WEBINAR TRANSCRIPT

Mobile Technology:
How to Mitigate the Risks

FEATURING

Terrell Herzig, CISO, UAB Medicine

Paula Skokowski, VP - Products & Marketing, Accellion

Scott Ashdown, Director - Products and Solutions, Imation

Robert Hamilton, Senior Product Marketing Manager - Data Loss Prevention, Symantec

Transcript of the Webinar Panel Discussion

ISMG INFORMATION SECURITY MEDIA GROUP

Mobile Technology: How to Mitigate the Risks

Sponsored by

Accellion imation symantec

Smart phones, laptops, tablet PCs, optical discs and USB devices. There are many new mobile devices and emerging technologies to help today's professionals do their jobs in any location - and increasingly private business is being conducted on personal digital and storage devices. Yet, these technologies create new risks to the security of information systems and privacy of protected data.

TERRELL HERZIG
CISO, UAB Medicine

PAULA SKOKOWSKI
VP, Products & Marketing
Accellion

SCOTT ASHDOWN
Director, Products & Solutions
Imation

ROBERT HAMILTON
Senior Product Marketing Manager, Data Loss Prevention
Symantec

See "Mobile Technology: How to Mitigate The Risks." VIEW WEBINAR NOW »

How do you ensure that critical information remains secure on personal mobile devices - even when the devices are lost or stolen? Read on to learn from this expert panel:

- Proper inventory management of mobile devices - and remember, mobile means more than just smart phones;
- Creating and enforcing mobile security policies;
- Strategies for encryption, data loss prevention and other elements of layered security to protect devices and systems;
- Unique mobile challenges for regulated industries such as financial services, government and healthcare.

The Panel

Terrell Herzig,
CISO, UAB Medicine
Herzig heads a team of security specialists at the delivery system, which includes a 1,000-bed hospital and numerous outpatient facilities throughout the state. He is editor of the book, "Information Security in Healthcare: Managing Risk," published by the Healthcare Information and Management Systems Society. He speaks widely on the topic of securing mobile devices.

Paula Skokowski,
VP - Products & Marketing, Accellion
Ms. Skokowski joined Accellion in February 2007 and oversees the company's product development and marketing initiatives. Accellion provides secure, mobile file sharing solutions that offer ease-of-use internal and external enterprise users need, while giving IT organizations the security protection they require. Ms. Skokowski has more than 20 years experience in new product introduction for pre and post-IPO companies in Silicon Valley.

Scott Ashdown,
Director - Products and Solutions, Imation
Scott Ashdown has over 15 years of experience in product development and product management in the data security, authentication, and VoIP industries. He held increasingly senior positions at MPR Teltech, Bioscrypt, ActivIdentity, CounterPath, and Wesley Clover prior to joining Imation. Focused on translating market needs into well-resolved products, Scott holds a Bachelor of Engineering in Computer Systems from Carleton University.

Robert Hamilton,
Senior Product Marketing Manager - Data Loss Prevention, Symantec
As Senior Manager, Product Marketing, Data Loss Prevention at Symantec, Robert Hamilton works with security and privacy executives at leading Fortune 500 companies across all industries to help them protect their confidential data. Symantec is the acknowledged market leader in Data Loss Prevention with the only unified solution to discover, monitor, and protect confidential data wherever it is stored or used.

Transcript

TERRELL HERZIG: What are the most popular mobile devices that we currently see out there? I know in my particular industry, we see a lot of smart phones and we see a lot of tablet computers. Specifically, we see a lot of iPads and Android-type devices, and the same in the phone market: iPhones and Android devices predominantly. Then we see what I like to refer to as mobile media, and in that we include thumb drives and external hard drives. I would be interested to hear from the other panelists, if they're seeing similar types of devices or what are they seeing in their respective markets. Paula, do you have anything you would like to add to that?

PAULA SKOKOWSKI: From our perspective, the iPad has really been a catalyst in the marketplace for people wanting to do a lot with information sharing on a mobile device. From our perspective, that sort of overshadows everything else in that it's really pushing the limits and pushing organizations to figure out how to enable business users to access information securely and stay out of trouble with an iPad.

HERZIG: Excellent. Scott, Robert, do you have any comments you'd like to add?

ROBERT HAMILTON: We see both iPads and Android devices. When we look at the device that people want to buy and bring into work, it's largely the iPad. And as companies are looking at moving to a mobile platform, they're really seriously considering Android

> "Could you imagine somebody being out in the field and getting a notification that they couldn't receive the data on their iPad because it contained confidential data and that they need to go and drag their PC out in order to get that e-mail?"
>
> ROBERT HAMILTON, SYMANTEC

> "How you deal with security on the device is going to impact the user's usability of that device, and you've got to remember they're going out and wanting to use these devices to increase their productivity."
>
> TERRELL HERZIG, UAB MEDICINE

because of the cost and management possibilities. We see both of them.

SCOTT ASHDOWN: We see several classes of devices as well. When it comes to mobile devices, people definitely are thinking about and have smart phones, iPads and other tablets. Users are trying to be mobile, mobility being the main thing that they need. USB devices are showing up a lot. Obviously, we sell those so we're maybe a little biased, but we do see lots of thumb drives and external hard drives, a whole range of them, because users are bringing their own stuff in and you have a lot more users that have access to those because they're ultimately inexpensive.

HERZIG: Paula, I know in your presentation you mentioned that there are a lot of files that users commonly share via mobile technologies. Can you give us examples of some of those and elaborate a little bit about that?

SKOKOWSKI: When you think about why … there's such a demand for mobile devices, it's really because professional people and businesspeople are looking to either increase productivity, increase their responsiveness or enrich their communication. Basically, they want to be able to keep business moving even when they're not sitting at their desk and they're outside the walls of their office or organization.

What are some of the things that they're doing? Certainly PowerPoints are very popular in terms of wanting to facilitate presentations when people are on the road getting updates. Also, any sort of document that's under review. That could be a proposal. It could be pricing – updating pricing – for sales. It could be spreadsheets, contracts. Really, if you think about what the documents are that people are passing back and forth during the course of the day in order to move business forward, those are the files people want access to on their mobile device.

With Accellion, people ask us: What size file can you manage? When we're not talking mobile, there's really no physical limit; there's just sort of a practical limit. We do have some of our customers moving 100 GB files, but that's really not a sensible thing to be doing on a mobile device. We're only just starting to see how far people want to push it on a mobile device, but certainly devices that are megabytes in size are quite reasonable to be accessing, viewing, possibly editing and re-uploading over a mobile device.

HERZIG: Robert, I noticed in your presentation that you had mentioned some specific risks of using tablets and tablet computing. Could you elaborate on that a little bit?

HAMILTON: It's really easy to share information to your personal e-mail, social networking or cloud-storage devices; it's really not a lot different from PCs, which are currently covered by DLP solutions. Really, the biggest risk to data is sending sensitive or confidential data out over your corporate e-mail system, which is something that customers have been using DLP to guard against now for years.

HERZIG: I think you hit on a key topic there that I always like to introduce whenever I'm speaking with people about mobile devices, and that's the issue of data loss, or data leakage as it sometimes is referred to. And I'm glad you mentioned DLP solutions. When it comes to it, how does your tablet solution fit into an overall data loss prevention program?

HAMILTON: We think of DLP as three distinct things. The first is discovery, understanding where your confidential data is. The next is monitoring its use, where it's coming from and where it's going to. And third is being able to take actions to protect it. So three things: discover, monitor and protect. Our tablet solution fits within the "monitor" and "protect" components and leverages any policies that may be already in place. You're looking for who is sending sensitive data out over the network and then being able to take measures to stop it.

HERZIG: Robert, if you had a chance to address people's concerns about DLP, what would you say they misunderstand the most about the use of DLP in today's mobile environment?

HAMILTON: I'd say that most misunderstood is that in order to protect data, you need to restrict the use of the device itself and, potentially, certain applications. There are DLP applications out there that limit the receipt of confidential data on a device. Now could you imagine somebody being out in the field and getting a notification that they couldn't receive the data on their iPad because it contained confidential data and

that they need to go and drag their PC out in order to get that e-mail?

It's kind of silly. I've also seen people, when it comes to mobile devices, actually restrict the use of USB drives, even seeing epoxy in the ports. What I want to leave you with is the thought that you can essentially be able to give your users unrestricted access to these devices, unrestricted access to applications and still be able to protect data at the same time.

HERZIG: That's a good point, Robert, and that leads into some of the policy discussions and things like that, and you actually mentioned USB port restrictions. One of the questions that I get a lot is: What are the biggest challenges to enforcing a mobile security policy? And I kind of agree with you. How you deal with security on the device is going to impact the user's usability of that device, and you've got to remember they're going out and wanting to use these devices to increase their productivity, but we have a responsibility, of course, to make sure that they use it in an appropriate manner.

One of the things that we tend to do is we use a complementary set of products. We look at it from the data loss perspective; we look at it from designing and building policy and educating the end user. But then we also have to deal with how it synchs up with the device. I know Paula has talked a little bit about how to do secure file sharing. Paula, what are some of those warning signs that I need to look at as a security officer for my organization that might throw up a red flag, that maybe some files that are being transferred shouldn't be transferred?

SKOKOWSKI: Coming from Accellion, I have a different perspective than perhaps some of the other panel members. One of the issues is USBs. That is, if you're allowing people to share files via a USB stick, you only have to do a search on data breaches to know that this is an issue. In terms of a security policy as it refers to a mobile device, first of all what we advocate is if you're going to implement some controls, I would agree with the other panelists that you can't stop something happening or restrict access, unless you enable a way to get to the information. Just shutting something off is going to make a motivated business user find a workaround.

In the case of file sharing, many business users have easy access to the cloud. They will just go up there and find themselves a free, personal file-storage, file-sharing, file-synching solution. There are many available. Dropbox is an incredibly useful application for personal use, but when it's used for enterprise use or business use, there's zero oversight, tracking management. From a mobile-security policy, if you're going to block the things that get you in trouble, if you decide, "We're going to block access to free file-sharing accounts," you have to, at the same time, provide a solution that lets people securely access enterprise information.

The bar is set very high. Consumer apps are incredibly easy to use. They work and that has to be true for any enterprise solution on a mobile device. If you're not going to let

"Just shutting something off is going to make a motivated business user find a workaround."

PAULA SKOKOWSKI, ACCELLION

people do things, you'd better give them a way to do it that seems just as easy from their perspective, but at the same time means that the IT and security teams have the tools they need to manage users, set security policy and set privileges.

For instance, with our mobile app, you can decide which users are allowed to view files, which users are allowed to locally save files onto a device and which aren't. And that's something that you have to have the ability to configure and also communicate to your users as part of your policy.

HERZIG: That's a good point. … It's important to get a firm idea of what devices [are being used] and how those devices are being used in your organization before even creating such a mobile-security policy. What we found when we were designing our solutions here is that there's a whole harvest of different things we need to account for. As you hit on and Robert alluded to was the use of USB devices not only to transfer files to the device … but things like thumb drives and even external hard drives that, at least in healthcare, if it's got PHI on it, it really needs to be encrypted.

Scott, when it comes to USB storage devices and securing the devices, can you, from your presentation, tell us what you think is most overlooked by organizations when you get to USB and USB device storage?

ASHDOWN: I think we're talking about two kinds of devices here: the ones that are authorized and the ones that aren't. You really need to consider the unauthorized devices first. You've got this consumerization of IT thing that everyone's sure means people with their iPhones, but it means everything. It means the teleworker who's using a general laptop at home and it means the guy who's bringing in a $3 flash drive he got at Best Buy and using it to transfer files around. These things are really plentiful now in offices. USB devices definitely are. And no matter what you plan around the authorized ones, the unauthorized ones represent the back door and users take advantage, just like Paula said. I wouldn't go so far as to say that USB devices existing are an issue. USB devices can hold data, but almost any of the devices today can exist as storage devices in some form. USB devices, given the way they attach to your network and are used, are actually in some ways a whole lot less of a problem than say a device that's starting to send e-mail around or has other wireless capabilities, for example.

When it comes to USB devices, you really have to protect the systems in your organization, like Robert was saying, with some form of data-leakage prevention or protection, whichever you want to call it. You want to make sure that the iPad, SD card, CD or a USB device can't be used to just suck data out of your network. If you can't control that media in question, you probably shouldn't be letting data escape onto them.

Control can definitely be pretty simple. You can block out all devices. Robert was mentioning epoxying ports and things like that. You can be more fine-grained by only allowing data of certain attributes to be pulled out of your network. But you're going to need a way to make exceptions for certain individuals like IT staff or executives may need additional flexibility; IT staff because of their job function and it may be necessary in some cases for an executive to take what they want on whatever device they want. If you don't have a solution with compromises that can be used in the real world, then you're probably not going to have an ideal solution anyway.

That's all of the unauthorized stuff. As soon as you say you want to authorize a device, now you're saying you're going to allow data to leave your organization on this. You really want to be making sure there are two things happening: that the data's only usable by the right person or persons and that you actually know what that data is. The first part of it, we'll tell you that if you're taking the data out of the organization, that data should be encrypted and that encryption should be protected with authentication. How you do those things is fairly important and there are different levels of security, typically hardware versus software, encryption and authentication. I mean, software encryption is certainly inexpensive, but it's much more susceptible to attack. The host computer or the host device has the keys on it; they invariably make it into a swap file, that type of thing. For a high-security organization, sometimes hardware encryption is better because you've got that trusted environment doing that encryption.

Authentication's the same sort of thing. No matter how good your encryption is, if it's protected with weak authentication like a short password, you might as well not be using encryption at all because the

point people are going to attack is that authentication point. You definitely want to make sure that only the owner of the data can get into that data, somebody who's authorized for it. In high-security environments, both for large corporations and government, multifactor authentication is something a lot of people look at. It could be a password and a biometric or a password and a token, something else like that. Again, implementation and hardware is the better solution.

Software-based authentication, again, is inexpensive, but a powerful desktop computer today can break a typical eight-character password in about 24 hours. If you've got all this fancy encryption protected with an eight-character password, anybody who wants to get that is going to get it pretty quick. Now that's just external attackers … but still, important stuff to be looked at.

If you're trying to say, "Am I going to deal with an authorized device and how do I want to use it in my organization," map it up against your security and look at how the technology is implemented. We've seen devices that are supposed to protect data, but we find out they have secret commands and you can send them and they unlock. I won't mention the names of products, but this is not the kind of product you want your data stored on if you're letting users take it out of your organization. The best assurance here is to get a product with a well-known security certification and one that covers all the security processes from authentication right down to encryption and storage.

My overall answer would be to manage your unauthorized devices, like Robert was saying; DLP solutions definitely. Make sure your authorized devices are encrypted and that they have solid authentication policies on them so that encryption can actually do its job.

HERZIG: Good point. And that reinforces, too, some of the things I had talked about in my presentation. Before we even approach the policy, including creating it, you always will need to handle exceptions in the policy: what qualifies as an exception and who to see about getting approval for the exceptions within the policy. One of the things that we found that we had extreme difficulty with out of the starting gate was trying to determine who in the organization was using devices and how they were being used and which ones would actually become unauthorized versus authorized. We used several products to gain a very nice inventory of what data was being moved among the different USB products and which ones were being used.

We then set forth, saying, "Here are the types of devices that we would support." Then we educated our user community as to why we wanted to select a certain drive, for example, and a certain encryption scheme versus the $9 thumb drive that you would get at an office supply store or even one of the discount retailer stores. And that we got a lot of mileage out of because people a lot of times just don't understand what the issues are.

> "It's important to get a firm idea of what devices [are being used] and how those devices are being used in your organization before even creating such a mobile-security policy."
>
> TERRELL HERZIG, UAB MEDICINE

Robert, in your presentation you talked about best practices around educating users for safe mobile computing. Would you like to take a few minutes and refresh the audience on what some of those best practices are? I know it really helps if the user understands why you're asking them to use certain devices because a lot of times they just don't understand the difference in the technologies and things.

HAMILTON: Safe mobile computing is a pretty broad area, so let me focus my comments in on data loss. You really can't hold your users responsible for identifying what is and isn't confidential data, at least all the time. It's really tough for people to make that decision. So as far as best practices, what we've found from our experience with customers is that one of the best practices is actively educating users as they're using the confidential data. What we have is something we call a "bounce-back" e-mail. That is, when somebody sends out confidential data over e-mail, the DLP system immediately notifies them of what they've done. This use of a bounce-back e-mail, more than any other practice, can reduce risk substantially. We've seen as much as an 80-percent decrease in DLP incidents in as little as two weeks when customers have implemented this type of control.

HERZIG: Paula, one of the things that I would like to get to is, once you've got the policy created, you're educating users and you're getting it out there, what safety tips that you presented in your presentation should be part of a good, solid mobile-device policy?

SKOKOWSKI: We recommend that, as part of securing file sharing on a mobile device, an organization blocks access to free file sharing. If you don't block it, it's going to go on. Everybody knows that it's going on in the organization anyway.

Next is, as part of the security policy, carefully considering where information can be stored, whether it can be stored in the public cloud or whether it has to be stored within the firewall on the private cloud. That's another major consideration.

Then, along with if you're going to block access to free things, you have to provision a suitable solution, and I think a recurrent theme has been this idea of education of users, and I think that, in the case of mobile, there's a general lack of awareness of some of the hazards of what people do. They are very quick to get their hands on apps and, as soon as they've solved a need, they don't really think about it again. There's a big education need. I like the previous comment about a bounce-back e-mail that sort of explains, "Well, did you realize you just did something?" That's pretty immediate feedback, but there needs to also be up-front education about how people should be viewing use of their mobile devices and some of the safeguards that they need to implement, whether it be password protection or use of particular approved apps. We haven't talked about that much, but for enterprise use, the use of white-vested applications, we see a lot of our customers heading in that direction.

HERZIG: You hit on a key point there that we have encountered as well. We use data-loss prevention tools here as an accompaniment to our mobile strategies, and one of the things that we routinely will see, for example, is people e-mailing credit card data out to individuals for payment. One of them that we caught one time in our product was an individual had e-mailed all of her credit card information, including her secure code on the back of the card, to her daughter's college so that she could pay her daughter's tuition bill. They just had not thought about all the different ways that information could be compromised after it was presented for its original use. That's one of the things that education can help with.

Scott, from an organizational perspective and using USB tools - or devices - to move data and things like this, how can I better monitor and enforce these policies in terms of USB and storage?

ASHDOWN: We've talked about the blockage of the data flow. If you block everything, we all know it can decrease user convenience hugely and it's also going to push stuff into the "loss" spot and, basically, people are going to move data into other areas. The DoD, for reasons other than data leakage, banned USB flash drives, and, several months later, somebody leaks hundreds of pages of documents on a CD to WikiLeaks.

What do you do to better monitor and enforce policy on storage devices? We have an analogy. We really look to the tunnel built under the English Channel some years ago. When they designed this tunnel, it became totally evident that leaks – in this case water leaks – were definitely going to happen no matter what they did, so they let the leaks happen and they built another tunnel inside it, another tunnel within a tunnel directing the water around that inner tunnel. And you could do the thing with devices, USB devices specifically.

Putting a DLP solution in place is the biggest thing. That's sort of your outer tunnel. If you can seriously stop flood from happening and, since you know the water's going to leak - you get stuff out of your network - the devices the user can use have to be authorized devices. If it's not authorized devices and you don't know what those devices are and you aren't controlling them well with all of that data, then you have a huge problem. We talked about it before. Encryption and authentication are seriously important and for lots of reasons, but definitely the lost device problem. If you lose a device, what's going to happen when that data is actually lost; when it's maybe in the hands of a foreign government; when it's in the hands of a competitor; when it's in the hands of a regular citizen who decides he or she doesn't particularly like your company that much? You can get devices today that, even if you're a government organization and the data on that device is classified as top secret and you lose one of these devices, you don't need to report its loss. That's the level of security that's available today. And I'm not talking about thousands and thousands of dollars. They're not that expensive. It's $50.

This is the type of thing that you can get. What are you doing to protect things? For us, we see managing authentication policies is really, really important. If devices are leaving a network with data on them, you've got to make sure those passwords are complex enough that they're changing often enough and so on and so forth. It seems almost silly, but it's amazing how many folks will rely on short passwords on a USB device where they would never dream of issuing a laptop to a user, where the users have to log in or are going to have to follow password rules to change it every 30 days.

> "If you don't have a solution with compromises that can be used in the real world, then you're probably not going to have an ideal solution anyway."
>
> SCOTT ASHDOWN, IMATION

HERZIG: Some of the things you're pointing out here are very important because in healthcare, encryption's kind of a safe harbor under HITECH for the breach notification rule.

ASHDOWN: … That's really, really vital. In healthcare, you might lose a flash drive with patient records on it and it wasn't encrypted. If you're not careful there, you're going to be in pretty deep trouble with fines. There are two aspects to dealing with a situation like that, both around compliance. First of all, you've got to prove that all the data must have been on the device, so you have to show that you can actually do that. You have a DLP solution in place and you see the devices that are approved? That's great; that's perfect.

The second thing you're going to want to do is find out what data was actually on there. That's a really key aspect of monitoring and enforcing policy, which is having an audit of all the data flows that go onto these devices. If you don't know what's actually on that device and if they're dealing with it actively, preventing the data from going out there, withholding it, or passively, just being able to do it forensically and see what was there, you're really risking a lot. You're not only risking that regulatory compliance, but you're also risking this sort of unlimited cost of your leakage. In healthcare, your hospital might pay a couple of million dollars in fines because they have leaked some patient records, but they might pay ten times that in having to notify thousands, or tens of thousands, of people that their records were leaked. If they know what was leaked, that helps to definitely limit the cost and the exposure.

HERZIG: Not to mention the reputational hit that any organization would take. We all in today's age vote with our purchases and I don't know of a business out there that doesn't have competitors and when it comes down to reputation, it's a very expensive stake to take into consideration there.

What I would like to do at this point is touch on a very hot topic today. It certainly is for our organization. I'm sure it is in many others when it comes to mobile devices, and that is BYOD, or bring your own device. I would like each of the panelists to comment about how they feel about this. I know in healthcare, just for the points you pointed out Scott, we try to keep our devices organizationally owned. We are looking at a hybrid mix right now of allowing some personal devices and we have controls in place to prevent any device from coming in and being used. I would like to get everybody else's opinion on bring your own device and some of the ramifications that it would bring

"You really want to be making sure there are two things happening: that the data's only usable by the right person or persons and that you actually know what that data is."

SCOTT ASHDOWN, IMATION

to an organization out there. Robert, I'll let you kick that one off if you want to add some comments about it.

HAMILTON: It's basically an unstoppable trend, but it really depends on your industry and the departments that you work in. Just a few years ago you saw [Macintosh] starting to trickle into the organization and now they're coming in full force, whether the users buy them themselves or not. It's also simply where you now have the device that's an important connection to the outside world. In other words, this is the device that you use constantly. It's going to be pretty tough to deny individuals the ability to focus on one device for both work and personal use. I think it's a trend that's going to continue.

HERZIG: Excellent. Paula?

SKOKOWSKI: I think it's fascinating that businesses have basically gotten themselves in this dilemma because, I agree, I don't see any stopping of the trend of people bringing their own devices into work and, yet, that's incredibly complicating because it really blurs the line between personal and business and it's going to require some demarcation in these devices. We see it already. What applications are you allowed to use to access enterprise information? Can you access information? What are you allowed to store on the device? It's really amazing that, in a way, this has sort of snuck up on people because it's a major change. Think about all the efforts that went into provisioning people with computers, laptops and desktops and controlling the configuration, provisioning your employees and rolling out new apps and all the sort of energy that went into that. Yet somehow we've just let this whole wave of mobile devices infiltrate organizations with no control whatsoever.

We're seeing two sets of people. We're seeing those who are very security-conscious who are really trying to implement systems, controls and policies and get some sort of control over this. Then we see another set of people within enterprise organizations who say, "Yes, anything goes." I think that the "anything goes" strategy is probably short-lived, probably as long as it takes for there to be a security breach, which is going to happen unless they have some control. I would agree that it's here to stay and I think the organizations that start to grapple with it and really try and get some sort of control over it will, in the end, be in better shape.

> "If you lose a device, what's going to happen when that data is actually lost; when it's maybe in the hands of a foreign government; when it's in the hands of a competitor; when it's in the hands of a regular citizen who decides he or she doesn't particularly like your company that much?"
>
> SCOTT ASHDOWN, IMATION

HERZIG: I agree, Paula. That's one of the key points that I had tried to make in my presentation … looking at the fact that managing the data is of paramount importance when it comes to mobility. Getting that kind of issue resolved or dealt with head-on will help you in regard to what environment your devices are going to present themselves to the organization. Scott, do you have any comments you'd like to follow up on about bring your own device?

ASHDOWN: … People are doing it absolutely and they're going to continue to want to do it. For a lot of organizations, anything that's relatively complicated, they need a lot of time to evaluate. This is why operating systems don't get used right away, why new applications don't get used right away. Also, there's a lot of cost. This is why laptops don't get refreshed every year. Meanwhile, the people that are working at these companies may be going after the latest stuff and they want to use the latest things.

I agree with what's been said, that there has to be some kind of a separation. It's tough though because if you look at the kind of adoration of things that you might want to assemble in one spot, it's not as easy as the comparatively easy situation of, say, running multiple apps on a Java card was ten years ago or 15 years ago. That was something one group had a lot of control over, but we have quite the plethora of devices, operating systems, vendors and applications that are all out there, and I think that the successful way of separating things might be something that's actually going to let people bring their workspace – the things they need to do their job – to a different device.

> "It's going to be pretty tough to deny individuals the ability to focus on one device for both work and personal use."
>
> SCOTT ASHDOWN, IMATION

That might be the right thing, where if somebody wants to use their laptop or their tablet, they can bring an IT-sanctioned work environment to that device, allowing them to - in some way - provide a barrier between work and personal use.

HERZIG: Those are some of the approaches we're taking in healthcare - at least from my perspective - trying to make sure that we've got both usability and some very definitively drawn boundaries there of what works and what wouldn't. Robert, do you want to kick us off with any closing comments?

HAMILTON: The onslaught of mobile devices has caused people to consider the potential loss of data on these devices. It's something they should be concerned about in organizations at large. Our recommendation is that if you haven't started looking into it yet, you might want to start considering data loss prevention as a company-wide solution.

HERZIG: Paula?

SKOKOWSKI: If you haven't considered how people are sharing files on a mobile device, now would be a good time to do that because it will have an effect on your data security.

HERZIG: Excellent. And Scott?

ASHDOWN: I definitely agree with Paula. Consider the risks to your organization. These devices represent a bridge out to the rest of the world, so anything in your network that a user can access can leave your organization using one of these devices. That's definitely an important thing.

The other thing I'd say is, as you're building a plan for what devices might be used, realize that data's not the only thing that they're being used for and definitely take a look at devices that are going to do more than one thing for somebody. The last thing you want to do is build a strategy around a device that's data-centric and then they'd be ignoring people authenticating the systems using cloud systems, tokens and so on.

Again, whether you're doing virtual-desktop work or you're carrying a portable workspace around with you, whether that's a tablet or something else, it's considering all those things and making sure that you're managing them as solutions. We talked a lot about data and it's more interesting and more powerful to be managing the data flow than it is to be managing the device. It's the solution that needs to be managed, what users are trying to do, as opposed to the system that they have in their hand. ■

VIEW WEBINAR NOW »

Don't miss "Mobile Technology: How to Mitigate the Risks"

http://www.bankinfosecurity.com/webinars.php?webinarID=256

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

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach Prevention. Response. Notification. TODAY

ISMG INFORMATION SECURITY MEDIA GROUP

4 Independence Way • Princeton, NJ • 08540 • www.ismgcorp.com