Mischief Managed?

Or, Is Your MMS Ready for Prime Time?

By John Burke, CTO

Jerald Murphy, SVP of Research and Consulting

Nemertes

October 2022

Table of Contents

1. Executive Summary

After an initial burst of enthusiasm a decade ago, many enterprises are pulling back from the move to BYOD for mobile devices.

Reasons vary, but it turns out that asking employees to use personal devices for work purposes isn't optimal for either employees or their employers. For one thing, BYOD cripples an enterprise's ability to develop mobile apps: it's impossible to roll out a mobile application if the potential universe of platforms that must support it is virtually infinite. For another, ensuring the security and privacy of corporate data on personal devices and in consumer applications is extremely difficult; enabling auditable compliance of such privacy and security is even more so. For a 500-device company, Nemertes finds that it would run to just over 3 full-time staff dedicated to mobile device management to ensure ongoing security and compliance.

And finally, once personal mobile devices end up being used for corporate purposes, demand from users for help desk and other support functions isn't far behind. At a minimum, executives will expect (and in most companies receive) full support for their work use of personal devices, whether or not they are running the company MDM/EMM client; others will and do ask for support as well, and not just for getting work done.

At the same time, employees resent having to install corporate applications on their devices, and often resist tools such as MDM (mobile device management) that partition personal devices into "company-owned" and "personal" sections.

The solution appears simple: Roll back mobile devices into a corporate fleet of devices, to which IT can apply the time-tested principles of standardization, consistent security, and scalable support.

But appearances can be deceiving. Although it's certainly easier to manage corporate-owned devices, for reasons of scale, staffing, and skills it's not as trivial as some may think. Mobile devices aren't just a single line item on a spreadsheet of "endpoint devices"—they're as complex as, perhaps more so, than traditional laptops and desktops.

The upshot? Taming the mischief of your managed devices is an endeavor worth your time and attention. If you do it correctly, you've enabled your company to add mobile applications to its portfolio of employee solutions—and speed the path to digital transformation. Doing it incorrectly means shoveling good money after bad. You get none of the cost benefits of BYOD with all the headache of managed devices.

2. Pulling Back: Enterprises Retreat from BYOD

Many enterprises are in partial or full retreat from BYOD, the "Bring-Your-Own Device" model of employee ownership of mobile devices. While acknowledging that employees prefer to carry a single device, rather than a "personal" and "corporate" device, employers are backing off the "just use your own" model for a number of reasons, including the lack of anticipated cost savings and the strategic importance of mobile platforms to running their businesses.

2.1 Requirements Complexity Trumps Cost Savings

The vision: Not having to pay for devices your employees use saves millions annually.

The reality? Trying to integrate and manage devices the company doesn't own or control usually creates more problems than it solves. On one side of the ledger, companies may be able to reduce hardware costs by not paying for the devices themselves.

On the other side:

- Compatibility issues with multiple operating systems
- Increased help desk calls to help users with untested issues on applications with different operating systems
- Increased security risks in having to deal with both multiple points of penetration, as well as employee-owned devices that contain multiple uncertified applications and potential infections.

The reality is, it's very difficult to manage devices you don't own (pre-pandemic, nearly 30% didn't even try, and there has not been a rush to do so since), and to level-set reasonable expectations among end users, and to deal with the additional security issues them using their own devices creates. Companies are starting to realize the true costs of BYOD, and these costs are leading many companies to bring mobile devices back in house.

2.2 The Increasing Importance of Mobile Platforms for Business

More critically, mobile platforms are an increasingly critical component of many organizations' digital transformation story. From front line staff to executives, more users are interacting with more applications and more business workflows from the "outside" because folks want to consume them on mobile platforms in the name of rapid response and convenience. For larger organizations, Nemertes sees anywhere from 40% to 75% of systems mobile-accessible, and up to 90% for smaller organizations. This is especially the case for newer generations of workers, who came into the workplace with the idea of BYOD commons, and who see mobile apps and remote working as a birthright and workright. As mobile applications and mobile-enabled platforms became standard practice, shifting mobile work from "nice to have" to mission critical, their reliability and security became more valuable than ever.

3. The Challenges of Managing BYOD

3.1 Compliance Issues

Compliance is a reality most companies must deal with on mobile devices. This is especially important for companies operating internationally, but increasingly an issue even within the borders of the US, with different states establishing different privacy and data management requirements. Compliance is difficult enough even if a company owns its own devices. Managing privacy of end points becomes more problematic if the end user has business applications on their personal device. Add to this the challenge of managing compliance for employees in different states and countries, and companies have multiple tiers of compliance complexity that add to mobile device management headaches.

3.2 Data Management and Security

Privacy and compliance are the tip of the iceberg. Companies must also deal with the challenges of data management and security, as well as application management. Companies must determine which applications what devices have access to what data. From a security and policy standpoint, companies must determine what applications and data are even allowed to be on a mobile device. Also, different devices with different operating systems are likely to have different versions of applications – it may be that only the current application versions for only some operating systems meet company data management or security requirements.

Not all data threats are external. Insiders historically have caused as many problems as external forces with hostile intent, or more. In some (many!) cases, internal users have lacked the training or experience and judgment to properly protect and handle data, unintentionally deleting it or exposing it to outsiders.

And then there’s the challenge of internal threats. Employees may become the bad actors themselves, whether they’re simply disgruntled or coolly calculating, intentionally opening back doors into the infrastructure, or selling credentials, or selling protected information for a profit. If the end user owns the phone, it is difficult to know if they are keeping more data than is needed on a phone, or even have data that should not be on a phone. And, the more use of mobile platforms expands within the business, the greater the scope of potential compromise: a fully “mobile-enabled” enterprise is fully mobile-vulnerable as well.

Finally, it is difficult to control whether the end user even has a password on their phone, or whether their password meets company password standards, not to mention how a company deals with any sensitive information existing on a phone that was lost. This is in addition to the confusion of mobile applications that have mobile software on the desktop, which create further problems. Clicking one wrong button or missing a button in the list of ones to click and so failing to properly configure permissions on some file or folder can all be prey to various errors, such as mobile-based phishing schemes.

3.3 The Bottom Line: Ease of Control

The reality is that all security and compliance requirements are easier to meet with enterprise ownership and control of the device. Nemertes finds that managing a corporate-owned device takes only 25% as much time as managing BYOD devices; roughly three-fourths of an FTE for 500 devices, instead of three. This is especially true when dealing with enterprise-contracted mobile services. Through the enterprise's contract, end users are forced onto devices and plans that meet enterprise needs when they walk into the carrier store or order through a company-specific portal. Enterprises have a huge advantage here, being able to dictate and modify contract terms and conditions, including configuration, installation, integration, and management of enterprise applications. Individuals don't get this flexibility and control.

4. Pushing Their Luck: Owning the Device is Just the Start

4.1 Scale

Controlling the device is helpful and perhaps necessary, but it certainly isn't easy. Managing thousands of devices is not simple. Global scope adds to the challenge of scalability and compliance, both in terms of what is required and in terms of what is allowed and forbidden. Not all tools and all functions can be used everywhere.

4.2 Staffing

Organizationally, it can be hard to devote the required amount of staff time to managing mobile environments. Mobile management may be perceived more as security and compliance activity (overhead) than as directly adding to business value (enabler), even though mobile security is clearly an enabler of conducting business sustainably. Everyone wants mobile access to everything to drive business forward faster. Doing that without acceptable security is foolish, short sighted, and prone to the self-sabotage that individual users accidentally bring on themselves.

Finding experienced security staff is hard and expensive. Retaining them is just as challenging. Limitations on staffing will lead to costly rehiring and retraining. This inevitable lack of continuity almost always has a detrimental impact on customer service.

4.3 Skills

Getting people trained on mobile device management isn't cheap or easy. Mobile platforms require their own expertise, as do mobile security systems, asset management, device-level support, inventory management, mobile software management, network security and management. In addition, integration of mobile devices into the business environment has its own unique requirements.

Device configuration and management is just the beginning. Wireless and device contracts need to be managed, as do the vendors that deliver and support them. Depending on how large your organization is, this management could be global in scope. The best vendor and contract managers must know how to optimize internationally for the best services and pricing.

All this work is best done by dedicated staff. All the above are special skills. It usually spells disaster if all this work is given to existing network, server, or application staff as "additional hats" they must wear. Of course, the reality is that a company rarely "staffs up", especially in today's economic environment. So, one more set of hats is given to an already overloaded staff to handle…which further increases the chance of those folks to follow the previous employees who already jumped ship. Add to this the speed and variety of changes happening with compliance requirements is yet a further challenge for internal staff wearing multiple hats. Supporting all the changes with existing staff is a pipe dream that simply isn't achievable.

5. Lifting the Burden: Managed Services for Mobility

There is hope for the beleaguered IT professional who needs to deal with these growing and shifting mobility requirements. Managed services companies that specialize in mobile device and infrastructure management can handle these tasks for less money and with better results than your existing staff. This is not going to be an issue of firing staff who are already doing this function internally. First, they are not likely primarily doing it. Second, those that are, are doing it as part of overloaded functions they were never brought on to perform in the first place. In reality, managed services mobility services performed by a managed service provider are more likely going to be performing services you need that you aren't able to hire for in the first place.

5.1 Benefits of Mobile Managed Services

Outsourcing mobile management pushes the burdens of finding, training, and retaining staff off the enterprise. The enterprise gives the service provider the requirements. The service provider delivers on these requirements, and the service provider is responsible for figuring out how to deliver them. You don't have the risk associated with spending time and money to train someone, only to have them turn around and leave you in the lurch. The service provider is responsible, regardless of who comes and goes from their company. The enterprise is free from the burden of hiring, training, and retention (all with their own costs that are rarely considered, but are very real).

Outsourcing puts the challenges of scale on the provider, who has experience and should have a proven methodology for dealing with challenges at scale. The fact that they are providing services for you and countless others already gives them the advantage of scale, which is a good thing for both consistency of service and cost.

Finally, outsourcing makes the costs completely visible, clearly showing what insourcing would cost. This eliminates the need for the enterprise to have to find and calculate all those hidden costs.

6. Shifting Priorities: Recommendations

6.1 Think Through the True Cost of Ownership

If you have pursued BYOD, price out a return to enterprise-owned devices. As it is clear from this piece, costs are FAR beyond the price of the device. In fact, once all the considerations of training, staffing, retention, compliance, and security are taken into consideration, you will realize the cost of the hardware device is just a small fraction of the overall costs of managing a mobile workforce.

6.2 Identify All Requirements for Secure Mobile Device Management

Scope and price out all requirements for securely managing mobile devices, including staff, hardware, software, training, configuration, integration, as well as ongoing management.

Your best assumption for compliance is that the regulatory context will shift regularly. An equally good assumption is that security threats will continue to grow in complexity and virulence. Be very conservative in your estimates of costs related to acquiring, training, and retaining security staff.

6.3 Compare Managed Service Costs Against Costs of Managing Yourself

Evaluate MSSPs against estimated cost of doing all these functions yourself.

When evaluating managed service providers, look for experience rolling out a mobile security program globally, at scale. Review proposed service level agreements (SLAs), paying particular attention to mean time to contain security events on mobile platforms. Finally, pay attention to experience level agreements (XLAs) for end users. At the end of the day, mobile device management should be a company value multiplier for both the end user and the business.

Effective mobile device management should ultimately help companies deliver better value to both their employees and customers, and do this in a cost-effective manner. Done right, effective mobile device management can help positive business transformation.

About Nemertes: Nemertes is a research-based advisory and consulting firm that analyzes the business value of emerging technologies. Since 2002, we have provided strategic, client-centric recommendations based on data-driven operational and business metrics to help organizations deliver successful technology transformation to employees and customers. Simply put: Nemertes' better data helps clients make better decisions.