

BYOD:

Manage the Risks and Opportunities

FEATURING

Malcolm Harkins, CISO, Intel

Dan Ford, Chief Security Officer, Fixmo

Benjamin Wyrick, Director – Sales, VASCO Data Security

Ahmed Datoo, Chief Product Officer, Zenprise

Transcript of the Webinar Panel Discussion

BYOD: Manage the Risks and Opportunities

Transcript of the Webinar Panel Discussion on Mobility

Sponsored by



From smart phones to tablets, laptops to USB devices, consumer technologies are ubiquitous in the workplace - and so is the 'bring-your-own-device' (BYOD) practice of allowing employees to conduct work on their own personal electronics. But how do these consumer technologies change organizations' approaches to securing corporate information assets?



MALCOLM HARKINS
CISO
Intel



DAN FORD
Chief Security Officer
Fixmo



BENJAMIN WYRICK
Director - Sales
VASCO Data Security



AHMED DATOO
Chief Product Officer
Zenprise

VIEW THIS WEBINAR NOW » <http://www.bankinfosecurity.com/webinars/byod-manage-risks-opportunities-w-266>

Read on to learn from this expert panel:

- How to properly inventory your employees' personal devices;
- Technology solutions to protect your corporate systems and data, as well as the end-point devices;
- Strategies and tactics for enforcing mobile policies and maintaining compliance in regulated industries;
- How to use BYOD as an opportunity to enable further proliferation of data and access security.

Malcolm Harkins, CISO, Intel

Harkins is vice president of Intel's Information Technology Group and CISO and general manager of information risk and security. The group is responsible for managing the risk, controls, privacy, security and other related compliance activities for all of Intel's information assets.

Before becoming Intel's first CISO, Harkins held roles in Finance, Procurement and Operations. He has managed efforts encompassing IT benchmarking and Sarbanes Oxley systems compliance. He joined Intel in 1992.

Dan Ford, Chief Security Officer, Fixmo

Ford has been an information security professional for more than 15 years, and has worked for notable organizations such as XM Radio, Secure Computing, McAfee, Nominum, and Accuvant. He has extensive experience running security programs within the government segment; his most notable role was as Director of Network Security at the Transportation and Security Administration, which was the largest managed service contract within the federal government. In his role at Fixmo, he is directly responsible for global security and information assurance initiatives - researching trends, discovering security vulnerabilities and exploits, building strategic partnerships, and attaining industry certifications - as well as product innovation.

Benjamin Wyrick, Director - Sales, VASCO Data Security

Wyrick is responsible for managing VASCO Data Security's business operations in North America. He joined the company in 2005 and has been a key contributor to the VASCO team which has become the market leader in global authentication. Wyrick and his team have successfully managed partner and customer relationships with some of the world's best known organizations. He has been involved in a number of two-factor authentication security projects with major banks and financial organizations.

Ahmed Dattoo, Chief Product Officer, Zenprise

Dattoo's experience in the technology industry spans strategic planning, brand marketing, software engineering and product management. Prior to Zenprise, Dattoo was with EDS, where he was a global Director of Product Development. While with EDS, he built and launched several workflow automation and monitoring automation modules that generated multi-million dollar savings globally.

"You can't secure that which you don't know exists."

AHMED DATOO, ZENPRISE

Transcript

MALCOLM HARKINS: Beyond the technology, what are the top BYOD challenges for organizations?

BENJAMIN WYRICK: From our perspective, it's really about securing the user and BYOD is an opportunity, really the first time employees are being enabled to bring technology to improve their work vs. being assigned something and restricted, much like the working from home movement has significantly changed for company's employees. BYOD will present opportunities for employees to balance how and when they work. I think with this freedom will come some opportunities to enable the user further with tools to secure themselves and secure their data, much like more universal strong authentication will allow.

HARKINS: I think that's a fantastic point and as you were saying about where to work and when to work, one of the challenges beyond the technology is the workplace things, the HR aspects of it, the differences between hourly employees and salaried employees, and how different organizations need to think of those employment items with the BYOD as they go to introduce them into their organization so that they can set the appropriate guidance, so to speak, for both managers and employees.

AHMED DATOO: One of the biggest challenges with BYOD is just visibility. Often times, organizations have no idea what types of devices they're connecting in. In fact, we've gone to some organizations that didn't realize that they've got iPod Touches that people are using to access e-mail. It's the same operating

“In this policy, you need to set what the minimum standard’s going to be for data access in this BYOD environment.”

DAN FORD, FIXMO

system as the IOS. And you can’t secure that which you don’t know exists, so I think the first challenge in BYOD is just getting an understanding of what’s actually connecting.

Then the second thing is it’s not technology-related, it’s process related. It’s figuring out what are the bare sets of security requirements and policies that you’re going to require across all the different devices, and what’s your stance going to be around access. What are you going to allow users to do and not do? There’s going to be trade-off because you can’t be thinking about these like you think about laptops. People spent their money on these devices so you can’t enforce the same kinds of controls that you did on the PC, so what you need to figure out is what’s the bare minimum from a security standpoint that you’re willing to live with and how do you enable the user to be productive. But the first step in the whole process is figuring out what’s connecting.

DAN FORD: I think I’ll echo with a lot of what Ahmed is saying here. It really comes down to - from a secure perspective - as being policy, policy, policy, and I’ll throw in a little enterprise architecture there for the mobile environment, kind of relaying this back to the framework so that way we can start trying to get ahead of the curve, because BYOD we’ve been hearing a lot for the last 12-18 months. In this policy, you need to set what the minimum standard’s going to be for data access in this BYOD environment. Ahmed mentioned iPod Touches because it’s the same for IOS. Are you going to allow iPads to all areas? What about Android? What particular version

of Android is acceptable for you because we know that Froyo is losing a little bit of market share - which is the Android version 2.2 - and Gingerbread is really picking up the pace, and now we’ve got version 4 with Ice Cream Sandwich. They all have little differences, especially when it comes to the vulnerabilities that each one has in them and as an enterprise you may not want to allow all of them.

But in the policy, what’s important for all of these enterprises is to layout what’s the minimally acceptable standards, publish it in readable format so everyone can understand it, as well as update this. It’s got to be a living, breathing thing because new devices are coming out all the time. Right now it’s Android and IOS. What’s going to be the next batch in mobile devices? This would be something that you would have to continuously look at for your enterprise. I think that enterprise architecture framework, if organizations start taking that to heart, your security challenges will start to be minimized going forward.

HARKINS: Building off of that, we have another question that came in directed at me from what we see at Intel as some of the key elements of effective mobile policies around BYOD, and I think you’re spot-on in the view that it’s living. You’re never done because the technologies are changing, the usages continue to change and the legal and regulatory landscape changes. The way in which we looked at the effective policy stuff, it kind of really separates to some extent into the technical side of it and that minimum standard you want to have, and depending

on what you’re trying to give access to, if somebody just wants calendar and contact information, your policy footprint and what you’re going to require because that stuff is less sensitive is different than if they want to get access to be able to do a transaction like approving a purchase order or accessing payroll.

The policies and technical standards you’re going to have are going to be completely different, and then there are the policies on the challenges beyond the technology ones, which depend upon the location and the role of the individual. Are they hourly or are they salaried? What are the policies around privacy? How’s the company obligated to protect the privacy of the individual and try and separate what’s their personal information on the device vs. the corporate information? How would we deal with investigations or court-required discovery requests where we have to go retain information that may be on those devices and how do we communicate that clearly in a way that the users can understand essentially some of the rights they have to potentially give up in order to have a bring-your-own-device in enterprise use? Because the enterprise now has obligations if that’s being used for corporate purposes to be able to get access physically to the device and logically in some circumstances.

Benjamin, how does BYOD change the traditional way organizations provide security?

WYRICK: I think BYOD creates an opportunity for simplifying the enterprise authentication architecture. With more uses, more devices and more types and complex passwords, and more and more networks and applications in the cloud, it’s becoming very challenging to properly protect the data. What I see is an opportunity to focus on securing the user by leveraging the mobile device for security, what’s called bring-your-own-token, much like VASCO has done with Intel by embedding credentials natively into their IPT chipsets. If we can bring and



leverage this opportunity to eliminate static passwords and expand dynamic credentials across the enterprise and the entire Internet, everyone will benefit. It will provide an efficient way to collaborate and exchange ideas and information but provide the security we all want and need.

HARKINS: I totally agree. Ahmed, any comments from you on that?

DATOO: One of the biggest things is a change in mindset. Often times we see, for example, companies approach BYOD very

similarly to how they approached corporate-owned laptops and one of the common mistakes I see for example is pass codes. People want individuals to have pass codes on the devices and they want them to be the same as the laptop: eight characters, a capital letter and a special character. And all it takes is one executive to be in the car, because let's face it, people end up checking e-mail or SMS in the car and have to enter in that pass code once before that pass code gets changed. The idea comes back to identifying up-front, from a policy standpoint and from a security standpoint, what's the minimum requirement

from an organizational standpoint from security, then identifying those sets of policies and applying to those sets of devices that you plan on supporting or allowing users to bring in.

HARKINS: Dan, how can an organization leverage BYOD successes across other key compliance areas?

FORD: The organizations are just now starting to think about BYOD. They're really already behind the curve. You've got to get ahead of this, and that means you have to start thinking about not just BYOD today from a policy perspective, but what are the next trends that are out there? Get out there and communicate with your peers and different roundtable sessions. ISSA has a mobile group. If you're involved in U.S. federal government, it has mobile groups. Find out what mistakes they have made so you don't make them again. What have they found that has been very successful and then start small. Don't start big when you're trying to leverage what other organizations have done because every organization has their own unique challenges with how they handle data and how the data owners are responsible for them. Again, I really go back to an enterprise architecture process because that's going to help start identifying where the data reference model is so you can understand how that data's moving around to the different technologies. You'll know what enterprise applications you're using and then how to move those enterprise applications to that mobile environment.

HARKINS: I think that makes a ton of sense. One of the things that we've seen with BYO successes is the power of the small wins in this space. I think you can leverage those successes as well from a security team to move the security team to be more than just being perceived as the "no" organization, and essentially kind of run to the riskier items in order to shape the path of the risk and manage the risk in order to capture the benefit. Then again, look at that from other compliance areas and say, "These things that

“You’re never done [with your policy] because the technologies are changing, the usages continue to change and the legal and regulatory landscape change.”

MALCOLM HARKINS, INTEL

have been ‘off limits’ in the past, can we look at risk differently and in a way that allows us to be more progressive toward some items but still manage the risk because we’ve seen the ability to do that with the BYO model?”

FORD: When you know where the data is, you know what types of security measures you have to put in place. When it comes to risk, it’s about getting the risk to an acceptable level for the data owners to feel comfortable as to how their data’s being used and shared amongst the organization or even between different organizations.

DATOO: I would love to share an example of a BYOD success as it relates to compliance. We have a customer that’s in the aerospace industry and they have engineers that manually print out the blueprints of an airplane when they go to inspect the airplane. They’re regulated by FAA requirements to at the end of the inspection physically destroy the blueprints because should these blueprints get in the wrong hands, it could be a huge national security concern. They’re required to destroy these documents. It turns out that this organization was fined \$17 million last year because of not actually carrying this out. You get an engineer who gets pulled from inspecting one plane to another and forgets to destroy these documents, and these documents are thick. So they started looking at mobile as a way of, “How do we use mobile to change the delivery model?”

One of the ideas is they actually handed each of the engineers an iPad and then those enterprises got a capability to securely deliver

files to these devices. What they did is they delivered these blueprints electronically to the users. The users are ecstatic because it’s just a pain to go and shred these documents, and then they were able to put policy controls on the documents delivered to automatically remove the documents after a certain time period. There’s an example of a BYOD success that’s able to address a specific compliance-related requirement that not only ends up saving the organization money, but actually makes the end users happier because you’re making their job easier.

HARKINS: That’s a great thing to build off of. A question came in for me around how one calculates return on investment of a BYOD initiative. I think the example you just gave is a perfect way to look at that use case. Again, there’s paper savings, there’s time savings. It’s more eco-friendly because you’re not having the paper. You’re not having the destruction of the paper cost. I’m an old finance guy and so for me, traditionally calculating that return on investment, cash is king. Follow the cash when you’re calculating your ROI first.

It’s certainly not free to do this so there’s incremental cost for providing and essentially registering and authorizing those devices on your network, getting legitimized and connected in. But if you’ve already started looking at it and go, “I’m not having to pay for the device, the user is. I’m not having to pay for the service, the user is,” you can follow the money and do that basic cash analysis.

Ahmed, with the example you gave, there’s

some savings with printers, paper and that type of stuff. The other thing that we’ve done in terms of calculation of our return on investment at Intel is we’ve looked at trying to measure qualitatively the extra effort or work that we might get from employees and we’ve done that by looking at mail sent or other things like that, and surveying the users. What we’ve found with the BYOD users is we’re seeing about an extra 57 minutes from our users of extra work per week that individuals were doing because they could work real-time to check a message, check a calendar, do something that made them more productive. The productivity benefit we’ve seen is just about 60 minutes a week.

Dan, what are the most compelling challenges for regulated industries and governments with regard to BYOD?

FORD: I think it’s really a combination of technical, regulatory and policy. I’ll go technical first. It goes back down to data management and really the risks to the compromise of confidentiality, integrity and availability to that data. It’s about trust. We have to be able to trust when we’re bringing up any of these mobile devices that as security professionals we know that nothing on that device has been compromised. We’ve seen just recently at RSA last week these devices no longer need to be rooted or jailbroken to have an attack and/or compromise to confidentiality and integrity. Zero days don’t have to exist, this notion of the half-day exploit where a vulnerability exists out in the wild, a patch is available but it’s never been distributed either due to the relationship between the manufacturer



and the carrier or the user just hasn't been prompted to have to download it, or they ignore it.

What we see in the trend is that a bad actor will purchase a list of vulnerabilities for an operating system. For this example, we'll just take Android 2.2 because there have been updates. We know 2.3 - all the way I think to 2.3.9 - but there are particular system files that can be easily modified by a browser exploit on there and then you can turn that device back into essentially a zombie in a way

where you're going to use the microphone and the camera. You'll be able to see and hear all the conversations going back and forth, the text messages and the e-mails, all because the user didn't update or the manufacturer didn't push out the update yet.

Then, not just from the technical side, we also got the regulatory compliance. Things are changing very fast. Today, the main thing that people always go back to when they're trying to prosecute individuals for things like I just described goes back to the Computer Fraud

and Abuse Act. The legal aspect needs to get modified out there in order to improve upon what the new minimally acceptable standard for devices is, especially when it comes to government data. As part of the regulations, how are we going to continuously monitor the risk profiles that organizations have said is acceptable to them, because tomorrow it changes? I think that goes again right back to the policy. You're supposed to be having a policy, following a policy, updating a policy and then also that rolls back down to the technical challenges when new laws have been established, policies get updated and the technical implementation needs to occur.

HARKINS: Ahmed, anything from your perspective around those challenges for regulated industries and governments?

DATOO: From a regulated industry and government standpoint, there's a whole host of issues. I think it comes down to data security. Often times folks in government, healthcare and financial services have a whole host of highly sensitive information that could come in the form of e-mails as attachments. We start talking to folks that are using iPads in lieu of laptops and the number one end-user requirement we hear about is, "How do I get documents to the device?" They will subscribe to fraud-based services like a dropbox or a box.net and now all of a sudden you have sensitive information that's out on the cloud, and when an employee leaves you can wipe the device clean, but you've got information that exists outside. So I think there are some challenges. Interestingly enough, it's not just about data; it's also around applications.

An example I like to give is in the financial services space. In financial services, from a regulatory standpoint, they're required to have an audit log of all SMS messages as well as all e-mail, because you don't want some people sending insider information and providing insider trading information. There are these sets of questions that are starting to emerge around BYOD where if a person ends up using Facebook on

“What I see is an opportunity to focus on securing the user by leveraging the mobile device for security, what’s called bring-your-own-token.”

BENJAMIN WYRICK, VASCO

their application, Facebook has an e-mail component and its got a message component so what are the regulatory concerns and compliance requirements for folks in the financial services industry around Facebook? It’s a personally owned device. They should be allowed to use whatever application they want, but there are these regulatory concerns. There’s some complexity that’s starting to emerge as it relates to BYOD and regulated industries. Typically what we’ve seen is some organizations embrace BYOD. But also, organizations that are starting to move to corporate-owned devices where they’re just buying devices on behalf of the employee, they can start dictating sets of controls on the device.

FORD: Ahmed brings up a good point, utilizing third-party applications like dropbox. I don’t think a lot of people know the ramifications of that from a legal perspective. When you hand over data to a third party, that data is no longer subject to the Fourth Amendment here in the United States. That data can go and be accessed as part of an investigation without the need of a warrant, when you willingly hand that data over to a third party. That’s one of the other challenges that I’m seeing going across different legal circles out there in D.C. I think it’s important for people to understand that aspect as well, and kind of going back to it’s all about trusting. Ahmed brought up applications. Are they trusted applications? How do we keep in a BYOD environment separate from what’s business vs. personal? I think that’s a great way that Fixmo is able to come in and help that out as well.

HARKINS: I think you’re right, and even what Ahmed had said with regard to the financial industry, I had a dialog with a peer about two weeks ago, and with their BYO initiative they have had to disable SMS texting on their phones because the way in which the implementation worked with that device, they couldn’t retain it. In that industry, with the audit logging and some of the retaining of communications, they had to disable that on the phone, which again presents a lot of unique challenges.

Benjamin, given those complexities, how do we get employees to accept their new security responsibilities, because obviously they’re going to have to play a part in this too?

WYRICK: As we talk to our clients and we listen to the market, we need to find a way to get employees to accept their new security responsibilities by enabling them and providing them the ability to protect themselves across all their online identities. This is an area that has really been open for a long time, an area for improvement. It’s been divided far too long and BYOD is an opportunity to unify personal and private lives at least as far as the Internet and application usage is concerned. Extending this unity toward security and to authentication and allowing them to control and secure any and all of their online accounts with strong authentication is good for them and I think it’s good for the entire Internet ecosystem.

HARKINS: I think that makes sense. One of the things that we’ve talked about internally

when we started our journey was we’ve all heard the consumerization of the enterprise but as we start looking at the policies, as we start looking at the expectation of employees, as we start looking at the technology we’re going to be using to secure them, we’re in essence enterprising the consumer. As we do that, we actually can up the level of their broader security, both at work and at home and at play, and change the behaviors and get them to think about things differently. One of the things that we’ve seen out of that and I’ve had discussions with some peers on this is when somebody owns the device, lost and stolen rates tend to be less. I think that accountability for the device and the usage of it - if you adopted it right and set the right expectations and essentially trust the employees to act appropriately - we’ve seen the employees accept that kind of new security responsibility.

FORD: One of the things that’s interesting about this question is they say there are new security responsibilities. I don’t really think they’re new. I think that they are the exact same responsibilities they’ve always needed to have when it comes to handling their enterprise data. What’s funny about this is that just last year the Wall Street Journal had an article stating that smart phone users were three times more likely to be susceptible to phishing attacks than they would have been if it came from their traditional computing environment. We’ve been trained for the last 10-15 years about spam, [not opening] up e-mails if you don’t know who it was from, and we’ve gotten a lot better, a lot more mature, in that enterprise security to where

e-mail or any types of web surfing that they're doing from the enterprise perspective, people have gotten a comfort zone.

I don't think it's necessarily new security. I think they need to be re-educated that these devices are the same but they are less mature. Therefore you have to be extra vigilant when you're going to be utilizing these devices for work and personal. There's that fine line that I think just needs to be a re-education to these users.

things: the maturity of the product type and it's predictability on how the risk posture's going to be after applying counter-measures. That's kind of difficult with where we are in the mobile-computing world today. I kind of equate the maturity level back to the PC market in the late 90s, early 2000s. We had antivirus. We had this little firewall called BlackICE. One of my favorite organizations out there called Cult of the Dead Cow - you may not be familiar with them - they made this little program called Back Orifice and

productive, right? The example I gave about dropbox and box.net, I don't think it's a user thinking, "I want to have access to all these corporate documents so if I were to leave, I can take it to the competitors." I think the user just wants to be more productive. I think when users start downloading some of these apps that may be malicious in nature, they download it out of ignorance. They don't know that it's necessarily malicious and they don't know the ramifications or implications, and so I think one of the key things when you start developing a BYOD strategy is the notion of trust but verify. Trust your end users to do the right things, but have some mechanisms in place to make sure that if there's a vulnerability that's identified on the Android marketplace - as there has been - you have a mechanism to identify which of the 50,000 devices out there actually have this application running. One of the biggest challenges that's emerging - at least from a threat perspective - is the ignorant user.

"One of the biggest things is a change in mindset."

AHMED DATOO, ZENPRISE

HARKINS: I think that's a perfect lead-in to the next question we just got, which is, how is the mobile threat landscape evolving?

WYRICK: I can address that from the authentication and security side. Of course we spend a lot of time focusing on the new threats and how those are evolving and what we see from mobile is that it really follows the PC in terms of threats, but at a quicker pace. The PC gave everyone - security companies and the hackers - a bit of an experience to learn from. We're seeing reports on man-in-the-mobile here recently, or really malware being placed on these phones to intercept messages; things like SMS, for example, used to deliver one-time passwords or passwords in general. I think it's important that as companies look at bring-your-own-device and using this for other things like security, we look to secure and harden these applications like most banks and other financial institutions are already doing.

FORD: A lot of my colleagues have heard me say this many times before. From my perspective security is really about two

this allowed these bad actors to install remote access tools on devices where they could get a shell and be able to really do whatever they wanted with these machines, and these things were on Windows 95, 98, 2000, even NT and XP. That's something that we're seeing now, as Benjamin just mentioned, about them getting text messages and they go and click on that link and all of a sudden they're having a Back Orifice-type tool on there.

I also believe that people should be very leery of the different alternative browsers you're finding in the marketplace and app store, because I think browser-session hijacking is going to be the next thing that starts occurring. I've already seen a couple of them. Charlie Miller at Accuvant did something very similar at Black Hat a couple of years ago.

DATOO: I might take a slightly contrarian view on this question. When I look at the mobile threat landscape, I think the biggest threat is actually the user. I don't think it's a malicious user. I just think it's an ignorant user. At the end of the day, users want to be

HARKINS: I think you're completely right, and in our view of the world with Intel, there are essentially two perimeters that we've moved with the extreme mobilization, consumerization, bolster computing, and it's the user perimeter and the data perimeter, and on the user side and even to some extent the data perspective - coupling some of that stuff together - I don't think at times users fully comprehend when they "check in" to places what that means, what privacy they're giving away, how they might be putting themselves even in physical harm because by letting everybody know where they are at, they've let everybody know where they're not, which could be their home or their apartment or something of that nature and if they're being targeted for let's say a crime or a break-in, by proclaiming to the world where you're at and how often you're there, you're creating a pattern for even a traditional crook who has any savviness to go look and figure out when you're not home and then break into your apartment or home or whatever.

Ahmed, beyond the basic mobile device management, what are the core elements that

**“Organizations are just now starting
to think about BYOD. They’re really
already behind the curve.”**

DAN FORD, FIXMO



need to be managed and how?

DATOO: I think most people think about just securing the device. If a device gets lost or stolen, they can remove the data on the device, but I think as we've heard from the discussions, mobile is an increasingly interconnected, complex ecosystem. By that I mean it's not just about the device; it's about applications that are running on the device. It's about the network connection and it's about data. We can go through each one of these and I think any good security strategy - forget about mobile - is one that has end-to-end protection. You can't just look at the endpoint. You need to look at all the points in-between, including apps, data and network.

When you think about a BYOD policy, you're definitely going to want to have an idea or sense of what sort of policies and security you're going to enable on the device, but you're going to want to also think about what are you going to do on the network side? Is there a way that you can start restricting access? We talked earlier about the notion of deciding the types of devices that I want to connect in or allow into my network. So we won't allow Android 2.2 devices; we'll allow Android 3.0 devices. We will allow Samsung tablets. We will not allow Amazon Kindle tablets. One of the ways of being able to enforce that is at the network layer. Think about, how do you empower and enable the user to be productive on the go? Meaning, most enterprises already have content repositories, be it a share point, file servers or whatever it may be, and people have access to that on the desktop. Organizations have invested in data leakage prevention tools and the whole host of content filtering systems and so the question is, how do you extend that onto the mobile device? How do you

allow people to have access to that same content repository on the mobile device so you eliminate the threat of the user going outside the IT service to use these third-party, cloud-based, data-sync services. In summary, I think in any good solution it has got to encompass more than just the device and it's got to look at the end-to-end security, which is network, data and apps.

HARKINS: I think you're totally right and it's two aspects, mobile device management

many, and you'd have to flip them all around and say, "Here are the only things I'm going to allow running on it."

DATOO: You're absolutely right about the white list. I think what's really interesting about the white list is in the world of end-users going out and buying their own device, it's really difficult to enforce the white list. I think that works really well when the company buys the device and you say, "I bought this device and you're only allowed to

run these four or five apps." I think in the BYOD world, the black list - as difficult and as painful as it may be - has easier end-user adoption than the white list.

HARKINS: Yeah I completely agree with you and the hope that I would have as a consumer of mobile device security solutions is when and if we can containerize effectively, if I can create an enterprise section of that device in a way that would allow me to white list and would make that manageable and then have segmented off the user side, but we'll see if we ever get there.

"We need to find a way to get employees to accept their new security responsibilities by providing them the ability to protect themselves across all their online identities."

BENJAMIN WYRICK, VASCO

as well as the mobile security side of it, and our perspective on how we're looking at it within Intel's enterprise is very similar to what you're talking about. You've got to look at end-to-end and you also have to look at it device-by-device, and look at the inherent trust I have in the device and the operating system and what's on it. You mentioned black listing. Another approach if you're going to do something and say enable a capability to get access to the super secret stuff is you might want to use white listing and say, "Here are the only things that are appropriate on this device if it's going to be accessing the super secret stuff," because the many things you would have to black list might be just too

Benjamin, how does the BYO change some of the traditional organizational elements of providing security beyond what we've already chatted about? Are there other things that we've missed here in our discussion around that traditional way and how that's changing or needs to change?

WYRICK: BYOD creates this opportunity for simplifying the enterprise authentication architecture. There are more and more users and more and more devices and more types and complex passwords and more and more networks and applications in the cloud. It's becoming very challenging to properly protect the data. I think we see that everyday in the news with any kind of update you get

“If you ... set the right expectations and essentially trust the employees to act appropriately, we’ve seen the employees accept that kind of new security responsibility.”

MALCOLM HARKINS, INTEL

- here’s the latest data breach. I think some of the complexity is the root cause of this. What I see is an opportunity to focus away from the data for a moment and focus on securing that user by leveraging the mobile device for security, what’s called bring-your-own-token, much like VASCO has done, Malcolm as you know with Intel, embedding these credentials natively into the IPT chipset. If we can begin leveraging this opportunity to eliminate static passwords and expand dynamic credentials across the enterprise and the entire Internet, everyone will benefit. It will provide an efficient way to collaborate and exchange ideas and information, but provide the security that I think we all want and we all need.

HARKINS: I totally agree with you on that and I think even where things are going today and not that far out in the future with things like near field communication where I’ve got my handheld proximal to my laptop and I’m using the telemetry of that to help authenticate Malcolm is with his devices, it gives me a high level of trust in addition to the authentication stuff that you mentioned.

We’re just about done here, but are there any closing comments from any of you? I can start first and then we can go around and get our closing summary.

From my perspective and Intel’s enterprise perspective, we’re looking at things like BYO and the consumerization as an opportunity

and so we’re really focusing on it, as our core mission and purpose as a security team is protecting to enable. Enable new users, enable new usages and enable new devices, but do it in a way that we capture the benefits, some of which we’ve discussed here today, but also do it in a way that’s reasonably protecting of the enterprise. Ahmed, any closing thoughts from you?

DATOO: I couldn’t have said it better myself. I think we’ve talked about all the security sets of risks and concerns. I really view BYOD as an opportunity. I would start with the perspective of, how do I use this as an opportunity to drive the business forward and make my users more productive? Start there and try to figure out, “What do I need to do to protect the organization?” If you start with that sort of mentality you will identify opportunities to how you will use mobile either through applications or through figuring out what existing business processes you can put on the mobile device. Really view this as an opportunity because you’re not spending money on the devices and, in some instances, you’re not even spending money for the service plan. So there’s a huge opportunity to provide business benefits to the organization.

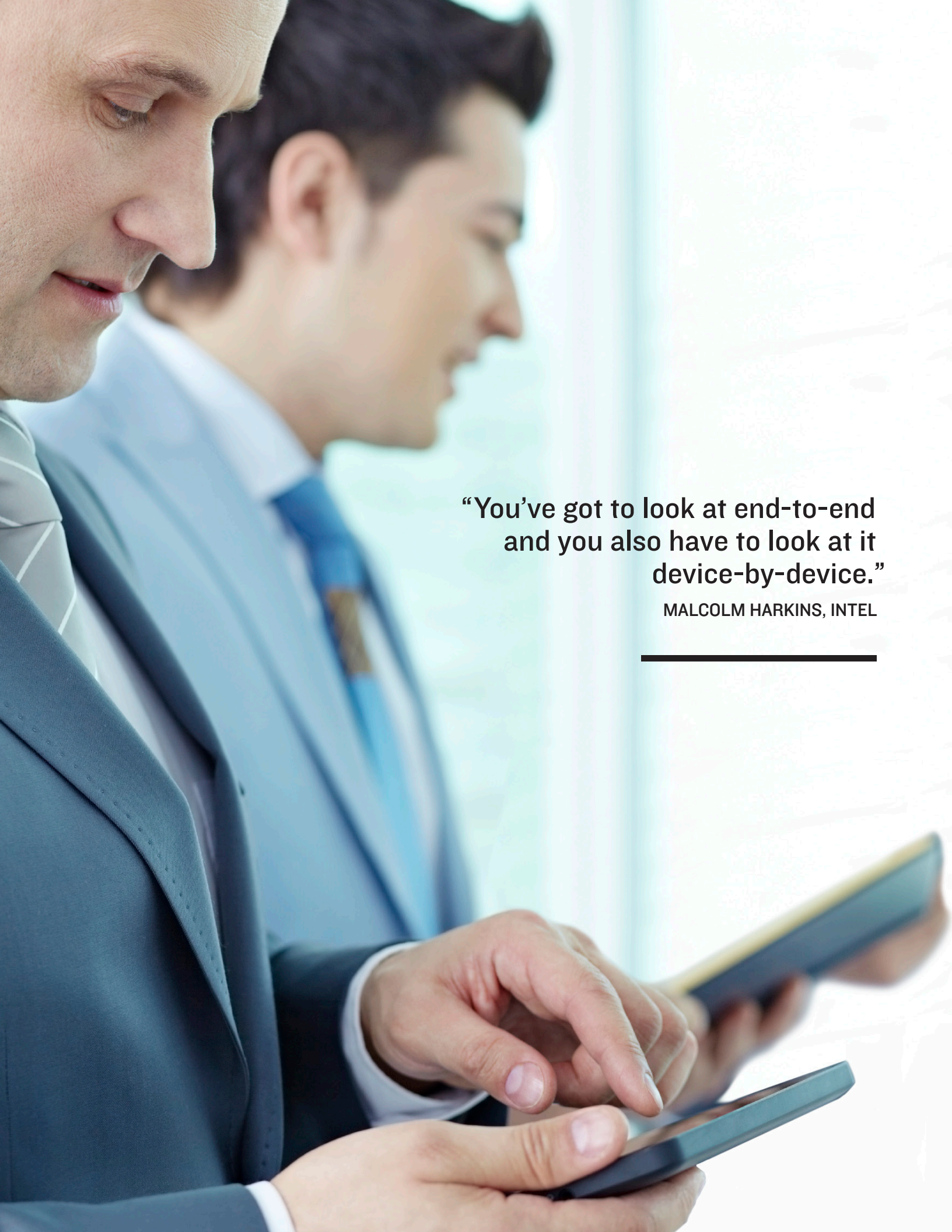
HARKINS: Benjamin?

WYRICK: From our side, this creates a very good opportunity for the employee as the lines begin to blur between their work

and their personal life as things become united on these mobile devices and access is broader. I think it’s a good opportunity for the industry and the entire Internet ecosystem to enable these users in a way that allows and helps us authenticate those users in a way to protect the data. That’s a bit of the shift that we’re seeing. By enabling this user, maybe this makes the network environment a bit simpler for the company; maybe it drives down that cost, but for sure it will enable that user to protect themselves and that access to their work applications, but also more and more as those lines begin to blur between their work and personal applications. I think that tends to be our view and it’s a real opportunity.

HARKINS: Dan, closing comments from you?

FORD: I was just at a conference a couple of weeks ago held by the United States Air Force and General William T. Lord, the current CIO for the Air Force, stated that we need to be able to operate at the levels of efficiency in a state where we’re always under attack. I think that’s kind of what we should be treating the mobile world as, the Wild Wild West. Assume that’s going to be compromised and because we know especially how open Android is and the malicious software that’s being reported almost on a daily basis, how can we ensure the integrity of the devices and the data and coming up in a known trusted state? I think this is one of the unique things as to how Fixmo was able to apply these. It doesn’t matter if it is a Blackberry or an Android device or an IOS device; how do we ensure the integrity of our data and the phones themselves always being in a known trusted state? I think that’s kind of where I see this world moving to as well. You need to make sure of the authentication of the users and we know who they are and it goes back to the old triple A - authenticate, authorize, and have full accounting of all actions that were taking place. ■

A photograph of two men in business suits. The man in the foreground is looking down at a tablet he is holding with both hands. The man behind him is also looking at a tablet. They are in a brightly lit office environment with large windows in the background.

**“You’ve got to look at end-to-end
and you also have to look at it
device-by-device.”**

MALCOLM HARKINS, INTEL

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401
sales@ismgcorp.com

