The Security Challenges (and Solutions) of Enterprise Mobility

MERIT SOLUTIONS

Content

1. Introduction

For all of its benefits, enterspise mobility comes with some significant security risks. There are the physical risks of a device becoming lost or stolen and there are the digital security threats of viruses and malware. Moreover, how does a company contend with the conundrum of storing corporate data safely on an employee-owned device? That in turn raises the question of which mobile devices are appropriate for use in the enterprise. Faced with all of these issues, it is not surprising that many businesses would rather ignore enterprise mobility altogether. However, that isn't a good strategy, either. Enterprise mobility is now a fact of life, security risks and all. The good news is that these challenges are not insurmountable.

One of the solutions that helps overcome the hurdles of enterprise mobility is mobile device management (MDM). MDM is a software tool that allows companies to keep their important data secure while enabling the productivity and efficiency of a mobile workforce. This software distributes applications, data, and patches. It also configures enrolled mobile device settings according to the user's specifications.

While technology plays a large role in MDM, there is a human component as well. Employees at every level of the firm's hierarchy need education about safe mobile device usage. They must understand how to secure their devices. Also, they should be taught to avoid certain behaviors, such as installing unauthorized applications, connecting to unsecured networks, or transferring sensitive data outside of the network.

Above all, employees need to know why mobile device security matters. They might not understand that malware can affect more than just an individual mobile device. It might not occur to them that a security breach due to leaked data can cost the company millions, not just because it will lose customers, but because its reputation will suffer dramatically. Everyone at a firm is responsible for implementing mobile device security policies, from the top down.

2. What Security Threats Will Mobile Devices Face This Year?

It's never too early to start thinking about the security threats your company will face this year. Expect one of the biggest security threats to come from mobile devices. So many people use them, especially for business. As a result, criminals have taken a greater interest in attacking mobile devices.

So what threats should you look out for this year?

Backdoor Attacks

In technology, a "backdoor" refers to an application that allows remote access to a device. Backdoors are especially vulnerable to attacks.

Hackers can easily leverage backdoors to access a device or even an entire network. Because mobile devices have so many apps that enable remote access, they're a goldmine for hackers.

What can you do to prevent such attacks? Select a strong security solution that monitors hidden gateways into the network.

Hacking Mobile Payment Services

Mobile payment services are becoming increasingly popular. Unfortunately, that means that they'll too be targeted by hackers and criminals.

Digital security expert Min-Pyo Hong believes that hackers will analyze services such as Apple Pay and Samsung Pay to bypass security and exploit vulnerabilities. Once they've done that, they can steal users' credit card information and commit fraud.

Mobile Web Browser-Based Hacks

Hong also predicts that hackers will take advantage of the vulnerabilities inherent in mobile web-based browsers. When a hacker attacks a device through a mobile web-based browser, he or she can bypass system-level security measures.

The security expert has even more bad news: he expects security analysts and hackers to expose even more vulnerabilities in mobile web-based browsers, and foresees this problem will plague mobile device users for years to come.

Remote Device Hacking and Eavesdropping

Android devices have gained a huge following in recent years. They're easy to customize... and easy to hack. If a handset includes preloaded apps that haven't been validated by Google, then it's a security risk. Hong sees the proliferation of Android devices as being directly related to the rise of Man in The Middle Attacks (MiTM) on mobile devices. During an MiTM attack, the hacker intercepts data traveling over unsecured wireless networks.

Mobile Data Risks in Healthcare

Many healthcare providers now use mobile devices. These devices enable them to deliver better care to their patients. Mobile devices also represent an enormous security risk.

Security expert Chris Bowen cites several threats to mobile devices used in the healthcare field: employees not adhering to policies, infrequent patching, misconfiguring servers, accidentally posting private information, and security testing that uses live personal information.

Bowen notes that healthcare provider organizations have a great deal of work to do in order to secure mobile devices. They need to invest in strong security tools and make sure that the correct patches are applied frequently. Furthermore, healthcare provider organizations must educate users about the importance of following policies and preserving private information.

Personal health information has high value to hackers, so expect mobile data risks to dog the healthcare industry for a long time.

3. Are You Prepared for a Mobile Device Data Breach?

Analysts from Gartner have predicted that by 2021, the focus of endpoint breaches will be predominately mobile devices such as smartphones and tablets.

The growing number of mobile devices makes the threat of data breaches ever more likely. Many of these data breaches won't be the result of hackers, say Gartner analysts. They believe that 75% of breaches will be due to the misconfiguration of mobile apps.

With these sobering statistics in mind, businesses can no longer say, “Data breaches can’t happen here.” Not only are data breaches possible, they are probable. Organizations must implement a plan to prevent data breaches, although they must also have a strategy in place for when a data breach takes place.

What to Do after a Data Breach Takes Place

Once you have determined that a data breach affecting mobile devices has taken place, there are several critical steps you must take to mitigate the damage.

The first step is to determine how the breach took place. Was it the result of a lost or stolen device? Did a hacker launch an attack on your company?

Secondly, the corporation’s security team must figure out the extent of the breach. They should be able to assess what information was on the device, the sensitivity of the data, whether the data was encrypted or not, if the device and information can be recovered, and whether or not further data will be exposed.

Similarly to a network data breach, the third step is to fix the problem. When it comes to mobile devices, a two-pronged approach might be necessary. Implementing an enterprise mobility management system is part of the solution. This software protects confidential corporate information, determines which apps are safe, and allows users to access shared content without putting the company at risk.

However, it is equally important to educate users about device and data loss prevention. A knowledgeable workforce is the first line of defense against threats.

Notification about Data Breaches

Many jurisdictions have enacted legislations requiring organizations to notify people affected by a data breach. Companies that have suffered a data breach might have a legal responsibility to carry out these notifications. And if the organization operates in more than one jurisdiction, it might be subject to different notification requirements.

How do you know what your legal obligation for notification is? Consult your legal counsel in each relevant jurisdiction. Your legal team will be familiar with the legislation regarding data breach notification (which continues to evolve on an annual basis in order to keep up with technology).

Even if you’ve fixed the problem that led to the data breach, you cannot sweep it under the rug and pretend it didn’t happen. There are harsh penalties for failing to comply with notification regulations. While your corporate reputation will suffer because of the breach, not following the law will worsen the situation.

4. App (IN)Security: A Hidden Threat

The mobile apps you use every day are an amazing tool that keep you productive and engaged with your work. They can also be a massive security threat. The risk mobile apps represent isn’t necessarily from malware or viruses; much of the time, user behavior is the bigger problem.

Below are some of the greatest risks connected to mobile apps and what to do to protect your company from them.

Personal Apps that Mine Corporate Data

There are many mobile apps out there which are perfectly safe...until the user permits them to transmit data from his or her device. That's when the problems start.

Some mobile apps need information available on the device or on a network in order to function. However, the user doesn't have any idea who's accessing and utilizing information, nor to what end. The app could be transmitting valuable corporate data to cybercriminals or hostile foreign governments.

What steps can you take to prevent this situation from becoming reality? Educate your employees about the risks apps pose. Explain to them that they shouldn't give permission to apps to transmit data, because it could fall into the wrong hands.

Hostile Enterprise-Signed Apps

In a way, these apps are similar to the applications mentioned above. They rely upon distribution code native to widely used mobile operating systems (such as Android and iOS) to send data outside of a network, into the waiting arms of cybercriminals or corporate spies.

Again, user education is crucial to preventing the impact of hostile enterprise-signed apps. Tell your employees that they should give their apps the minimum amount of necessary permissions. If the app is asking for more permissions than seem unreasonable, don't give in.

Running Apps that Haven't Been Updated

App developers are under a great deal of pressure to bring their product to market as quickly as possible. As a result, they don't always have the time to spend on updates to apps that would make them more secure and less prone to malware and other security threats. Furthermore, users don't realize that updating their apps is important. So, even if there is an update floating around out there, chances are they haven't bothered installing it. If user education sounds like a recurring theme, it is. Explain to your employees why it's critical to update their apps, and to choose apps from developers that they know will have frequent updates.

Downloading Suspicious Apps

Some people would never fall for an email phishing scam, yet they'd readily click on a link to download an app they received in an SMS on their smartphone. These people also see nothing wrong with downloading an app they found outside of an app store.

Yet again, user education about choosing safe apps is vital. You can also use technology to prevent suspicious apps from wreaking havoc on your network by implementing a mobile application management (MAM) system. This software creates a list of trusted apps and distributes them to corporate user devices.

5. Mobility, Security, and Collaboration: The Challenge for the Enterprise

This scenario is probably quite familiar: your colleague has sent you a PowerPoint presentation to review before your team's presentation. You decide you'll look at it on your tablet during your subway commute. When you open the file, all you see is garbled font. What about those images your co-worker spent so long creating? They don't appear. Mobile device users have been frustrated that their smartphones or tablets make it difficult for them to collaborate on a document. Viewing, annotating, editing, and sharing are activities that don't seem to work as well on mobile devices. Many app developers have attempted to solve those problems with apps that make viewing, annotating, editing, and sharing easy. Those apps represent another issue, though – none of them are built with enterprise security in mind. How do you enable employees to collaborate effectively yet securely?

Securing Mobile Collaboration: Two Approaches

Currently, companies have two paths they can take to enabling secure mobile collaboration. The first path is to choose a solution that offers all of the capabilities users need in order to collaborate efficiently and effectively with their mobile devices.

Doesn't the first path sound perfect?

You might be wondering why anyone would bother implementing any other solution. Here's the problem: there aren't that many solution providers that offer a secure mobile collaboration solution. And you might discover that the "perfect solution" lacks an important capability such as annotation.

That's why many companies wind up along the second path. Instead of implementing one solution that does everything (or almost everything), they deploy multiple apps through an app store. They also use an enterprise file sync and share solution.

The second approach has its drawbacks, too.

Having to use several apps in order to achieve the simple tasks of viewing, annotating, editing, and sharing has a negative impact on user experience. Furthermore, IT administrators must ensure that they have added all of the correct apps to the app store. For example, certain firms require the use of watermarks on documents to prevent data leaks. As such, IT administrators need to be certain that they have that app available before users need it.

Collaborating Securely through Mobile Devices: An Emerging Field

Although mobile devices have gone from being a nice-to-have to a critical need for the enterprise, they're still a maturing technology. Humans continue to test the limits of their capabilities.

Secure mobile collaboration is in its infancy as well. It will take solution providers time to develop effective, efficient approaches to collaborating through mobile devices in a secure manner.

What can businesses do in the meantime? They should choose a solution that offers the best possible user experience while ensuring that security is a top priority. Selecting a solution that will integrate with current infrastructure investments is also crucial. Becoming locked in to a single vendor isn't a good idea, because it doesn't give you the flexibility to choose a better solution when one comes along.

6. Taking Control of BYOD

Before the proliferation of smartphones and tablets, employees had no choice in what type of device, let alone platform, they used to do their job. The IT department made that decision for them. And if the employees didn't like what the IT department chose, too bad.

Those days are over. The rise of BYOD means that employees at every level of a company's hierarchy have the unprecedented freedom to choose their device and platform. However, unprecedented freedom isn't always a good thing. In this case, BYOD can be a nightmare for IT departments. Who is responsible for providing technical support for these devices, which allow users to access corporate data and store personal information? How does the IT department keep corporate data secure? Moreover, how does an IT department cope with the vast array of devices and platforms which employees bring to work?

For IT departments at large companies, dealing with BYOD can be overwhelming. Fortunately, there is a solution to the headaches that BYOD can bring. Mobile device management (MDM) is a software tool that allows companies to keep their important data secure while enabling the productivity and efficiency of a mobile workforce. This software distributes applications, data, and patches. It also configures enrolled mobile device settings according to the user's specifications.

The best MDM solutions allow IT administrators to monitor mobile devices on the network in the same way that they can see PCs and other equipment. In addition, they ensure that devices operate at their optimal capacity, so the MDM should be able to quickly push out performance updates and monitor devices for any issues that would interfere with the devices working well. When searching for an MDM solution, firms should also look for application management, file synchronization and sharing, data security tools, and a wide variety of supported devices and platforms.

Another approach to BYOD is called the corporately owned personally enabled (COPE) method. Instead of employees bringing whatever device they want to work, the employer either provides them with the device, or they can choose from a list of pre-approved devices that the IT department will support. While there's an argument to be made that COPE curtails employee freedom to choose their own device, the COPE concept is a boon for IT administrators. COPE allows them to select a set of devices they can support with confidence because they have the technical or physical resources to do so. Even if an enterprise chooses COPE, it should still implement an MDM solution to provide security updates, support and other services to employees.

Technology is only part of the solution to managing BYOD (or COPE, for that matter). Education is vital to taking control of enterprise mobility. All employees must understand the risks associated with mobile device usage and how to mitigate them. It doesn't matter how good an MDM solution is. If employees find a way around it, they can put a company's network in jeopardy. Educated employees are the best way to control BYOD.

7. Is an MDM Solution Good Enough to Protect Your Company? Maybe not?

For several years, mobile device management (MDM) solutions have been touted as the best way to protect a business' mobile devices. MDM solutions are software programs that enable IT administrators to push security updates onto mobile devices, remotely wipe a device, and ensure that a device complies with security policies. Although MDM solutions haven't been on the market for very long, they're already running the risk of becoming outmoded.

Why an MDM Solution Alone Isn't Enough

The purpose of MDM solutions is to safeguard devices. Devices are important – no one is denying that. However, when you only focus on protecting devices, you lose sight of other elements that endanger enterprise digital security.

What else is critical to security? There are two things: applications and content. Applications enable employees to collaborate and communicate quickly and effectively. They can also conceal viruses and other threats which could wreak havoc on your network. Mobile application management (MAM) solutions provide IT administrators with control over apps. They can place apps on whitelists or blacklists and decide which apps should be allowed in the corporate app store.

What does content have to do with security? Like applications, content management systems or repositories store valuable business data. You don't want someone who isn't authorized to be viewing confidential information. A mobile content management (MCM) solution provides secure access to content repositories such as SharePoint as well as the ability to share files safely.

Enterprise Mobility Management: A Better Security Solution

Some businesses are beginning to realize that their information should be protected to the same extent their devices are. They're beginning to turn to vendors for enterprise mobility management (EMM) solutions.

EMM solutions refer to technology that combines MDM, MAM, and MCM. They provide more complete protection for devices as well as data.

Which EMM Solution Is Right for My Company?

Vendors also understand that EMM solutions are becoming an important product to offer business customers. There's no shortage of them on the market today. With that in mind, how do you find the one that's best for your firm?

To determine which EMM solution you should select, you must carefully evaluate your needs. Ask yourself which devices you should be concerned with – those belonging to employees, customers, contractors, or business partners? Furthermore, what types of devices do you need to support? Bear in mind that what you answer now might not hold true in a few years. You want a solution that will grow with you, not keep you locked in to a device or platform.

Also, don't limit yourself to mobile devices such as smartphones and tablets. Wearable devices, such as smart glasses and smart watches, could become a fixture in the enterprise. They will also need to be secured.

User experience matters, too. Security tools become meaningless if they hinder performance. Strike a balance between a great user experience and protecting your corporation's data.

8. What Are the Two Things That Protect Your Mobile Network?

What if you could prevent threats from destroying your network? You would jump at the chance to keep one of your most important assets safe, wouldn't you? There are many IT professionals who understand the necessity of protecting their computer networks. However, it might not occur to them that they need to shield their mobile networks, too. When it comes to mobile network protection, there are two components: technological and human. Read on to learn how these complementary factors are vital to safeguarding mobile networks.

Technological Protection

As the name implies, technological protection of mobile networks involves a software or hardware solution that will defend them against threats. There are a number of these solutions on the market today.

These solutions scan the network and identify any data that appears anomalous or threatening. Then, they will quarantine those packets so that they can't infect the rest of the network. They know that those data packets might be threats because the solutions come with a database (that's constantly being updated) of malware, viruses, and anything else that will harm your mobile network.

The Human Touch

Human beings, of course, are the users of mobile devices. They're also the ones who create the threats that imperil mobile networks. And, of course, they're the ones who (many times unwittingly) unleash havoc on the networks by infecting them.

How can humans pose less of a menace to the mobile networks designed for their benefit? They need to modify their behavior. In order to do that, people need to be made aware that their behavior is problematic.

What types of human behavior jeopardize networks? They download files or apps from questionable sources, they lose their mobile devices, they damage their mobile devices - the list could go on. While virtually everyone knows that if you drop your phone, it doesn't bounce, many people don't realize that some of the other things they do on their mobile devices could be putting their hardware and their corporate network at risk.

Businesses must educate users about the danger mobile threats pose. Moreover, the company's leadership needs to explain exactly why this matters so much. When a network suffers a security breach, the firm's reputation suffers. In addition, it could face penalties if hackers stole sensitive data.

Which Form of Protection Matters Most?

Your mobile network protection relies on two components: people and technology. They both matter equally. Your mobile network is vunerable when those two things aren't in place.

You might be reading this and thinking, "Why do I need fancy technology if my people understand how to protect themselves?" Well, sometimes people slip up. A mobile threat detection system protects your network no matter what.

"Why do I need to educate my people, then?" you may ask. Your employees won't understand why safeguarding the network is vital if you only put a technological solution in place. They might find a way to get around it by bringing in devices that aren't covered by the software.

9. Mobile Security: A Business Enabler, Not a Cost Center

If your organization hasn't implemented a mobile security solution, ask yourself - "Why not?". Chances are that the answer will come down to cost. Many organizations do not invest in this technology because they believe that it will be an unnecessary expense.

This mindset does more harm than good. When businesses defer implementing an EMM solution (or decide not to implement one altogether), they are only saving money in the short term. The cost of implementing an EMM solution is far less than the price tag of a data breach. Firms don't take into account the impact of reputational damage, forensic analysis, fixing the security problem that caused the breach in the first place, and possible financial penalties for allowing sensitive data to be compromised.

The right EMM solution is an investment in a company's future. It will protect the business from threats that could completely cripple it. The right EMM solution enables an organization to continue its operations without hassles or delays. Don't let your organization become a statistic because of the misguided and shortsighted belief that it can save money by neglecting mobile security.

Life Sciences organizations have to account for a lot of moving parts when trying to ensure they have a future-proof infrastructure. Maintaining and simplifying regulatory compliance, enhancing operations both digitally and by weeding out inefficiencies, and taking the steps necessary for growth – these are all steps which require a highly coordinated approach.

Thanks to Merit's industry leadership, Life Sciences strategic partnerships, and delivery methodology, we feel confident we are the right partner to support you on your path toward success.

Visit www.meritsolutions.com to find out how we can help your transformation initiatives.