Securing Mobile Devices aka BYOD
Transcript

Part 1: Motivation for BYOD; Policy and Practices

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Program is part of the Software Engineering Institute. We are a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a principal researcher at CERT working on operational resilience. Today, I'm very pleased to welcome my colleague, Joe Mayes. Joe is a member of CERT's Cyber Workforce Development team.

And today Joe and I will be discussing a really hot topic, I think -- some of the actions that organizations should take to help secure users' personal devices. Often in the press this is referred to as BYOD or "bring your own device." And certainly we're all interested in being able to use our own personal devices in the workplace.

So welcome, Joe, really good to have you on the podcast series.

Joe Mayes: Glad to be here.

Julia Allen: So, always good to start with some definitions. So from your frame of reference, what is BYOD and why do you think, what do you observe as the interest growing in such a significant way in BYOD?

Joe Mayes: Well BYOD is the concept of people bringing their own portable computing device, in most cases. I mean technically it can be a desktop but I don't see many people dragging their desktops from home to the office.

But now that we have portable devices where we have all the power of a desktop in a handheld, in a phone, in an iPad, people are really tempted because they like the freedom they get in their own personal lives to be able to access anything, anytime, anywhere, and they want to be able to do the same thing with their work.

They don't want to have to carry around another piece or they don't want to have to find other ways, other more cumbersome ways, to have to get back to work when someone from work calls and says "I need your help" on whatever.

Julia Allen: So as you travel around, I know you do lots of teaching. Over the last couple of years, have you noticed a real uptick in people using their own devices? Have you seen a significant change?

Joe Mayes: Yes I have. I've spent a lot of time in the work environment, and I also spend a lot of time in the military in the Army Reserves. And what I saw in the military was it was key leaders who were the first people to do this. There were no policies on mobile devices or BYOD or anything like that. But the military has a funny rule and the rule is "The general gets what the general asks for."

So when the general says that he wants to have a Blackberry, then he gets a Blackberry. When President Obama said, "You're not going to take my Blackberry away from me" or "You're not going to take my mobile phone away from me," suddenly they found a way to accommodate the president of the United States.

And that just trickled down now to regular employees, regular users, and regular businesses. They all want to be able to do the things that they feel they need to do, but they only want to have one device to do it rather than having two phones on the belt or dragging two computers behind them or anything like that.

Julia Allen: Right, so I think you touched on a key topic which is policy. And often we know policy lags actual use. But as you reflect on some of the key topics for a BYOD security policy, what are some that occur to you?

Joe Mayes: Well in the beginning, the first one is do you allow anything to touch it at all? Do you actually allow BYOD? Some places do, some places don't, and some places may never be able to. But you have to make that decision.

Once you've made the decision that says yes, we want to at least support BYOD, then the next question becomes what do you allow people to connect to? How trusted are they? Do they get to access email? Do they get to go a little farther and get the internal website? Do they get to access data on the corporate servers? Do they get to do queries? Do they get to actually run machines? How far does this go? This is not an on-off switch, and one of the first questions is how far do you let people get?

Julia Allen: Right, so I know access is clearly probably the most critical topic, but are there other topics that you think a policy needs to address once you've established what some of the access requirements should be?

Joe Mayes: Yes, when you give people access, the next question is what can they do with that access? In the world of computers and data, do they have read-only or do they have read-write? Can they change documents? Can they delete documents? Add documents? Can they bring in things from the outside?

If they want to pull queries on a corporate database, do they do that remotely or do they actually pull the database down to their mobile device so that it's with them even when they're on an airplane or disconnected? And each one of those has a different level of security and a different, whole gamut of security issues to consider.

Julia Allen: So, Joe, that was a nice summary of some of the things we need to think about with respect to policy so let's dig a little deeper and talk about practices. So what do you see as maybe a few of the most critical security practices that need to be put in place to secure the enterprise and enforce the policy?

Joe Mayes: I believe you've got some practices and policies and responsibilities that cross both sides. It's going to be some things the employer is responsible for and some things the user is responsible for.

Julia Allen: So let's start with the employer. What are the employer's key responsibilities when it comes to personally owned devices?

Joe Mayes: They need to look at among other things which devices do you want to use? Are you going to allow all devices in or just iPhones or just Androids? The more devices you have, the wider your variety is and the more different types of security issues you're going to run into and the more different types of security procedures you're going to have to learn. So some people in some companies will limit the types of devices just to limit the size of that problem.

Beyond that, when you know what devices you're going to have, probably one of the most important things is encryption. And encryption can go two ways. One is the encryption between the mobile device and the home office so that you're not leaving things exposed and vulnerable when you're going over a wireless environment or things like that.

And the other is any data or passwords or anything that you keep on the mobile device itself need to be encrypted so that if the device is compromised or lost or whatever, the data or the passwords or whatever else is not at risk.

There should also be some kind of security management. There are third party companies who set up and have security suites that will remotely manage, in an enterprise manner, all these personal devices, but the personal device owner has to let you put that software on for that to work.

Julia Allen: How about on the user side? What do you see as -- assuming that the employer does their job in terms of training and security controls and proper enforcement -- what do you see as some of the responsibilities on the user side?

Joe Mayes: Well users see these devices as tools, but they also see these devices as toys. I mean we play with them. We think they're fun. And the problem with thinking they're fun is that we tend to not always be safe with them. We don't worry about viruses because we've never seen a phone get virused. Well phones get virused every day.

Who are you connecting with? If you're out at some resort or some restaurant and you just connect to their wireless, then you're really exposing your data back through their wireless, which is why the corporate side has to encrypt things.

If your company requires password authentication, it's the same issues that you have at work. You can't put a sticky note on your phone with your password. You can't leave the passwords unencrypted. You can't click that little button that says "save this password" so that anybody who gets your device can just jump right into the corporate network.

Julia Allen: Do you find that users are typically or at least becoming more aware of their responsibilities when they're using their devices for corporate access? Or do you think that's still a learning curve that needs more attention?

Joe Mayes: Unfortunately, we are creatures of habit and what makes us change habit is some bad experience. And bad experiences can either be that you've done something bad with corporate data and now you've got a problem with your boss, a problem with your company.

Or just that people had their personal phones compromised and having lived through a compromise, having lived through an identity theft issue, or having lived through having your bank account messed with, makes you suddenly more aware that “oh, security really is real. It's not just issues that happen to other people. It happens to me too.”

And as more people -- either it happens to them or it happens to someone they know -- their attitude toward security goes from “who cares” to “now I understand why.” And that's beneficial to get the feedback and make people more likely to comply with policies and procedures to protect the data on mobile devices.

Julia Allen: Right and it seems to make good sense to me across many aspects of day-to-day life. You need something that's going to get your attention before you're really going to attend to it, right?

Joe Mayes: Yes and unfortunately that's usually a negative something.

Part 2: Deployment Challenges, Dealing with Breaches

Julia Allen: Right, right. So while we're on the topic of challenges from a corporate or institutional perspective -- as you're thinking of putting policy in place and as you're putting security practices in place, what do you see as some of the key barriers or challenges to actually making policy and practice happen?

Joe Mayes: The challenges and barriers are pretty similar to other policies that don't get followed. I mean, it's difficult for anyone to follow a policy, and it's more difficult when you keep thinking of this as being my phone or my device because you only allow people to tell you so much what you get to do with something that's yours or that you consider yours. So that makes it difficult to deal with that.

For corporate boxes, right, corporate boxes -- they have physical control of the equipment, they have physical control of the workplace, and even then, even when they own everything and control everything, they still get compromised and you still have huge data theft problems. It's even worse when you think of mobile devices that are carried around by a person.

Nobody has got real control of the environment. They may get forgotten in a bar. They may get forgotten in your neighbor's house. You may give it to your kids to play games with while you're driving somewhere. There's just so much less control and so many more ways that it can be compromised.

Julia Allen: Right so that's why I believe you said earlier, I think that's why you said really concentrating on protecting the data so the personal device just ends up being another container, another place where the data lives. But if the data is protected, then would you agree that goes a long way towards beginning to address that barrier?

Joe Mayes: It does and that's where a lot of these protection suites work because they work in the background. They work without you having to invoke them. They are automated and they just occur all the time. And those are the things that when you don't have to choose to do it right and it's just done automatically, then you're in a lot better position with regards to security.

Most of those systems also have a way that automatically remotely will wipe the data off the device. Some of them are triggered to how many days since there's been a connection or how many invalid connection attempts might have occurred. There are various trigger mechanisms that a company can choose to use that automatically just wipe the mobile device clean of all corporate information.

Julia Allen: You know that's a good point. It causes me to ask you -- do you see changes or different approaches to monitoring and logging and reviewing logs and generating alerts of bad

things potentially happening or suspicious behavior? Do you see any kind of an uptick or a change in that corporate behavior with respect to mobile devices that isn't perhaps already in place for normal desktops and laptops?

Joe Mayes: Well, you obviously have to find a way to get the mobile device to send the logs back if you want the logs to be of any value. Logging on the phone itself doesn't help if the logs never get transmitted back to someone who can review the logs.

The other issue is just from an architectural standpoint. The iPhone products have a what they consider to be a secure methodology that's not used by anybody else, and they tend to rely on that methodology. Other device owners can treat mobile devices more like other physical devices and rely on the same physical structures that we use to protect desktops and laptops and other things.

So some of it is corporate philosophy or a vendor philosophy as to what's the best way to protect something. And that's where corporations have to go back and look at what model do I want to buy into? Which models do I trust? Which models do I feel are adequate for the security that I need?

Julia Allen: Great, great, well thank you for that explanation. So I would like to explore with you to see if there are other issues that you've run across. I know one of the things as we were preparing for this podcast we talked about accidental versus deliberate data breaches. Can you say something about that?

Joe Mayes: Mobile devices have capabilities that we didn't think anything would have just a few years ago. They have phones on them. They have recording on them. They have video on them. They have cameras. They have all these methods for moving information, and the more methods you have for moving information, the more it can be used for someone who wants to deliberately move information.

So accidental misuse is one thing and we can write policies to protect against that. And people may honestly make a mistake but it wasn't their intent. If you're dealing with people that have intent to defraud or intent to misuse or intent to steal information, that's a whole other problem. That gets you back to physical security.

There's a reported breach down in Florida at the Jackson Health System where a former hospital volunteer used his cell phone to take pictures of a thousand or more than a thousand patient records. And if you think of either taking a picture of the physical documents or even on computers, when you have screens up and they don't have a print capability, they don't have a store capability, and you think you've got that secure. Well, you're not secure against somebody pointing a camera at the screen and just snapping a picture of the information you thought was unreachable.

So when Jackson Health, they decided eventually to ban the use of cell phones by volunteer workers, so they took the BYOD and then decided they'd gone a step too far and came back a step. And that's alright to do too. Your decision for how you use the BYOD doesn't have to be a one-time decision. You can modify it based on experience.

Julia Allen: Yeah, I'm thinking more about that issue that you described. I mean, how in the heck would you monitor for someone taking a picture of something on their phone and then forwarding that picture a variety of places? I guess you could monitor on the sending side but

the actual act of taking a picture, I mean I'm not real conversant with this technology but I can't even imagine how you would know that even happened. Is there a way?

Joe Mayes: Not a way that normal mortals know.

Julia Allen: Right, right.

Joe Mayes: There may be people in some hidden room someplace that know how to do that but I have not run across them yet because you don't even have to send it out, right? You're going to walk in with your phone; you're going to walk out with it again. You can do the sending after you left the corporate environment. All you have to do is have the image and carry it out with you.

Part 3: Getting Started – First Steps

Julia Allen: It boggles the mind. Well so we've painted a pretty gloomy picture here so why don't, before I let you go, why don't we talk a little bit about what you see as effective or recommended first steps for putting a good policy in place, putting some good practices in place. What do you think is a good place to get started?

Joe Mayes: Well I'd like to start by taking some of the gloom off of this gloomy image. There really are wonderful valid uses for this and they really do increase productivity. You just have to do it in a smart manner and one of those ways to do it in a smart manner is to start with a risk assessment.

If you can walk through a risk assessment, understand which worst case scenarios you're willing to expose yourself to, then you're a lot more comfortable to say within that range of risk we have either mitigated it or are going to accept it. And as long as you can live in that world, then wherever you decide to go that should be a comfort zone. And within that comfort zone you should be able to get the benefits of the mobile devices and not have too many of the risks.

Julia Allen: Do you recommend or have you seen effective this idea of piloting or starting with one device type first or maybe starting with a particular part of the organization? In other words, is there a way to scope this initially as organizations are getting their feet on the ground that helps them get a better handle on what their exposures might be?

Joe Mayes: I've seen two different types of pilots. One type of pilot is where you take one department and often it's the IT department or it's the executives because it's people who are clamoring the most for it and have the most ability to actually get in front of the line. And watch them as a pilot and see how it works.

The other type of pilot is to take a sprinkling of people across all departments and then that's a more monitored pilot where you can, you are trying to see how it works for different divisions and different ways and different use cases because you're trying to set a corporate policy that may have to be tweaked or specialized per use or per organizational unit of the business.

Both ways work. If you do it with one department then you're going to have to do it over and over again if you go to new departments because different departments use it in different ways.

Julia Allen: Have you seen the idea of starting with a particular type of device helpful or is that really not -- you don't really learn that much? Like let's say you start by allowing iPhones or iPads or is that really not that effective?

Joe Mayes: That's the other half of it. You can start with one device type and then you can redo the scenario again by adding another device on to see if that brings in another risk factor that's outside of your comfort zone. And you can keep adding devices until you find one that's outside of your comfort zone and then back off again.

Julia Allen: Right, so I guess as you said earlier when you talked about what roles or what users to get involved in the pilot; it really just depends on where the pressure points are in the organization, right?

In other words who has got the biggest need, where is the greatest pressure demand coming from? Who would produce, what part of the organization would produce the greatest benefit, right?

Joe Mayes: Right, when you look at the use cases too -- I mean for some people the biggest thing they need is email access. For other people, email access may be important but then there are field instigators or they're, for a company they may be insurance adjusters and for them that mobile phone and the ability for them to send information back immediately is a whole other use case that the average office worker doesn't have. So different ways to use it, different issues.

Julia Allen: Got it. Well, I know we've only barely scratched the surface here but do you have some resources or other sources of information that you can point our listeners to, to learn more about this?

Joe Mayes: That world has gotten a lot better recently. For a long time there weren't some standardized documents you could point to. There were a lot of loosely associated documents. But NIST (US National Institute of Standards and Technology) has come up with some documents for hardware rooted security on mobile devices. They've got a document for managing and securing mobile devices in the enterprise. They've got a draft policy for telecommuting the mobile computer security.

And just new things are coming up at the highest standards level every day. Some people who want it. There's a whole separate set of standards called STIGs (Security Technical Implementation Guides) that you can for the most part download and get information on that come from the DoD (US Department of Defense) side, which tends to be a little stricter than even NIST standards.

Julia Allen: Right and I know I see new articles and new guidelines popping up all the time, but I like your recommendation on the NIST standards, so at least you can anchor your data search and your guidance in something that's pretty well established, right?

Joe Mayes: Right, it also makes it easier later if you have auditing or other requirements to point back to a federal standard and say we meet this federal standard.

Julia Allen: Great. Well, Joe, I can't thank you enough for your time today, your preparation, your expertise and giving us some good insights and ideas to follow to make this happen in our organizations. Or if it's already happening, make it happen more securely. So thank you again for your time today.

Joe Mayes: Oh you're very welcome. I had a great time.