MOVING TARGET

With 'bring your own device' fast becoming the mobile policy of choice at many hedge funds, *HFMTech*'s Sean Creamer and a panel of industry experts discuss harnessing a successful, safe and secure BYOD roll-out

It's a given that hedge fund data and IP are sensitive and it's a technologists job to protect those assets. But what to do when a hedge fund manager's new device of choice is less secure than the last most popular gadget? That's the CTO's quandary just seven years after Apple introduced the iPhone, so popular it's practically a de facto standard but one that's significantly less secure than a CTO would like.

With the expectation that Blackberry may be on its way out as the preferred professional device among financiers, it's more critical than ever that firms' bring your own device (BYOD) policies are thoughtful, robust and all-encompassing.

HFMTechnology spoke to three executives— Jeffrey Miller, CTO at Serengeti Asset Management, Jerry Levine, managing director at Risk Advisors, and Ojas Rege, vice president of strategy at MobileIron—to get their perspectives about securing their professional networks, new technology, and the challenges and opportunities on the horizon.

What is your top concern related to employees bringing their own mobile devices to work?

Jeffrey Miller (JM): My main concern is data leakage prevention. When it comes to end users and the applications they choose to put on their mobile devices, they may accidentally install malware and spyware by installing a free app that is infected. I read a report the other day about the amount of malware on phones and how it is directly proportional to the number of apps installed, which makes sense as viruses and spyware on mobile devices are commonly inserted into apps rather than picked up through web browsing on mobiles. The issue is that most people on mobile devices are using apps for various purposes, both business and personal. The fear I have is people using a device for work that may also contain downloaded gaming applications for themselves or their kids and those can contain malicious content. I have seen devices that have 50 or more downloaded apps, and chances are that one or two may contain something malicious.

> "The fear I have is people using a device for work that may also contain downloaded gaming applications for themselves or their kids and those can contain malicious content
> Jeffrey Miller, Serengeti

What solution have you chosen for your BYOD policy?

JM: At Serengeti, we decided to use a mobile device management system that could ensure we have control over specific aspects of a user's device. For instance, the day an employee leaves the company, we have the ability to delete company data without erasing the entire device. Regardless of this, there is no way to fully secure a phone from data leakage, but gaining control of the device by locking down and securing company data is a paramount goal.

We currently allow employees to bring their own devices to Serengeti. When an employee gets a new phone, we ask for access to install work-related apps and content, and we will then allow them to download whatever applications they please.

Employees are able to read research documents through a secured version of Box.com, which gives end users the ability to save documents when on working on a computer and have it available on an iPad or iPhone while out of the office.

We also have a concern about data leakage through email and employees attaching documents such as position reports. In order to protect against this we encrypt the work related emails and files in a secure container and do not allow them on the native unencrypted storage of the device.

Jerry Levine (JL): My first experience with non-Blackberry mobile devices was the Apple iPhone, when I was working for a large hedge fund as head of IT. The employees had heard about the iPhone and wanted to get it to replace their Blackberry [devices].

I was tasked with looking into ways to ensure message delivery. There were no solutions from Apple or Blackberry to guarantee message delivery with any mobile phone other than a Blackberry device. What gave Blackberry its advantage was that it has proprietary servers for message management and if a message was not sent to a recipient, it would be stored and eventually delivered.

So Blackberry would have emails pushed, whereas the iPhone pulled emails with no audit trail.

Employees wanted the latest technology from Apple, but were told they would not have the guaranteed message deliver. They were fine with experimenting and would carry two devices. Now we've come full circle where Blackberry is either gone or on its way out for the most part at hedge funds.

How would a BYOD policy have helped this situation?

JL: In its place, BYOD quells the issue of dealing with people wanting new devices and dealing with replacements. This policy places the responsibility on the user for mobile devices and plans. Overall, many tasks are made much easier when BYOD is correctly employed. It takes the technologist out of managing network plans and it is a better experience for end users.

Also, technology provided by companies such as MobileIron has introduced a stable mobile device management platform ensuring iPhone as well as Android message delivery and enterprise control. I authored a mobile device policy, which was required, to manage the ownership of phones and carrier plans. This provided guidelines for upgraded devices as well as lost or damaged devices.

Ojas Rege (OR): The concerns and questions have changed quite a bit. Turning the clock back to 2011, the first question for financial services and hedge funds was, "How do I support secure email on an iPhone?" The second question appeared when the iPad came out and technologists said, "This is cool, should I build apps for it?" But first they needed to secure the native email app.

In 2012, the questions broadened and a new one was added: CTOs liked the idea of BYOD, meaning that the organisation didn't have to pay for the device, but that gave birth to the ultimate question of how do I secure a BYOD policy? It opened up new risks in data loss due to the fact that the device belonged to the end user and was not locked down by Blackberry's servers. So once we developed a way to secure the native iPhone email client, BYOD began to take off in 2012.

Fast-forward to 2013 and it was a watershed year in a lot of ways. The first instance was the Blackberry migration. Financial issues at Blackberry drove companies to develop migration programs. The second event was that Android became a real player in terms of operating systems. Of course iOS was still dominant in the enterprise, but financial service firms needed to at least look at the Android operating system as a credible platform since it was widely accepted by the public.

Finally, in the latter half of 2013, iOS 7 came out and it was a massive evolution in Apple's app security capabilities. The ability to deploy iOS securely became even stronger when you deployed through MobileIron. Since 2010, the financial services industry has been our largest clientele for mobile security.

Do the concerns of your hedge fund clients differ from the financial industry broadly?

OR: Essentially, the concerns of the hedge funds mirror those of the financial services industry as a whole, but due to the smaller size of hedge funds, there is not so much of a need for global capabilities. Many hedge funds currently are focused on the Blackberry-to-iOS migration and tend not to be looking at a lot of apps, which I believe will change in the coming years. For the most part hedge funds are really looking at getting a secure native email experience on iPhones.

From the security perspective, the concerns are the same as other financial services organisations. Emails have to be encrypted, attachments cannot end up in Dropbox and CTOs want to ensure that if an individual leaves the firm, the hedge fund data on the device can be deleted.

Many times, these are personally owned devices so IT has to be able to delete enterprise data without deleting personal data on the device. With MobileIron, hedge fund managers don't have to worry about this because personal and professional data is separated.

Jeffrey Miller

Jeffrey Miller is the chief technology officer for Serengeti Asset Management, a multi-strategy opportunistic asset management fund. Serengeti is based in NYC. He is responsible for all of the technology at the company, and has been working in finance for over eight years.

What are the roadblocks to securing personal mobile devices for work?

JL: When it came to the iPhone there was no guaranteed message delivery for the early models of the device. The roadblock was that there was no software to push guaranteed delivery of messages and it was important to set that expectation with users. If they wanted to carry two devices they had to understand that the emailing client was not robust.

Jerry Levine

Jerry Levine is a managing director at Risk Advisors where he heads up the trading systems and technology practice. Previously Levine held roles at prominent hedge funds, including a position as the director of global trading technology at Millennium Partners and the head of information technology at AQR Capital Management.

OR: The number one issue for us in the early days was securing Apple's native email app. The other option was to force the employee to use a separate email app. But the reason people love the iPhone is the native experience, so the tech challenge for us back when we built out email protection was to make sure the native solution was secure and you didn't need to force the user into a non-native experience.

For example, if there was an attachment, that attachment shouldn't be forwarded to a personal Gmail account. This was the largest issue for hedge funds: email security. We solved it, and that is still the number one requirement for many clients. Apple itself did a lot of work in the field of security and encryption.

Every iPhone is encrypted; you cannot buy one that isn't. Apple not only did a single level of encryption, they added secondary level of encryption if an end user opted to have a passcode. MobileIron enforces a password on the device so you get both Apple encryptions and an additional MobileIron layer for the app itself. We have FIPS 140-2 validation for our encryption on iPhones as well.

Ojas Rege

Ojas Rege is responsible for aligning product development and corporate strategy at MobileIron as the vice president of strategy. Prior to joining MobileIron, Rege was vice president of global mobile products at Yahoo! where he was responsible for mobile search, email, messaging, and content services. The team delivered SMS, mobile web, and client applications for phones, and built extensive platforms to deal with the daunting global fragmentation of mobile technology. He has been working in mobile technology since 2000.

What about employees utilising Android devices?

OR: The approach to Android is different technically, but with a similar outcome. Android today is less relevant to the hedge fund market, but will be much more relevant in 2014 because, overall, Android has become more mature and gained substantial traction in the consumer world. On Android, the encryption is very fragmented, but it has become much better since Samsung began providing additional encryption on its devices. MobileIron can monitor devices for encryption and operating system integrity.

Additionally, our FIPS 140-2 validated encryption is ready for Android too, and financial services as a whole absolutely need the data on the device to be encrypted. We began our FIPS 140-2 validation process a year ago and received it in November of 2013. It is the standard that the federal government uses and so it is a standard that the financial services industry looks toward as well.

When employing a BYOD procedure, are permissions (ie, related to social media access and/or participation, access to data and IP, and online services) strict or more relaxed?

JM: In terms of dealing with social media upon phones being used for work, we don't restrict access at all. We treat our employees' phones as their own personal devices and it is not a concern as long as the business part is secured and encrypted within the MobileIron container.

What do employees generally use their phones for at work?

JM: Employees generally will use their email, which is a primary function for many end users when it comes to working from their phone. We will lock down documents through box.com so that if they have data imported to their phone we have the ability to delete it if they leave the firm, and we are also safe from the data leaving that container.

If they are doing work beyond that, end users will connect back to their desktop in the office, and they can do it from and iPad through the VMware view app. To do this, we use VMware Horizon View for virtual desktops. One hundred percent of our employees have a desktop and can connect to their desktop from their mobile device. While employees can access the desktop, it is not the best experience due to the smaller screen and lack of a physical keyboard and mouse. So VMware Horizon View is mostly used to do work from a home computer or laptop.

JL: The last hedge fund that I worked for locked down phones to the point where there was no way to install apps, take photos or send multimedia messages. Corporate believed that there was no need for these functions from a business aspect and that you only needed to accept calls and emails. It was just like having the old green screen Blackberry.

I know some senior people at firms who don't want personal texts or anything recorded and willingly carry two phones to protect themselves. This is because when you are issued a corporate phone or accessing company emails, the phone is subject to being recorded for auditing purposes. So any messages sent on a company phone are recorded and can be discovered.

OR: The user is always in control. Back when hedge funds would issue laptops, IT would stop users from downloading anything onto the medium. Now end users control what's on their device because MobileIron has a function where if a CIO is worried about users downloading social media, the company can see if a particular app is on the phone.

If "Joe" downloaded whatever social media app, Joe is sent a message that he has downloaded an app that isn't allowed and he has to delete it. If there is a substantial breach, you can block access to email until it is deleted. You can take several actions: notify, block, or in dire circumstance, wipe the device. One of the concerns is that sales and trading will use messaging apps that don't leave audit trails.

CTOs and other executives are recognising that there are so many apps out there, there is no way to restrict them all. The practical approach is that a CTO will put in place rules in MobileIron to limit certain apps and then put in place corresponding HR controls to educate employees to not communicate in unaudited ways with the consequence of dismissal.

> "A virus in Windows that is downloaded by mistake could destroy file systems. In iOS, apps don't have access to the full files system. This means that there is no need for antivirus security
>
> Ojas Rege, MobileIron

What about stopping the sharing of company data?

OR: Ultimately, you cannot stop a malicious insider from doing bad things, so you have to have stiff penalties. The consequences have to be substantial, but the mobile experience should not restrict the guy just doing his job from using the tools he needs to. Application black lists don't work in the long term because new apps are developed every minute. There is no way to know all the apps out there that might cause a problem. CTOs have to monitor for the important ones and educate their employees.

All CTOs worry about rogue apps. They worry employees may use rogue apps to transmit data they shouldn't transmit. One way to solve that is by having the aforementioned app control rules, education, and consequences. CTOs also worry about rogue apps putting malware on the device.

How is this issue handled by Apple?

OR: From a tech standpoint, Apple solves this issue through the underlying architecture of iOS, which is fundamentally different from traditional Windows. A virus in Windows that is downloaded by mistake could destroy file systems. In iOS, apps don't have access to the full files system. This is an architecture called sandboxing and it means that there is no need for antivirus security.

MobileIron adds additional controls to lessen the chances of a rogue app damaging company data through the addition of jailbreak detection. If you jailbreak iOS, then your data is up for grabs. So long as a phone is not jailbroken, the apps remain sandboxed and safe. We monitor for jailbreak and the moment it is jailbroken, all enterprise data will be deleted so it is not at risk. We do the same thing for Android, where this is called rooting.

There are three reasons why there are so few exploits on iOS: one, the Apple app store is curated and bad apps are blocked. Second, the architecture is sandbox style. The third is that Apple controls firmware upgrades and patches.

If a bad guy wants to build a nasty Trojan to deploy to iPhones and steal money or whatever, Apple can put a patch out and 40% of global iOS devices will be on the new version within two days. Since Apple has that level of control they can close holes really fast. The ROI for a bad guy is poor because Apple will shut down any malware quickly. The iOS operating system is secure and the app store is secure too. Because of this, bad guys cannot write bad software and will target the fragmented Android OS.

What are Samsung and MobileIron doing to lock down security?

OR: Android devices have a lot more malware than iOS. However, Samsung is doing a lot to add security to their Android products. As a result, the first devices a CTO would look at for Android are usually Samsung for the higher security and MobileIron adds additional security on top of that.

The other thing we do for Android is containerising every application on the phone so even if malware is on the device, enterprise data is not at risk. Beyond that, if our customer wants employees to have up-to-date antivirus software on a device, MobileIron will make sure that antivirus app is in fact on the device. If it is not, we can block enterprise access from that device to the enterprise and delete local enterprise data.

Samsung is lending a hand by launching KNOX to provide additional security.

What applications can funds use to ensure device security?

OR: We don't write apps ourselves, but we do secure apps. We have an app ecosystem of the best-of-breed business apps that can all be secured by MobileIron.

Beyond email, a second app that is important for financial services is content management. There are always a lot of documents to read and employees want to do it on their phones or tablets. We have a plethora of partners that offer various content managers for phones to do things like that.

Hedge fund guys increasingly are needing access to documents on the go. Another important category is analytics apps to access and analyse data on the fly.

After you've developed a BYOD policy, what implementation process do you go through?

JM: So what will happen when an employee brings a new device in for work is that the phone or tablet will be handed to me, I install MobileIron and make the under-the-hood changes, but on the surface, end users won't notice changes and will be able to use it the same way they used the device before handing it off to me.

Employees then have to install an EMC2 (squared) RSA two-factor identification app, which will then allow them to log into their phone for work-related tasks. Employees are then able to do research via a management system that comes from Box.com, which gives end users the ability to save documents when on working on a computer and have it available on an iPad or iPhone PDF reader on the road.

How does your firm keep track of intellectual property and stop people from taking items from work when their mobiles are not just for work?

JM: We feel comfortable that documents cannot get out of our network via remote access. Various protection layers prevent end users from uploading sensitive documents, thus making it difficult to get the data out without it being known by me or just being blocked.

JL: There are some hedge funds that are liberal and open about phone security, so long as work-related items are containerised. On the other hand, some firms are still locking down phones to protect sensitive information at all costs. There really isn't a wrong or right way to approach this, because it all depends on your firm's security policy.

Are there specific security threats related to social media?

OR : It used to be that employees just couldn't have social media access. Now they know they cannot stop users from using these apps on the phone and so they now need to make it clear how people should and shouldn't use them. One concern I've heard is employees wasting time, but the chief reason CTOs are wary of social media access has to do with regulatory issues. They worry about trading information being communicated through non-audited channels. This is more of an issue for people on the trading floor than the average hedge fund, but auditability is the core. ■

Just getting started with BYOD? Keep these issues in mind...

1. Ensure that downloaded data can't be shared or stolen off devices.
2. Require personal staff devices to be outfitted with encryption, ideally a container-like environment, and authentication software.
3. Containers also record and track messages, so they will aid in meeting requirements for creating audit trails by capturing investor-related correspondence.
4. Ensure data can be wiped or destroyed, ideally just firm proprietary data, in the event of theft or loss.
5. Don't stop at e-mail encryption when considering third-party providers—consider all use cases for the devices, such as users working at home or business travel, and ensure that use in atypical situations will still allow staff to comply with BYOD policy.
6. Meshing technology and policy is key—focusing on one at the expense of the other will increase the chances of a security breach.
7. Complete thorough due diligence on available vendors to determine which is the right fit for your firm. Some elements to keep in mind: Does the vendor provide a containerized environment for downloads so documents are not stored on devices? Will security for the devices be run internally or externally?
8. Stay up-to-date on the current viruses and malware-- iPhones and Androids can become infected with malicious content by downloading apps that include free games or that ask to gain permission to an end users' contact list.