4 Business-Ending Risks of not Leveraging Mobile Device Management Software

With employees no longer tied to a desk, mobile devices are now what keep your business moving. And the mobile workforce trend is only accelerating and expected to increase to 1.8 billion by 2023, meaning more than 40% of workers will rely on their devices as business tools.

However, managing and maintaining all those devices, if not done right, can stop your business in its tracks. We all know the benefits that Mobile Device Management (MDM) tools provide, including optimizing the functionality and security of corporate mobile devices, as well as BYOD, and increasing efficiency, productivity, and the security of your corporate network.

Still, many businesses hold back from leveraging MDM tools, citing the cost or capabilities of their in-house staff to monitor and manage the growing number of mobile business devices.

But is it really worth the risk? Let's take a look at 4 of the top risks businesses face when rejecting MDM software.

Data Breach

The leading argument for electing not to leverage an MDM tool is cost. However, according to an IDG study, 74% of global enterprise IT leaders report experiencing a data breach due to a mobile security issue. In that same study, 95% say a rise in data on or accessed by mobile devices increases the risk of a security breach. With the actuality that a cyberattack is coming and the average cost of a data breach in the millions, is mobile device management software really too much of an investment in your company?

Putting the financial costs of a data breach aside, the loss of business data and intellectual property, the compromising of your customers' data, and damage to your business's reputation, are enough to close your business permanently.

Weakest Link Exploitation

The weakest link when it comes to mobile device security are your employees—and managing their usage habits and accounts is a full-time job. Unfortunately it's all too common for employees to download unauthorized malicious apps. In just one year, Google caught more than 700,000 malicious apps in the Play Store. When an employee downloads one of these apps, it increases your threat vector, providing unauthorized access to your company network and critical data, and opens the door to a breach.

In addition, ex-employees can wreak havoc since after they quit it may take a while for their names to be removed from the active directory, leaving vulnerable loose ends and opportunities for them to download classified company data to exploit for their own benefit. This has led to stolen corporate secrets being shared with competitors and confidential customer information being sold to the highest bidder.

3 In-House Inexperience

Let's face it, most IT staffs are so overworked managing the day-to-day that they don't have time to become proficient or productive in learning a vast array of new technologies. With mobile devices being the hardest enterprise asset to defend, is it worth putting the responsibility for the variety and multitude of devices employees use in their hands?

Without the right certifications to set up or support the infrastructure, they're on their own or will need to reach out to the OEM to get additional support, which doesn't come cheap.

4 Productivity Lethargy

To keep up with the fast pace of business—customers' ever-changing needs, lighting-speed technology innovations, or the always-expanding number of competitors popping up—productivity is key to success. One of the biggest hits to the productivity push is relying on employees to ensure their mobile device business software is updated.

Applications pushed to thousands of devices can take a substantial amount of time, putting the onus on end users to do it themselves, ship their devices across the country for your IT team to set up and ship back, or wait until an event to make the shift isn't realistic or cost-effective. In the meantime, how much business are you losing since your team isn't up to date?

Vox Mobile and Workspace ONE

Business owners and CEOs juggle a host of risks every day. Mobile device management software doesn't have to be one of them.

Vox Mobile invites you to remove the risk of not having MDM tools and realize the security, efficiency and productivity VMware Workspace ONE can deliver for your business. A Gartner Magic Quadrant Market Leader, VMware is leading the unified endpoint management (UEM) game enabling enterprises to manage all of their workplace devices under one, simple-to-use management solution.

As VMware's largest Workspace ONE Managed Service Provider (MSP), Vox Mobile provides you with:

- Substantial license discounts
- Unbeatable certified support team
- Scalable service packages based on your prioirities, now and for the future
- Full lifecycle management from consultation through implementation to ongoing support

In short, Vox Mobile's approach to Workspace ONE accelerates your business success.

Get started today.