/release.asp?id=2014042301

the compatibility and reliability of future communications purchases and the implementation of those over the long term, sacrificing company-wide uniformity and safety for individual preference and convenience.

Corporations that operate in hazardous or sensitive environments cannot afford the risks associated with BYOD. The clear choice for these industries should be communications systems that address the physical safety needs of personnel and property, limit the use of such systems to work-specific tasks and allow for organization-wide infrastructure development over time.

Potential solutions for the hazardous industries space would meet the following requirements:

1) Be manufactured from square one to be intrinsically safe, with each component complying with global IS standards and certifications
2) Be designed with the specified uses in mind, limiting unnecessary features that could distract the user
3) Be compatible with existing company infrastructure and able to be upgraded and aligned with future technologies in a complete communications package that gives longevity and continuity to the organization's operating goals

Airo Wireless, an Atlanta-based manufacturer of IS solutions for mission-critical operations, offers a variety of products that meet these requirements, providing companies in the hazardous industries space with the tools they need to communicate more effectively – and safely.

See descriptions and specifications for the Airo I-Safe 28 smartphone and the Airo I-Safe 810 tablet for details.

About Airo Wireless

Founded in 2000, Airo Wireless specializes in manufacturing intrinsically safe industrial smartphones, tablets and handheld computers for hazardous environments such as Oil and Gas, Petrochemical, Pharmaceutical, Public Safety and Utilities.

Airo Wireless is headquartered in Atlanta, GA, U.S.