Surviving the iPocalypse: Mobile Device Security

Version 1.1

Released: January 21, 2011

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051 info@securosis.com www.securosis.com

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog <http://securosis.com>, but has been enhanced, reviewed, and professionally edited.

Licensed by McAfee

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the Web more securely. Backed by unrivaled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee secures your digital world. For more information, visit www.mcafee.com.

Copyright

Table of Contents

I Can Haz Your Mobile

In the olden times, life for IT professionals was much easier. Keep the systems up and play some Tetris. Now we have all of these attackers and compliance and cloud thingys. It's enough to drive someone crazy. We also used to just have to worry about computers. You know, traditional desktop and laptop devices. Now, not so much. Given that pretty much all the smart phones out there are as powerful as the computers we used 5 years ago, clearly mobile devices are the next frontier for badness. We can call this the iPocalypse.

We can probably consider ourselves more lucky than good that we've been spared a truly problematic mobile attack to date. Luck is no better a strategy than hope. So in this paper let's outline some of the realities of protecting mobile devices.

You've Lost Control: Accept It

You may have missed the obituary, but control of devices was pretty well staked through the heart by the advent of cool iDevices.

First let's point out the elephant in the room: Control. If you feel the need to control your end-user computing environment you are in the wrong profession. The good old days of dictating devices, platforms, and applications are gone -- along with the KGB interrogation lights. You may have missed the obituary, but control of devices was pretty well staked through the heart by the advent of cool iDevices. Yes, I'm talking about iPhones, iPads, Androids, and Palms. OK, Palm not so much, but certainly the others. Some smart IT folks realized, when the CEO called and said she had an iPad and needed to get her email and look at those deal documents, we were entering a different world.

Lots of folks are calling this *consumerization*, which is fine. Just like anything else, it needs a name, but this is really just a clear indication that **we have lost control.** But you don't have to accept it. You can try to find a job with one of the five or ten government agencies that can still dictate their computing environment (and good luck as they move all their stuff to the cloud). But the rest of us need to accept that our employees will be bringing their own devices onto the network, and we can't stop them.

So we first need to figure out what the big deal is. How many ways can this consumerization wave kill us? And yes, you need to know. Sticking your head into the sand like an ostrich isn't a viable option.

Risks to your Mobile Devices

As always, you need to start any security-oriented program by understanding the risks you face. To be clear, a lot of these risks aren't necessarily caused by the *bad guys*, but security folks already knew that. Our own people tend to do more damage to our systems than any of the attackers. So we'll cover a mix of external and self-inflicted wounds.

Data Loss

The first issue with having key people (or even non-key people) access your company's stuff using their own devices is data security. Clearly things like email and the fancy iPhone app from your CRM vendor are driving 24/7 access via these devices in the first place. So thinking about data loss is tops on the hit parade:

- **Device Loss:** You'll be amazed at the number of ways your employees lose mobile devices. It's not impossible to leave a 17" laptop in an airplane seat, but it's hard. Leaving smartphones I-don't-know-where happens all the time. And Find My iPhone won't save you when the battery dies or the thief engages airplane mode. So you have to plan for the fact that these devices will be lost with sensitive data on them, and you need to protect that data.

- **Device Sale:** Oh yeah, these devices are owned by employees. So when they feel the urge to buy the new Shiny Object, they will. Those crazy employees usually find a buyer on eBay or Craigslist and send them the old device. Will it be cleaned? Definitely possible! Is it more likely to have your Q4 forecast on it? Don't answer that, but make sure you have some way to address this.

Malware

You can't discuss security without at least mentioning malware. So far attacks on smartphones have been relatively tame. But it's not smart to build a security strategy on a bet that they will remain tame. Again, hope is not a strategy.

- **Weaponized Exploits:** To date there hasn't been much malware targeting mobiles, although sites like jailbreak.me show what is possible. So it's not a matter of *if*, but *when* some self-proliferating exploit will make the rounds and spread like wildfire.

- **App Store Mayhem:** Sure, all these app stores include controls to ensure malware doesn't make its way onto authorized applications, but you have to expect that at *some* point, one of these process will experience a breakdown (even if it's just an obscure third-party store operator losing their keys), and something bad will get in. And if it's a widespread application? Right: mayhem and anarchy, which is always 'fun' for us security folks.

- **Jailbreak:** Remember, these devices are not owned by your organization. So employees can consciously decide to bypass whatever security controls are built into the platform. They don't necessarily care that jailbreaking basically obviates all security controls you might be counting on.

Are you having fun yet?

Manageability

Finally, let's talk a bit about the complexities of managing thousands of devices -- some you own and some you don't. And sure, that's not really a security issue until you mess up a configuration and open up a huge hole on the device(s). So managing and enforcing policies is critical to maintaining any semblance of security on these devices.

- **Misconfiguration:** What happens when you get 20 different device types with 5 different versions of operating systems, and 25 different apps (that you care about) running on each? Configuration nightmare. This is where automation becomes critical, because configuration errors enable many successful attacks.

- **Patching:** Remember each smartphone is a computer, and every so often the vendor will find a thing or two (or forty) that must be fixed. And believe me, the only time they fix something is when it represents clear and present danger. So in many cases not patching is a very bad idea. This is easier said than done, however, when you don't control the device.
- **Network Hijinks:** Remember that these devices all include WiFi radios, which means their access to all your critical data will connect to the network via the cyber cesspool of public WiFi. You need to factor in what types of connectivity make sense -- and more importantly which don't.

Of course, this isn't a comprehensive list, but should be enough to make sure that any chance of you sleeping well is pretty much gone. Now that you know what you are up against, what can you do about it? At Securosis, we recommend a two-pronged attack, one hard (involving technical controls) and the other softer (process and communication).

Saying No (without saying no)

Let's face facts here. You aren't going to tell your CEO or any other exec 5-6 pay grades above you that they can't use their iPad to access the deal documents on that multi-billion dollar acquisition. You know it's much easier to read an iPad on the can, than to lug the laptop around when taking care of business, right?

If you are like most security professionals, your first instinct is to blurt out a resounding **no**, when presented with a request to connect an Android phone to your network. But your instincts are wrong. That wasn't a question. It was an order -- or soon will be. So your best bet is to practice the deep breathing exercises your meditation guru suggested. Once you've gotten your pulse back to a manageable 130, then you can and must have a constructive discussion about what resources are needed on the smartphone and why.

You know it's much easier to read an iPad on the can, than to lug the laptop around when taking care of business, right?

User Profiles Are Your Friend

The (sometimes fatal) mistake we see most often is treating every user as equivalent to every other user with the same device. This leads to providing the same level of access, regardless of who the user is. How about an alternative? Profile users based on what they need to get, define 3-4 user types, and build your policies based on what they need, not what devices they have.

For instance, you might have three user types:

1. **Executive:** These folks can crush you with a stroke of their pen. Okay -- a pen is old school. How about a click of their mouse? These people get what they want because saying no is not an option. They should be configured for email and document access, with a VPN client so they can access the corporate network (from the can).

2. **Connected Users:** There will be another group of users who might have compromising pictures of the executives. Or maybe they actually provide tangible value to your organization. Either way, these folks need access, but probably not to everything. Design the policy to give them only what they need, and nothing more.

3. **Everyone else:** If a person doesn't fit into either of the other two buckets, then you give them access, but not enough that they can hurt themselves (or you). That means email, but probably not VPN access to the corporate network.

These buckets are just examples -- you'll need to go through the use cases for each type of job function and see what levels of access make sense for your organization.

Yes, but...

As we mentioned above, your first instinct is likely to say 'no' when asked to support smartphones. But let's tune the verbiage a bit and say **"Yes, but"** instead. After this easy mantra, go into all the reasons why it's a bad idea for the user to have smartphone access to the organization's sensitive stuff. You aren't telling them no, but you are trying to convince them it's a bad idea.

But let's acknowledge the truth: you'll lose and the requestor will get access. The goal of this exercise isn't necessarily to win the argument (though being able to block someone's every so often access is good for your self-esteem), but instead to get folks put into the right user profile buckets. Everyone wants access to everything. But we know that's a bad idea, so success is really more about how many users (as a percentage of all smartphone users) have limited access. That number will vary based on organization, but if it approaches 0% you need to practice "yes, but" a lot more.

Cover Your Hind Section

The last suggestion we'll make relative to process is to ensure that you have documented the risks of supporting these devices. It's critical to understand that our job as security professionals isn't to stop business from happening -- it's to provide information to the decision makers so they can make rational, educated decisions. That means you need to inform them of the risks of whatever action they are going to take and push them to acknowledge the risk.

If you fail to do this, you'll be the one thrown out of the car at high speed when something goes wrong. Without ensuring clearly, and in writing, that everyone understands all the things that can go wrong by taking a particular action; you'll end up in the proverbial creek without a paddle.

Acknowledge that you won't like all the decisions. Your job is to protect information and that requires reducing risk. Every company needs to take risks to continue to execute on their business plans. These two goals are diametrically opposed, but at the end of the day, it's not our job to decide what risks make sense for your business. It's our job to make sure everyone is clear on what those risks are, and enforce the decisions.

As helpful as it is to put users in specific profiles, there are still a number of things you can do technically to protect your organization from the iPocalypse.

5 Tactics to Protect Those Buggers

Given that we've tackled the threats these new ~~handheld computers~~ mobile devices present, as well as how we need to deal with folks culturally when they demand access to sensitive corporate information on mobile devices. Now we can talk about a few things we can do to protect these devices.

As we all understand that these mobile devices are really handheld computers, we need to think about the tactics that are successful for securing our more traditional computers. Admittedly, 'successful' may be a bit optimistic, but there are still many lessons we can learn from the controls we use to protect laptops. Some of these fall into a traditional *security* technology bucket, while others tend to be more operational and management oriented. But really, those distinctions are hair-splitting. Things like secure configurations and access policies contribute to the safety of the data on the device, and that's what's important.

Tactic 1: Good Hygiene

You hate it every time you go to the dentist and see the little sign: *Only floss the teeth you want to keep*. You may not like it, but it's true. And the same goes for protecting mobile devices. We need to have a strong posture on these devices, in order to have a chance to be secure. These policies won't *make* you secure, but without them **you have no chance.**

1. **Strong Passwords:** If you have sensitive data on your mobile devices, they need to be password protected. Duh. And the password should be as strong as practical. Not a 40 digit series of random numbers. But something that balances the user's ability to remember it (and enter it *n* times per day) against the attackers' ability to brute force it. And you want to wipe the device after 10 password failures or so.

2. **Auto-lock:** Along with the password, the device should lock itself after a period of inactivity. Again, finding the right setting is about your users' threshold for inconvenience, the length of their passwords, and your ability to dictate something secure. 5-10 minutes is usually okay.

3. **Data encryption:** Make sure the device encrypts data on it. Most mobile devices do this by default, but make sure.

4. **Approved Applications:** There are some applications that exhibit bad behavior and you may not want to allow employees that have access to sensitive corporate data to load those applications on their mobile devices. That's a good thought, but in practice, you have to remember that these devices belong to the employee, so it's not clear you can dictate what they can and can't run. That being said, you certainly can tell them they can't have access to corporate data if they insist on running a specific application. Yet another example of "yes, but."

Continuous Hygiene

With your dentist, doing a good brushing right before your appointment probably won't going to fool him or her if you haven't flossed since Reagan was president. But unless you are checking constantly whether the mobile device remains in accordance with your configuration policies, you can be fooled. Just because you set up a device correctly doesn't mean it stays that way.

For traditional networks, a technology like Network Access Control (NAC) can be used to check a device when it joins the network. This ensures it has the right patches and right configuration, and has been scanned for malware, etc. You should be doing the same thing for your mobile devices. Upon connecting to your network, you can and should check to make sure nothing is out of compliance with policy.

This helps block the user who gets his device from you and promptly jailbreaks it. Or does a hard reset to dump the annoying security controls you put in place. Or the one who turned off the password or auto-lock because it was too hard to deal with. Remember, users aren't as dumb as we think they are. Well, some aren't. So some of them will work to get around the security controls. Not maliciously (we hope), but to make things easier. Regardless of the security risks. Part of your job is to make sure they don't manage it.

> *Remember, users aren't as dumb as we think they are. Well, some aren't.*

Tactic 2: Remote Wipe

Despite your best efforts, some users will lose their devices. Or their kids will drop them (especially the iDevices). Or they'll break and be sent in for service. However it happens, the authorized user won't be in control of their devices, and that introduces risk for you. And of course they won't tell anyone before sending the device is into the shop, or losing it. So we get a memo asking for a replacement/loaner because they have to access the deal documents in the can.

You need the ability to eliminate the data on the device remotely. This doesn't have to be complicated, right? Authenticate properly and nuke it from orbit. Hopefully your user backed up his/her device, but that's not your issue. Ultimately if there is sensitive data on the mobile device, you need to be able to wipe it from anywhere in the world. Though do understand you will create tremendous angst if a device is wiped and the employee loses pictures/videos, etc. So make sure to communicate clearly that in the event of a data issue, you have the right (and responsibility) to wipe the device, even if it means the employee could lose some personal data. Then again, they have the choice of whether to use their device to access corporate data. Right, another example of “yes, but.”

One caveat here is that in order to wipe the device you must be able to connect to it. So if a savvy attacker turns it off, or puts it into airplane mode or something, you won't be able to wipe it. That's why having an auto-wipe policy in case of 10 password failures is critical. At some point, someone will try to get into the device, and that's when you want to destroy the data.

Tactic 3: Lock down Network Access

It's no secret that most public wireless networks are the equivalent of a seedy flea market. There are some legitimate folks there, but most are trying to rip you off. And given the inherent bandwidth limitations of cellular data, most users leverage WiFi whenever and wherever they can. That creates risk for us, who need to protect the data.

> *...most public wireless networks are the equivalent of a seedy flea market. There are some legitimate folks there, but most are trying to rip you off.*

So what to do? Basically, get a little selective about what networks you allow users to connect to. You can enforce a policy to ensure any WiFi network used offers some kind of encryption (ideally at least WPA2) to avoid snooping the network traffic. Or you can VPN all the devices' network traffic through your corporate network, so you can apply your web filtering and other protections, with encryption to rebuff sniffers.

Unfortunately this isn't easy to swing in reality. Remember, these devices don't belong to your organization, so mandating that all network traffic goes through your network may not fly. In that case, what you can do is make sure that any inbound traffic to sensitive information goes through a virtual private network (VPN). This way you can require strong authentication and an encrypted tunnel to make sure that it's the right person, and only the authorized users gets access to your corporate data.

Most of the large network security vendors provide a mobile device VPN client to force a secure connection. This is something you should strongly consider.

Tactic 4: Support Technologies

Although not a traditional security capability, being able to support these mobile devices will contribute as much (if not more) to your ability to protect the data as anything else you can do. Why? Because if a user can quickly have you unlock their device if they forget the password, it becomes easier to enforce a strong password policy.

If they have trouble connecting to a network because you require the VPN, you've only got one shot before they actively work to get around your security controls. So basically, by making sure their user experience isn't adversely impacted by the additional protection, you are giving your security controls a much better chance to succeed.

Tactic 5: Reporting

Finally, we have to mention the *C word*. No, not *that* C word -- I'm talking about Compliance. Regardless of the business you are in, the reality is that you are likely dealing with some kind of regulatory oversight. And that means you'll need to prove to an assessor (or 8) that the private data on those mobile devices is protected. Which ultimately means you need to be able to generate reports about what you are doing. The good news is that any technologies you'd consider for any of the other tactics will be able to generate the reports you need. But keep in mind the need to document what you are doing when you are setting them up.

Tool Anarchy

Odds are you have a lot of other devices and tools in place to protect your infrastructure and devices. Just as it's a hassle to have to manage thousands of devices, it's also a hassle to manage 10 different tools separately. Any advantage you may get from more effectively managing these devices could be offset by the overhead of managing yet another tool. So another consideration should be the degree of leverage you can achieve when managing mobile devices.

To be clear, you shouldn't default to a strategic vendor's tool, if it doesn't meet your requirements. But all things equal, having leverage in managing all of your security tools will make life easier. And we all want a life that easier, right?

Wrapping Up

As we've discussed, it's not a matter of **if**, but **when** you'll need to provide access to critical corporate information on mobile devices. Saying 'no' is not an option. "Yes, But..." helps you ensure folks have legitimate reasons before providing access, but you'll still have to build a plan to support these devices.

That means you need to keep apprised of the current attacks being used against mobile devices, and also that you need to pay attention to both the process and the technologies used to protect them. Along with all the other stuff on your plate every day. Have fun with that.

About the Analyst

Mike Rothman, Analyst/President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security, such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and a networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held VP Marketing roles at CipherTrust and TruSecure — providing experience in marketing, business development, and channel operations for both product and services companies.

After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy and CMO at elQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published *The Pragmatic CSO* <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, L.L.C. is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services.

Our services include:

- *Primary research publishing*: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements, and follow our Totally Transparent Research policy.
- *Research products and strategic advisory services for end users*: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessments.
- *Retainer services for vendors*: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Example services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluations, and merger and acquisition assessments. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.
- *External speaking and editorial*: Securosis analysts frequently speak at industry events, give online presentations, and write and/or speak for a variety of publications and media.
- *Other expert services*: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These services tend to be customized to meet a client's specific requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis.

For more information about Securosis, visit our website: http://securosis.com