Bill:

Hi everyone this is Bill.

Speaker:

Hi Bill this is Speaker.

Bill:

Hey Speaker how are you?

Speaker:

I'm doing well and yourself?

Bill:

Pretty good, pretty good. No complaints on my side.

Speaker:

(Chuckles) other than it got real cold on us real quick.

Bill:

Yeah someone opened their refrigerator or everyone opened their refrigerators at once - cuts off mid sentence as new speaker connects - is this Speaker?

Speaker:

No this is Speaker.

Bill:

Hi Speaker how are you?

Speaker:

Good.

Speaker:

Yeah Bill I'm here too this is speaker.

Bill:

Hey Speaker how you doing?

Speaker:

Doing alright how bout yourself?

Bill:

Good, really good. *brief pause* Well I thought uh, I thought we could get started if everybody's ok, we have several more that are registered but I'm sure that they'll be logging in as we go. Um, I have a - can everybody see my screen?

All speakers:

Yes.

Bill:

Ok great. So this is a bit of different structure then we normally do, but I thought it was kind of an interesting format because um I'm certainly being asked a lot of questions about it and I'm sure you all are thinking about it as well, and that is how do we develop policy around mobile devices and I thought we could do this more from a collaboration amongst many minds, come up with an uber policy or at least a framework that then I could send to everybody, you know the output from this and then everyone has this for their own records as they develop something that might be more tailored for themselves. Does anybody have any comments on that or the session overview that you wanted to bring to the table before we got started?

Speaker:

I think it’s a great idea Bill I'm curious to see how it works out for us.

Bill:

Cool! Great, and I think that I don't see much of a difference form what we've done, but I think the difference is that we'll actually have something sort of as a net result of it and its from several minds working on it as one. And we've all been exposed to different technologies, techniques, and different corporate philosophies and I think from that point of view you'll be able to balance this out so that when you're actually in a meeting - if this was so easy we're wouldn't be talking about it - so if you're in a meeting talking to senior executives and such you can not only say this is what I think we should do but based on collaboration with peers, that’s part of my intent with it.

So from a philosophy - I know from some of you on the phone - that some of you have varying philosophies, maybe we should capture the philosophical approaches just from a spectrum of zero to ten, zero being like we don't let anything, we don't let any mobile devices into our network to the other side of the spectrum we let everything in and we're trying to develop policy around it now that we've done that. So why don't we just share a couple philosophical approaches and then as we go let's, I formed a kind of an outline here from categories of devices, Identity based access, to different issues regarding if someone has their droid verizon tablet that’s has the droid applications on it, that they can

hit salesforce for example direct what's our policy about accessing or Hr application versus coming into company applications, how many device type categories, - what's our policy around - and I just put a couple these are meant to change and grow or shorten - but data loss, backups, encryption, time bombing, remote wipe, any other technology capabilities that we wanna bring up, and then situations. I think this is kinda, we have contractors bringing devices, kiosk access, access from home, employees on the road, employees at work that are bringing their own tablets, so we have a corporate use of internet if they want to surf the internet on their tablet direct 4G or the wireless.

Bill:

So let's start with philosophies, does anybody want to help me get started there?

Speaker:

This is speaker I can get started. So without addressing each one of those points individually I would say we're probably a seven on your scale, where we allow tablet or your phone based devices, which are wifi enabled, we pretty much enable those to do whatever they need to do on the network. Now if it's a computer device then we only allow it to have internet access, it doesn't get any access to our secure network, (pause) but we do help enable that in all cases.

Bill:

So allowing tablets and phone access and can you repeat the last part Speaker?

Speaker:

We allow tablets and phones on our network internally at all locations. If it's a laptop based device, so if it's either a windows, a linux, or apple, we don't specify any, we'll allow it internet access only it does not get file level or active directory authentication.

Bill:

Gotcha, perfect. Thank you.

Speaker:

This is Speaker3, and I can add to that, the only other difference with mine is that its only blackberry and iOS devices that get access on the wifi, laptop is the same policy.

Bill:

So BEZ and iOS, you allow them access to applications?

Speaker:

Well the only application they're really getting is email but -

Bill:

Gotcha.

Speaker:

Yeah.

Speaker:

This is Speaker, just to beat out Speaker there, we're about an 8, we allow iphones and droids on those we basically use Citrix from the tablets, although we don't restrict, I don't if you guys restrict and kind of file attachments or attaching to, there's some apps that let you sign in and connect to shares. I haven't eliminated that, I don't know of anyone using it right now, but I'd like to stop that if I could.

Bill:

So you're allowing uh, Speaker4 just to repeat yourself or just so I could understand it, are you saying that you don't allow file access now, or you do to these other devices via Citrix?

Speaker:

Through Citrix we do. We do although, on iPads there's no real drives, but there are apps out there I can get for Ipad to connect to my file shares that (Bill: Gotcha. Yep, Yep.) I don't prohibit, and that's a little concerning to me, but again I have such a big hole that someone could come in with a usb drive and download whatever they want, so you know I'm resting with this whole policy saying i want to plug this hole if I spend a lot of money but I got a lot of gaping holes in other areas I haven't addressed, so I'm wrestling with the logic of that.

Speaker:

I think Jim made a really good point and I'll echo that. We - We don't inhibit but we also don't enable in some cases.

Speaker:

Mmhmmm.

Speaker:

I think there's a big distinction between that.

Speaker:

Yeah.

Bill:

So you don't inhibit access but you don't enable either, is that what you're referring, what you're saying?

Speaker:

Correct. So they're kind of on their own if they find a cool, innovative way of doing it. Then we learn about it and then I think the stage we're at now, we're educating ourselves and figuring out which one of those things makes sense and which ones we ones we do want to enable.

Speaker:

I guess the thing about, again I don't know if you guys prohibit the use of usb drives but, you know, for someone to take data out of this building, I guess the tablets and the wifis, that makes it easier, a little more remote, little more covert, but again they can come in here, put a usb drive in their machine, download stuff and walk out the door.

Speaker:

Yeah.

Speaker:

I don't wanna just throw up my hands but, I'm throwing up my hands I guess.

Bill:

Well let's, um I do have my -where - where is my section here on policy. Uh I should probably put a section here on USB um so I guess we're sort of talking about poli- interesting policy but then we have the unique perspective on what we can enforce. So is, is part of -part of the output for today's meeting to talk about what we want the - what are some- what can we do from a policy perspective but we can't enforce necessarily or are unwilling to enforce, based on corporate culture and what are those things we're actually willing to take on from an enforcement point of view?

Speaker:

Speaker from American Chemistry Council, I think it actually goes beyond that. The question for me is - you know is uh - moving towards the vision of mobile user, how can I enable my folks to get what they need to be able to do their job. So if it was left to me I'd restrict access to everything because I'm the security Nazi, but my organization says no. My CEO no, I want this as wide open and easily accessible as possible. Now how do I balance that against my you know inning *pause* I guess instinct to lock everything down.

Speaker:

Mmmhmmm.

Speaker:

You know is it - is it through written policy, and if somebody does happen to walk away with a USB full of information that somehow makes its way onto the internet then, I mean would it - do I have a get out of jail free card?

Speaker:

Probably not.

Speaker:

Right.

Speaker:

But there's the thing, if we can restrict it by technology do we really need policy? Other than staying with us, does policy really guide people's practice?

Speaker:

Well the policy should also dictate what you're doing technologically.

Speaker:

Yeah from a notification standpoint, but there's - there's nothing to really have to guide people's actions if you've taken care of it through technology.

Speaker:

Right.

Speaker:

Yeah from a cyber security perspective you that we work with the chemical industry here at the American Chemistry Council and specifically with cyber security. And that's one of the things that they're actually working on right now. We're actually working on right now with our members and trying to educate our government on you know what re the standards that should be out there relating to cyber security that isn't going to kill our organization's or our members' ability to produce chemicals out there, and for us that it's to produce information and advocacy.

Speaker:

Mmhmmm.

Bill:

I guess one of the, one of the pieces that comes up with this policy part is if you have a content, if you have a right use for a company owned machine on a corporate local area network that is coming out through your security infrastructure and hitting a variety of resources they need to do their job, there's a web-surfing policy. However when you have a mobile device, and you bring a mobile device whether its a company owned phone or not that's a web-enabled browser, they can do what they want because there's no way for the corporation to have any sort of lock down on that, or at least it's harder to do that, and so they can also hit company cloud resources that are simple like HR websites and salesforce things like that so from a policy perspective is that something that one states. That no matter what device one has you have to follow the same standards of corporate use as if you were behind the company firewall.

Speaker:

Mmhmm.

Speaker:

Absolutely and the policy that I'm currently crafting right now, it says pretty much that, I'm trying to think of it off the top of my head but uh, an individual policy or I'm sorry an individual device once connected to our network has now, now has to be treated as a company device. Whether that's an Ipad, iOS or sorry Iphone, a uh android, any kind of android device, a blackberry, a laptop, whatever the case may be. The other thing that I'm working to try and do is implement a mobile device management solution. I'm currently looking at Air Watch as well as Mobile Iron to help me with that piece of it.

Speaker:

You plan to have your users accept the policy and hit the box and either that or they're not on the network?

Speaker:

That is correct yes.

Speaker:

Mhhmm k.

Speaker:

And they don't - not only are they not on the network but they don't even get access to email.

Speaker:

Mmhmm.

Speaker:

And you're doing that as part of NAC or as part of the end mobile device management tool?

Speaker:

As part of the mobile device management.

Speaker:

Ok.

Speaker:

Right now the only way we can restrict it is primarily through, or not restrict it but put any type of restriction mobile devices is through Active Sync and Exchange.

Speaker:

Mmhmmm.

Speaker:

We've uh, we've basically here at the ACC with the exception of our finance application, everything else is web-enabled so as long as you have your user ID and your password you should be able to connect to it from any device.

Bill:

I brought up this point about identity based access to applications so I guess if you can identify a user who has an identity in the company, that has gone through the human resource process, then they would normally be given a rights to applications on your network based on their hiring, based on their level of hire, based on who they are. I guess in some respects that if they are in the directory structure of your network they be given the appropriate rights and permissions to applications that would then adhere to whatever device they are going to be using. Would that be a fair statement?

Speaker:

I'm sorry I came in a little bit late. This is Speaker with Nettrition and I'm curious to interject. Are we under the assumption that everybody on these devices has already authenticated through some sort of SSL VPN type authentication or what's the sort of realm we're considering?

Bill:

Good question Speaker6 I think Speaker5 you might just want to go back through what you said but I think it’s you're trying to apply secure access through to all applications.

Speaker:

That is correct yes.

Bill:

Regardless of device type?

Speaker:

Because right, at this point in the conversation it almost seems like we're talking about authentication correct?

---Bill and a Speaker respond at the same time---

Bill:

Go ahead, sorry.

Speaker:

Speaker with American Chemistry Council. I think the way we got there was you know I made a comment right from our internal policy, which I'm currently working on mobile device management policy. What I'm working on is the ability to enable a mobile device management solution such as Mobile Iron or Iron, not Iron Watch, Air Watch, I get them confused sometimes, working on investigating those and that being the only way our employees can actually access our network or our network resources whether it be email or their time sheet, whatever the case may be.

Speaker:

And in terms of mobile are we actually making a distinction of something small, a handheld device or laptop, or someone working from home who just as well considered. I mean mobile and remote, are we making a distinction between that. So someone working at home, they're not necessarily mobile but they're certainly remote.

Speaker:

Yeah there's an additional layer on that piece of it. The way I describe mobile is any noncorporate device or any small handheld corporate device. So that would include as an example if we have internally issued laptops those are actually considered, to me they're considered mobile devices, but they don't need to go through the mobile device management solution because they're already controlled on our network through Cisco VPN you know from that particularly piece of it. They're internally managed through AD, but anything that is not specifically managed by AD. I guess the way that we got on the authentication piece was I mentioned that right now the only way that we have to restrict or place any policies on mobile devices is through our exchange active sync and right now we're just enforcing a pin on mobile.

Speaker:

I'm curious because my company just simply doesn't use up anything really beyond laptops for mobile or remote so I'm just kinda curious why anyone needs to make a distinction between a handheld or a laptop it seems like they'd all simply fall under the same, it's not on my VPN it's not a did I need some way of authenticating it's a why even make a distinction. I don't have a lot of corporate experience using those kinds of devices so I'm kind of a noob in terms of that.

Speaker:

Yeah I look at it from a laptop perspective. If it's already on our network and sitting in a docking station inside our office then it's managed by -

Speaker:

Oh certainly inside your office but in terms of take the laptop home, a lot of my employees work from home, but they all use laptops so I'm just wondering why the distinction between a laptop or a palm-held top or a tablet or what not. If it's not on my VPN or it's not getting behind my firewall within the corporation I would put it all under, in the same box, but like I said I don't have a lot of experience, perhaps they present different challenges but I'm not aware of them.

Speaker:

And I would agree the only distinction for me is I have no way of controlling an individual's level of, or at least right now, their level of virus protection or internet protection on their personal home laptops or computers. That would be the only distinction for me.

Speaker:

I would agree then, right.

Bill:

It seems that once those devices are, it seems that the closest with the walls of the castle being pushed down, and having multiple access points and sort of a corporate mandate to absorb different types of devices and if that device can see policy that you currently have through a directory structure then it's fine but if it can't then that's where it gets weird, that's where it gets a bit of an issue so how are people handling if someone is on the road and someone needs to hit an external system that's not on the network or does that not happen often with people on the phone?

Speaker:

It doesn't happen simply because everyone is authenticated through SSL VPN so I know who they are.

Speaker:

I'm not sure I completely understand your question Bill.

Bill:

Well if someone has to hit like salesforce or hit an HR application that's out and delivered from the internet but not, I'm not gonna use the word cloud because I don't like that word at the moment, but if it's an application that's being delivered outside of the company firewall and somebody needs to do their job by accessing it but they do not have to be authenticated after directory to access it they are accessing a service that's being provided to the organization but they don't need to be in corporate after directory to hit that. And for that matter for example, you can control what type of web training is being delivered down to the desktop through your regular infrastructure so if someone is doing web training we can differentiate that from watching YouTube for other purposes so you could sort of mitigate and allow all types of things and discriminate, but all of a sudden when someone brings a tablet and is running that from work and is bringing their tablet into work, how is policy going to be created for that use?

Speaker:

Got it, but I saw there's really two distinctions in what you've stated. So the first one if I had chosen to outsource a product and put it in the cloud, let's say salesforce for example, I really could care less, by the nature of me choosing that decision, I could care less what type of device they use to access it. That's not necessarily my problem. I put the rules and responsibilities in place and there's only a certain level of those I can put in play with a product like salesforce. And then access from inside of my network is a completely different topic.

Bill:

Yeah I've had to read these policies recently that are being created by legal departments and they really don't match reality, and that's what's a bit of struggle. I totally get what you're saying Speaker that it's not the problem of the CIO from a say that you can actually do something about it if something happens but do we address some of these things with policy and state in the employee handbook that an employee must adhere to the same policies that they would normally adhere to behind a company firewall when they're using a mobile device when accessing applications that don't require, I don't know what the word to say would be, but when they don't require access in the company network to go to.

Speaker:

Sure I think you can say it all you want but if you can't enforce it at the technological level its almost moot.

Speaker:

Right I was gonna agree saying how would I prevent somebody form bringing in their own laptop and connecting it to my internal network and just putting on DHCPing and getting access with that when I would have preferred that laptop not be brought into my network. I suppose if I register a list of 1000 MAC addresses or something and it didn't match the Mac address it's not given DHCP, I guess that's up to the capabilities of the firewall or the DHCP firewall you're using, but yeah a lot of these things just come down to you don't do these things and if we catch you that's a violation, so yeah a lot of it's hard.

Speaker:

But in your point you're assuming that that device is connecting from your trusted network. What if they're in a hotel?

Speaker:

Right, cuz in the case of using SSL VPN and using certificate base, could they export their certificate and place it someplace else and get access and download the SSL VPN software, Yes I guess it's the same situation. Of course which devices can I restrict and how else could you restrict them other than by MAC address I suppose and then could you just as well set that rogue device's MAC address to one that's already been known. I don't know how you'd solve that.

Speaker:

The question is whether you want to solve it or not.

Bill:

I think that's a good point just do we want to.

Speaker:

It depends how much of a control freak are you-

Speaker:

Well it's not about whether you're a control freak or not, it's about what your business needs you to enable them to be able to do. It's not really an IT problem, the problem is for us to put technologies in place to support either the philosophy or the rules by which the company operates.

Speaker:

Correct, but I said it goes back to the question is it solvable, so if it's not solvable then it's just policy. I think that was the crux of the question but maybe I missed something.

Bill:

So is it fair to say that some people on the phone are going to be having policies and just let the business know that these are gonna have to be a training and education and awareness part of the plan and not necessarily something that can be enforced with the technology.

Speaker:

Yeah in my case yes, Speaker from Nettrition, I would agree with that.

Bill:

Does anyone else have any areas that are similar?

Speaker:

Speaker, yes actually we approach that in many cases, we choose not to do it technologically.

Speaker:

Speaker with the American Chemistry Council same thing here. I mean from our legal and senior leadership the philosophy is is that we expect our employees to act with a certain amount of business conduct associated with our HR and association policies. And if they can't comply with that, that's when we really have to look at what the result is from that. Again you know from our perspective it is my job, as I believe someone else here said, to enable advocacy within our organization and do that to the level of importance of the data that's placed within our systems. I also inversely struggle with saving our organization from itself sometimes because of the lack of, I can't even think of a good word to put in this particular description, for lack of knowledge, let's say, of data that we have. There's no amount of convincing that can take place so we're kind of stuck in between you know we can make this as wide open as possible but recognize that you know our data could walk away and hearing that well what do we have that' so important that we can't have it walk away.

Speaker:

Speaker from Nettrition going through like a payment card industry, PCI process, a lot of simply comes down to policy. You have these policies in effect and are you enforcing and reviewing them, so policy plays a huge role in this.

Speaker:

Yeah speaker I would certainly appreciate any knowledge you have from a PCI perspective. We are going through that as well but it doesn’t seem to be overly restrictive because I think we're almost at the lowest level of PCI compliance.

Speaker:

Yeah I'm at the opposite level because we take cards, and we do our own processing so we have to hold the card on our disk, so yeah it’s huge, I've spent the last two years conforming to it, it's a monstrous project. And a lot of it simply, I'd say half of it is simply technology and half of it is simply policy and having the right documents in place and are our employees reviewing them and the ones that can be enforced are they being enforced, and the ones that have to be enforced by people are the people enforcing them, so yeah a lot of it is just an exercise is writing documents and passing them out and making sure people know about them.

Speaker:

Identifying who's watching the watchers right?

Speaker:

Exactly, is anybody else here doing PCI, other than the one person who responded at a low level?

Bill:

I think there's one other person on.

Speaker:

But like I said a lot of simply is you know, if you've ever read through the data security standards its, do you have this policy in effect? Are you reviewing it? Are you doing it? So it'd be like question one do you have this in place, are you actually doing it? Sometimes some of the questions are a little bit comical to read.

Bill:

Having some experience i that PCI world speaker, I would agree with you, but I think that it becomes, it can be very very, it can be hard to tackle mobility with 100 percent technology enforcement and I find that actually the education and awareness piece if that's handled from a philosophy that's education and awareness and not necessarily the hand of God slapping an employee down, I think if it's handled from education awareness it's actually is quite useful and would support the existing security apparatus quite nicely and we're finding huge progress. It's like the old fashioned days when you started putting content filters in you let people know you're putting content filters in all of a sudden like traffic got really fats on the network.

Speaker:

Chuckles right, that's exactly right. Like when you announce, when we implemented our sonic walls with your company. I announce, one day I just wanted to see what people were doing I didn't

enforce it anyway. Ok I'm gonna out content filters on starting tomorrow, and all of a sudden the warnings and such and what not went away.

Bill:

Chuckling

Bill:

So as far as, let's talk about from building out a policy, do you do - and then data, Speaker you mentioned the part about data leaving, do you philosophically, or just form a policy or technical perspective, want to deal with backing up devices, backing up data that is on mobile devices, and what is your all's thoughts on that.

Speaker:

Ahhhh, very good one. So within our policy also references our record retention policy and indicates that our repository for all corporate records is within our intranet we don't even use LAN shares any more, we use SharePoint. It also makes it very clear that mobile devices are not to be used for the storage of records in addition that for, obviously for editing that those types of activities, they're obviously used for that but should be moved to our corporate repository as soon as possible. And that's done simply through policy that's all.

Bill:

Ok great. Good point, great point. Anybody else have an example of them building, I hope everybody can see the document I'm working on right here, but does anybody else have an example of either a policy or, or actually an enforcement option that you all are thinking about or have in place?

Speaker:

This is Speaker, AHIP, and I talked to you bill about this as far as email. I don't have an MDM yet but it seems one of the big reasons and drivers to get it is because people, policy or not, are going to inadvertently, if they've got email on their iphone ipad whatever and they're gonna back it up to their laptop by mistake or they're gonna put it up to the cloud and now I've got email that really isn't supposed to be there, they shouldn't be backing it up. So I don't know what everybody else is doing if they don't have an MDM, how are you enforcing, or maybe you just can't, email just going to different clouds, personal computers at home, what are you guys, how are you guys taking a look at it?

Speaker:

I could tell you how we do it, I shouldn't say we, I could tell you how I do it at the ACC. When I discover that people are accessing their email from home I tell them it's wonderful because we make sure that they access it through owa through the web, but I also make sure that they understand that any time that they are in their email and they download anything to their personal computer, then in

the event that we get sued or um, -Speaker: mmhhmm- that their home device becomes fully discoverable.

Speaker & Bill:

Good point.

Bill:

That's a great point.

Speaker:

Yeah but how, *chuckles*, that's right their device would become, that's when the problem would arise or if a -Speaker: right- or I don't know legally if they can go out to everybody's home device that was you know an employee during a certain time period, but that would be a nightmare. You wanna make sure you can say hey we haven't enforced this policy, that it's, that they're not capable of doing that, that's the way I'm looking at it. I guess an appropriate MDM is what I'm saying. I don't know how else I can do it.

Speaker:

Yeah it's interesting our legal team takes a bit of different approach to they that uh, because I'm with you, if I get called to the stand and they say to me ok well this is what your written policy is, it says that your employees are required to make sure that they're required to do this on an annual basis, what are you guys doing to check and ensure that they're actually doing that from an IT perspective. I'm gonna have to stand up there and say that I really rely on our individual employees to certify that have followed the general counsel's directive to remove all records associated with this particular retention policy.

Speaker:

Yeah, Yeah.

Speaker:

And according to our legal department that's all we need to do.

Speaker:

Yeah that's, I've seen that yep, *laughter* It's crazy but, it might not even be a legal thing it might be an operational thing where somebody leaves now you know you lock them out they don't have access to their email, they don’t have access to contacts and calendars, but if they're just restoring it from a file device then they still have it, you don’t have any control over it, so they taken all that intellectual property with them and you've terminated them so it doesn't matter, you gotta look at it that way too.

Speaker:

Yeah I guess I’m looking at it from a perspective of you know even if they do restore it from the cloud, my assumption is, is that the device they used to connect had to go through active sync and active sync would require a password to be able to get into that, so once we've gone through and disabled their account on AD getting through owa to access that email, it wouldn’t be possible because the password wouldn't work. That's just my assumption I haven't tested that theory.

Bill:

So that's a really good point though, so a noncut, this is, wow what a gnarly topic. What do you seeing legal counsels kicking back in regards to going back and discovering email on other devices that are either employee owned or company owned and the has that come up in any situations either with someone who has left the company or someone who is currently employed?

Speaker:

It well, this is Speaker again, it has come up here where HR has told us that a terminated employee has said for some reason or another oh well I can just restore even though you locked me out, I can just restore and I'll see it still. They volunteered that information, that's what created the ground swell. I've got my helpdesk looking at that now. It's looking like they can restore it and still see it. They can't do anything with it, because you know they're not connected anymore, but they can still see it and cut and paste and whatever else is what I'm hearing.

Bill:

Ok let's hit an easy one, USBs, what are people doing with policy around connecting flash drives to company devices via policy or enforcement. *pause* Speaker you're unusually quiet.

Speaker:

Well we, we have to allow it. I mean it's part of how we do business, so other than putting some policy together you know guiding what they should download and what they shouldn't, I don't know.

Speaker:

This is speaker, we allow it, we're not restricting it technologically. We do disable the auto run feature so it doesn't automatically run in case there's something destructive on it, we also do an initial scan of the device first before it's allowed to connect, but other than that we don't restrict it.

Speaker:

This is Speaker with Nettrition; the last policy was ours as well. You request the need for it and it's approved, and the same procedures, disable auto run and so forth.

Speaker:

Speaker with the American Chemistry Council, we don't really have any specific policy on it other than a few communications that have come out in the past with respect to you know how to remove, a couple of years ago when people were ensuring they had the files that they needed or if we were taking the system down for maintenance. What we've done from an IT perspective is we've said if you need a USB type device call the IT helpdesk and we will help procure one for you and what we do when we procure that is we will procure one of the ones that has security associated with it so when you stick it in you have to actually put in a password. I guess that doesn't address the fact that people could download everything within our network on these things, because they're getting that large nowadays, and mobile, but it does address the haphazard way in which people tend to leave them leaving on tables or whatever the case may be, and lose them.

Speaker:

This is Speaker, yeah it's a big whole for us too and I think it's exasperated because they're so cheap. You know with a mobile phone you have to at least spend some money to have it month to month, but this thing you could have ten of them and not think twice about losing it and leaving it and everything else.

Bill:

In regards to, I know a couple of folks on the phone have started to explore this and have some enforcement in place, on the data loss side of this that they can actually see data typed going down to that USB. So Yes they go through the IT department for a specific device that is encrypted, that maybe has a pin, so that if it does get lost it is encrypted and has a pin, but then they can actually see the device type the data going into the different authorized devices that have been issued through IT. Does anybody have any data loss enforcement tools in place or are considering?

Speaker:

This is Speaker. Bill, like you know we were considering it but we've probably moved the MDM above it. Seems like it's sort of taken precedent at this point. Both are gaping holes at this point.

Bill:

Is anybody looking at handling data loss if not from a technology perspective just from a policy? As far as data types that are allowed on to, is legal coming back and saying you're allowed to put certain data types onto a USB? I know Speaker you had mentioned you can't use your mobile devices as storage, what about USBs?

Speaker:

I think from the same perspective, the USBs are used for convenience whenever you don't have access to the internet. Again we put everything in our internal cloud so that, and I apologize for using

that word, our internal network accessible from the internet, so that individual employees don't necessarily have to have the mobile device, or I shouldn't say mobile device but USB, when traveling in an area where if they were to connect to the internet it would cost $12 a minute, that type of thing. They know they're going there ahead of time or they're going to a conference where they have to do a presentation. For us it's really a temporary thing. Our mobile device policy, including the USB piece, points back to the record retention policy saying this is our sole repository for corporate records.

Bill:

Ok. Thanks for that clarification. Does anybody want to speak to remote wipe and policy? I hear a lot of MDM vendors being mentioned, and active sync was being mentioned, is anybody looking to have a more flexible remote wipe or very specific ability to wipe as part of their policies?

Speaker: For us at the American Chemistry Council once we get our MDM solution in if an individual were to as an example, put in their password 5 times in a row their device is wiped. If they lose their device, part of what we want to be able to with mobile device management solution is be able to lock the device, track device, remote wipe, separate out the corporate information from the personal information, those types of things. I guess with mobile device management solutions or the good ones at least, those are pretty standard features.

Speaker:

I put a ditto on that this is speaker.

Bill:

Ok great. I think, is it fair to say that with the policies that you're looking to, so you're absorbing some flexibility in the ability to have company owned and employee owned devices that are fully managed on MDM. Is that philosophically where people are heading?

Speaker:

Certainly is from my perspective here at the American Chemistry council. One of the things I will bring up though is you know we talked about mobile device wipe, or remote wipe I should say, and I was just thinking about what happens if we've wiped the device and all of a sudden our end user comes back and says oh I found it, it was actually in the back of my briefcase, so now I want you to put all my pictures back on it, you know all my personal phone numbers and things like that. That gets back into the backup side of things. Where I think we talked about before, should we encourage people to backup into the cloud or not. I mean I think from my perspective I certainly would encourage people to backup to the cloud.

Bill:

Does anybody have like a forced mechanism where they're pushing data from mobile devices they're issuing to secure vault in the cloud. Where it's just a company owned vault where they drip backup the devices just to address that situation Speaker talked about?

Speaker:

No we're not.

Speaker:

It's one thing I haven't explored yet but, I was thinking about being in common, well I don't know if its common or not but I know its common here at the ACC, being a repeatable type of sense so to speak with the mobile device, I lost it, let's wipe it for security purposes, oh i found it now. I'm wondering if mobile device management solutions, and I haven't really delved into that side of it very far yet, even to have that capability to back up a specific device. And if that being the case would that back up remain separate from the cloud, would it remain, or I should say would it remain separate from your network at the solution provider's hosted location or would you put that back up on your internal network, and then discovery becomes part of that, and legal record retention because as folks have eluded we've backed up the email and things like that. It's a never ending circle I think.

Speaker:

Yeah I have the same question. I'm kind of hoping that MDM is the panacea, but I'm doubting it.

Bill:

I guess even without MDM though if someone even today if the data is lost to them on a mobile, on a laptop, I guess I'm making a distinction between something that's a consumption device and something they're actually creating documents on, if the device is lost is anybody here concerned about the intellectual property on that device if it's just lost?

Speaker:

Well we, I mean if its mobile we can remote wipe it right, they'd just lose everything, but they already understand that when they sign up for it. So if they bring in a personal device we make them sign a form. You know it's not the best solution but it's what we have right now until we can implement some kind of MDM.

Speaker:

You know it's interesting that you mention that because I've thought through that as well. I'm thinking to myself ok well is anyone smart enough to get or take a mobile device with the intention of trying to get information from it. They're gonna be smart enough to know I'm not putting this thing back on the network or the internet before I try and get this information off. It really revokes the remote

wipe piece unless you have it associated with either starting up on a bootable disk not related to the network, that type of thing, or the device totally encrypted, the number of password failures that would remotely wipe the device, those types of things. We used to put the security, oh not the security but the tracking devices on our laptops and if our end users have basically walked away from laptops or forgotten them somewhere or had them stolen, we've never been able to recover a single one because people who are taking them are taking them wherever and they never put them back on the network until they've totally changed everything and basically made the tracking information useless.

Speaker:

But then you didn't lose any data either right? Did they wipe it out or

Speaker:

Well they don't necessarily have to. If you pop an operating disk, a Bluetooth disk into any remote, or I shouldn't say remote but, any laptop especially you can boot from that operating system and get right to the root drive.

Bill:

What about the encryption piece. What if the device is encrypted?

Speaker:

To me that would be you know part of the saving grace, absolutely yes.

Bill:

I'm wondering form a lowest common denominator just cuz it's a, sort of moving target out of this mobility and mobile devices and I wonder if there's no enforcement necessarily in place if we just need to address this from maybe policy, or policy enforcement at the lowest common denominator which might be just encrypting the darn thing. Maybe that's the advantage of some of the mobile device platforms. I haven't heard about them backing up but maybe what type of encryption is enforced on whatever container, can you encrypt on the corporate container and leave the personal stuff alone. Certainly on laptops, can we just make the darn thing irrelevant if it's found, just totally irrelevant. I think one way maybe the encryption part is just enforcing very simple encryption technology. Is anybody using any encryption just for the sake of the group knowledge, is anybody using any clever encryption technology with any known manufacturers?

Speaker:

Uh we're using Sophos for encryption on laptops that are DNS cause they don't want to lose any data, but we've had some issues with them so I wouldn't suggest that. I guess at this point now when you buy a laptop you buy an encrypted hard disk and you're done. The problem is managing it all. With Sophos they gave us a management console to mange it.

Bill:

Yeah with Mcafee that's the same thing as well.

Speaker:

At the ACC we use bit locker here. what we've found is, we only do this when absolutely necessary if our folks are traveling to China is an example we will encrypt their hard drive, what we've found though is two things number one it certainly increases, I shouldn't say increases, actually it does it increases the response time of the machine makes it slower, the second thing is god forbid if the individual working on the device ever puts anything on their flash drive and now they've forgotten their password or anything associated with that it becomes a bit of a challenge.

Bill:

A challenge to recover right?

Speaker:

Well it's a challenge to walk them through. Most of these, at least that I've investigated, these encryption programs they do have a hash key or some type of key that will actually make them work, and if you lose that key you are S.O.L. Unless you know some of the folks using Sophos or Mcafee may have found something different or a magic feather out there.

Bill:

I think it's similar with the cloud backups as well. They give you the key to the vault of the backup so if IT loses that it's a bit of a challenge as well. Certainly two interesting options, backing up the data to the cloud so at least we have the data. Certainly we might not have the device but at least we have the data. The other piece being just making the device irrelevant. I guess part of this is trying to think what's the simplest simplest statements from our policies that achieve the most mileage whether or not we can enforce them or not but certainly if we can enforce them it's nice, and it seems like we had two ones there that could be enforced. Speaker I thought had the most clever piece with kind of a statement on data just going on SharePoint. From a policy perspective that seems to be pretty darn clear especially if there's some training and education around that.

Speaker:

I thought, I forget who the gentleman was but early in the discussion somebody mentioned about a device being connected to your network regardless of if it's personal is treated as a corporate device, I thought that was a very good statement because then it ties right into whatever your corporate policies are.

Speaker:

Yeah that was me again but I don't know that our legal folks actually like that.

Speaker:

Oh wow, I thought that was really nice I was gonna go talk to my legal about that one. *chuckles*

Speaker:

I'm sorry I kinda delayed in response there; I was trying to find my rough draft of my policy here so that I could bring it up and share the actual information. I've got windows 8 on my computer here and I'm still playing a little bit with it. Let me give you the exact wording that I used for both of those statements. The interesting challenge is this, and this has come down from my leadership, senior leadership, and that is, is that the policy that we have is supposed to be an enabler. So what the intent of this thing is is to enable our coworkers to be able to perform advocacy activities more effectively and efficiently while mobile. That's the whole intent so put restrictions on it, to make it more difficult, things like that my senior leadership is not gonna go for that. My CFO he says, we wanna strip the administration out of this so if we're going to allow people to connect their own devices and we're going to require them to have a device but we are not going to provide them with a device then we have to somehow be able to give them a refund or a reimbursement associated with their own personal plan, but we don't want them to have to submit an expense report every month for it. So now we started to involve tax law and all those lovely uh, so we're still working through that piece of it trying to figure out because we have received a couple of remote policies from other associations, my CIO network is very good and my CFO's network is very good we've had a number of people share with us and we're trying to craft it from everything.

Bill:

I would just add on that Speaker, the PCI piece which I would put kind of on the spectrum of 0 to 10, if we had to look at this from a continuum of 10 is the most stringent security, I think though that if there's going to be an unfettered open approach and totally enable the user the downside being that folks like Speaker from Nettrition and some of the other folks on this call that we have to segment those systems and some of those access rights around some of those systems that are really intense from a policy and security point of view. I guess that's what makes the job such a challenge. Anybody have any parting comments, it's 9:59 and we have one minute left, oh actually it just turned to 10, did anybody have a final comment as we wrap up?

Speaker:

One thing that was put in every single one of your policies, this was one I stuck in mine, the ACC employees are strictly prohibited using a company issued mobile device while operating a motor vehicle. Believe it or not I was at a conference where coco-cola down in Texas somewhere did not have that in their policy and one of their drivers got into an accident and I believe injured himself to the point where he couldn't come back to work. They subsequently said that he did not follow the policy because he was working, well it was never in the policy and he won.

Speaker:

Huh.

Speaker:

I know it makes absolutely no sense but-

Bill:

And Speaker, what was the one you mentioned that Speaker liked, not the specifics but the general intent of that policy that your senior executives probably won't allow, what was the general intent of that?

Speaker:

It was the mobile device if it's connected to network it has to be treated as a corporate device. That way if they're skirting around, like if somebody's in, like right now we have all these filters right for web surfing and it runs through everything, but then somebody comes in with their 4G, LG, LTE and you know surfs a bad site and somebody sees it over the shoulder that we're not responsible. Kind of like when you said worry about somebody's lookin at something and it's you know sexual nature and its abusive to an admin or something on the corporate computer well now they can't do it, I mean we've got something enforced, but to come with a mobile on the 3G, it's uh, I think that sort of allows like at least we can have a policy in effect to say hey we're treating this a corporate and corporate has certain rules.

Speaker:

Yeah the way it reads in my policy is personal owned electronic devices are your property. However, once connected to the ACC network they must be treated, used and safeguarded as an ACC owned device. That's kind of the way that I stated it.

Speaker:

Hmm I like that.

Bill:

Yeah that's nice, that's good language.

Speaker:

Speaker from Nettrition, we're just, we're small enough that our policy simply states that if anybody wants to use work related stuff outside of the office or at home we simply provide the device. Which is mostly laptops, but from financial issues we're small enough that that's not a problem.

Bill: Well I appreciate -*speaker coughs*- oh go ahead final comment?

Speaker:

Speaker again, yeah I'm sorry I got a bunch of final comments, but this'll be my last one I promise. With the rollout of Windows 8 on the surfaces, I've had Windows 8 on my asis slate here for probably 6 or 8 months and I mean I just love it, but with the Surface coming out I'm looking at replacing laptops here at our organization with the Surfaces. So again windows mobile mobile device or mobile device management is gonna be a real up and coming thing here within our organization.

Bill:

So you're trying to say Windows Surface rules!!

Speaker:

I'm, what I'm, I like windows 8

Bill:

chuckles

Speaker:

Windows Surface RT you know I don't even have one of those. I do have the full blown windows 8 package on my asis slate and it's, I really enjoy it, but it's different.

Bill:

I've seen it, it is quite nice. My CTO has it and likes it a lot. Well everybody thank you so much I hope everybody got a lot out of this I know I certainly did. I'm gonna go stop this recording and provide this back to everybody as a soft copy for everybody to have it for their records. So i hope this met everybody's expectations.

Speakers:

Thanks Bill.

Bill:

Ok have a great day everybody.

Speakers:

Ok Bye.