RunAs Radio

http://www.runasradio.com

RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.

Text Transcript of Show #157
(Transcription services provided by PWOP Productions)

Robert Hamilton Prevents Data Loss!
April 21, 2010

[Music]

Brandon Wenn: From runasradio.com, you're listening to RunAs Radio, the Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Brandon Wenn, announcing show #157, with guest Robert Hamilton, recorded Friday, April 9, 2010. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at pwop.com. You can follow the boys on Twitter at twitter.com/runasradio.

Richard Campbell: Thank you, Brandon. This is Richard Campbell and with me as always, my co-host, Greg Hughes.

Greg Hughes: Hey Richard, how are you today?

Richard Campbell: I am well, sir, and odds are I'm in the midst of the .NET Rocks! road trip when the show gets published so I will be somewhere in the United States in an RV.

Greg Hughes: That's a relatively small geographical area so I'm sure we can find you.

Richard Campbell: Oh, yeah. Well, for anybody who is a .NET Rocks! fan or have no idea what we're talking about, go over to the .NET Rocks! site under the link road trip. Carl and I are driving across the country doing 15 cities in three weeks.

Greg Hughes: Cool.

Richard Campbell: Talking about the Studio launch and all of that madness.

Greg Hughes: So what's the route? Where do you start and where do you finish, and what are some of the highlights there?

Richard Campbell: We're doing 15 cities so we we're doing West Coast, then Midwest, then East Coast and on the weekends we move the RV between the regions so I think at one point we drive from Phoenix to Houston, which is, I've done it before the other way, it's a really long way. There's a whole lot of nothing in western Texas.

Greg Hughes: Yeah. I-40, right?

Richard Campbell: Oh yeah and it just goes and goes and goes, but we get to meet a lot of folks. It's a gas, the fun things to do.

Greg Hughes: You know what? I didn't ask you before, are you driving through Portland?

Richard Campbell: We're not going to Portland, my friend, again.

Greg Hughes: Oh, well.

Richard Campbell: I have promised to do the Portland code camp next time around. Carl and I will come out for that, and it's just distances get too far when you get up in the northwest corner. We also miss Denver which is another great place that I wish we could get up to.

Greg Hughes: Yeah, yeah. Well, good. Have a great time.

Richard Campbell: Ah, it will be. I'm sure there will be stories when we get back out the other side. I'll be happy to be home for a while. All right, Greg, let's introduce our guest. Robert Hamilton is a senior product marketing manager for Data Loss Prevention at Symantec. Robert 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. Prior to Symantec, Hamilton served as senior product manager for RSA Security. Hamilton has held a variety of product management, product marketing, and corporate marketing roles at Postini, Mirapoint, NetApp and Hewlett-Packard. Welcome, Robert.

Greg Hughes: Hey, Robert.

Robert Hamilton: Good morning, Richard. Good morning, Greg.

Richard Campbell: So Data Loss Prevention. Boy, that's a broad topic.

Robert Hamilton: It sure is.

Greg Hughes: Something I've certainly learned a lot about last year.

Richard Campbell: So are we mainly talking about protecting credit card numbers here? Is that what this is all about?

Robert Hamilton: Let me just tell you. To start off with, a lot of people talk around the term Data Loss Prevention and sometimes they're talking about encryption, sometimes they're talking about port control. But when we talk about data loss prevention, what we're talking about isn't a specific application that's called Data Loss Prevention. It certainly is about protecting credit data; that is certainly one of the major reasons people buy Data Loss Prevention. But increasingly it's about protecting people, customers, private information, protecting health information, protecting intellectual properties like product designs. So there are a number of different

types of data that people are looking to protect, basically what they call high business impact data.

Richard Campbell: Okay.

Greg Hughes: So before we jumped into -- let's take the direction of define the need before we jump into technology. You know, we don't want to have technology looking for a problem to solve. We have problems that exist. What are they, and what are some of the common reasons that people consider data loss or data leakage, or whatever we're calling it now, prevention, the DLP product or that type of technology?

Robert Hamilton: There are a couple of drivers and it's not onerous or not everybody is affected by it, but there are many industries that have regulations that are pretty prescriptive in terms of protecting certain private information. Certainly the credit card companies compel anybody that processes credit card transactions to protect those numbers, but there are a lot of people that thinks seriously about data loss prevention because they want to keep their names off the front page of the Wall Street Journal.

Richard Campbell: Right.

Robert Hamilton: They need to protect their brand equity and they don't just want to be caught in that position of having to disclose that data got out of the organization that they didn't want.

Greg Hughes: Sure. When you're thinking about sensitive data that are high level, you've mentioned some examples of that, but what makes data sensitive? What is it that we have to think about when we start to deal with data and what is DLP in relation to sensitive data?

Robert Hamilton: That's one of the things that organizations have to get a handle on, what constitutes their sensitive data, their highly impact data. The type of data that could cause a financial lost if it were to be disclosed either because a product design gets leaked out to a competitor from an ex employee, it could be a fine or the inability to process credit card transactions that get slapped on by one of the credit card issuers, it could be not passing a PCI audit, or a bank not passing a GLBA audit. There's a number of things that could drive the impact of lost data.

Greg Hughes: Is it just banking data we're talking about or is there other types of data that you can also protect against the leakage or the loss of?

Robert Hamilton: Well, certainly banking data because typically that involves a lot of accounts, credit card.

Greg Hughes: Right.

Robert Hamilton: The types of information where an identity, when you have name, address, Social Security Number, other identifying things that constitute what we call personally identifiable information or someone's identity can be stolen. But it also involves intellectual properties, it involves protected health information that's described under the HIPAA law. So it really runs the gamut in terms of what constitutes confidential information, but again it's up to each individual organization to decide what is the high business impact data that matters to them.

Richard Campbell: Yeah, and I'm always falling back to credit cards because that's the thing that I've dealt with in the past myself, but I guess as soon as you're talking about a customer's name, address, telephone number, all of that is effectively sensitive data. Right?

Robert Hamilton: Oh, absolutely. I think there's virtually all of the states now. It was initially led by the state of California when we enacted the SB 1386 that prescribes protecting private data like that and tells organizations that they have to disclose when there has been a potential data leak. There are a number of people I know and probably a lot of listeners have at one point in the last few years received a letter from one of the companies that they've done business with explaining that their account data may have been somehow compromised and they offer a year's worth of credit monitoring service. I know I received a couple of those.

Greg Hughes: Yeah, I have as well. It's a bit of a disconcerting letter to get, isn't it?

Richard Campbell: Well, chilling because there's nothing for you to do per se. But you're right, in terms of brand damage, I mean what a nasty thing to receive. You can't help but think badly of whatever company sent you that letter.

Robert Hamilton: That's true. It is a little chilling, but a lot of companies I found are just very conservative when it comes to that. In fact, one of the cases where I received a letter was apparently one of my credit card companies explained that a tape, like a system backup tape that had account information on it, was somehow inadvertently lost and based on the law that they're operating under that state they're compelled to inform you that. Was it likely that my account information was compromised? Probably not.

Greg Hughes: Yeah. I mean, reporting and all the laws around reporting, well, there's a new Massachusetts law now and there's a lot more coming, a lot of requirements on business these days when it comes to how to communicate, when to communicate, or why to communicate about even like you say just potential lost of data.

Robert Hamilton: That's right. Certainly there are a lot of other reasons that people are interested in protecting data. It's not even covered by the disclosures laws particularly intellectual property. People have become very sensitive to concerns about losing product designs, oil companies that have seismic data that's considered intellectual property, tech companies that have source code that needs to be protected. With the mobility of workers in the US these days, there's a big concern that employees are taking data with them when they leave their jobs and in particular when they go to competitors. So they're thinking about that sort of thing as well.

Greg Hughes: Yeah. I mean if I'm a, I don't know, to take one of your examples, if I'm a software engineer and I am not happy or even if I get fired for example and I have a couple of seconds to stick in a USB key or burn a CD or DVD with a bunch of source code on it, it's not that hard for me to walk out the door I guess, is it really, with that information.

Robert Hamilton: It isn't, but let me tell you what some of the tricks that the DLP can do these days. Our product working with another Symantec product that we call Workflow can set a series of actions in place when that engineer puts a USB drive into his computer and starts to download a source code. Our software that's running on his PC is identifying that he is downloading source code. The Data Loss Prevention application knows that that's a prohibitive application so what happens is the DLP application talks to another application that can lock the user's ability to leave the building, deactivates his card key in other words until he goes to talk to the security department. Security department can see that he has done something that is probably not within reason and can stop the data loss before it occurs. That's a real application that works today.

Greg Hughes: So taking DLP and using it to trigger some other activity outside of a DLP type of product is what you're saying.

Robert Hamilton: Exactly.

Richard Campbell: But what I find interesting about this is the idea that the guy can still copy stuff onto his USB key. Hey, baby, he's doing it for a legitimate reason. It's not stopping him from doing that, it's just making sure everybody knows that there's a notification process and maybe he has to step through the next hoop and say, "Well, here's a request from my boss to make a copy of this and take it out of here," so that he can still proceed. I find that fascinating, this idea that I'm coming from the group policy, I can certainly stop anybody from putting anything on a USB key, to let him do it....

Greg Hughes: There might be legitimate reasons to do it, yeah.

Richard Campbell: Exactly. Let the legitimate reasons still function.

Robert Hamilton: You know, that's the way most people use Data Loss Prevention. Certainly we talk about DLPs capability to stop the ability of data to leave an organization, but the reality is many, many customers choose to use the product in a monitor mode so that they simply understand where the information is going, who's sending it out, how the information is being used, and they don't want DLP to stand in the way of user's productivity or to get users confused or unable to do their jobs.

Richard Campbell: Well, and you don't want to run in sort of a police-state mode either where everything is constantly locked and you have to ask permission to do what would be a fairly normal thing in a home-based machine.

Robert Hamilton: That's right. In typical fashion, they will monitor how data is flowing here and there but only when it comes to super, super sensitive information like maybe a list of credit cards or a list of employee names and account numbers where they actually have the system put lbocking in place.

Richard Campbell: But you can't stop it before it starts. Can you stop it while it's happening?

Robert Hamilton: Oh, absolutely. Here's a typical example. An employee downloads a list of name and addresses and attach it to a Gmail email that they're sending to their home account and when the user hits the send button our software kicks in and actually reads the content of that attachment and says "This falls outside of acceptable use policy," and will actually keep the email from leaving the company's network.

Greg Hughes: Uh-hmm.

Richard Campbell: But I do like the fact that he's done the crime, so to speak. He has attempted to send an email, and if the DLP software hadn't blocked it; it would have sent.

Robert Hamilton: Right.

Richard Campbell: So there's clear evidence of malfeasance here. He has done something that's outside of what his employee contract said he is allowed to do.

Robert Hamilton: Right.

Greg Hughes: I think it's probably worth pointing out to everybody that if somebody is bound and determine to steal something internally that there's always a way to do that, take a picture of a screen, get out a pencil or pen and paper and write

something down and have a photographic memory and remember what you saw and there's always a way to do it, but the idea here is to make more difficult. But isn't another point of DLP also just to prevent the accidental and inadvertent misuse of data?

Robert Hamilton: I agree. That's a good point that you bring up. In fact, typical studies tell us that around 90% of the data loss incidence occurs because well-intentioned employees are simply trying to do their job. You know, they want to send something home to work on it at home in the evening. They want to put something on a USB drive, the USB drive gets lost. Those are the typical sort of incidence that the Data Loss Prevention products are really designed to solve, educate employees on acceptable used policies and actually what we call stopping stupid.

Greg Hughes: Right.

Richard Campbell: Yeah. You accidentally mailed the entire customer's list to somebody you shouldn't have.

Robert Hamilton: Exactly. Or an HR manager who puts the employee roster on an unprotected file share.

Richard Campbell: Right.

Robert Hamilton: That's the sort of typical thing that we're trying to prevent.

Greg Hughes: So we've talked about a lot of different, I mean sort of alluded to even just indirectly, a lot of different places that data can show up. Maybe we should step back and think about DLP technology. Can you explain what makes DLP technology a DLP?

Robert Hamilton: Sure. Actually the core of Data Loss Prevention is what we call content awareness, it's that we're not just looking at what a file type or the name of a file. We actually as data is being sent over the network or being copied to a USB drive or being put on an email as an attachment, at the point in which that action takes place some component of the DLP product actually opens up that file and reads the content and then makes a determination whether or not the contents of that file match a particular DLP policy. A policy is defined in the system as I want you to find credit card data, I want you to find resumes, I want you to find product design, CAD drawings, certain press releases. So what we're doing is what we call Deep Content Inspection. So every file gets opened up, every file gets looked at and a determination is made whether or not that file constitutes confidential information and that really is the core of how DLP works.

Greg Hughes: So I might have stuff that's sitting, we've talked about emailing things for example or putting things on a file share. You know, I mean organizations that I've worked with and worked in, there are file servers out there that contain just terabytes and terabytes of information. I mean, it's a huge amount of information. It might sit there for quite a while.

Robert Hamilton: For years, and people are really reluctant to get rid of it. That's one of the values of Data Loss Prevention as well, it's going out and being able to scan these terabytes and terabytes of file system data and identify data that really shouldn't be there and once that's done measures can be taken to either get rid of it or move it to protected file shares. We even have products that let people identify who owns the file, not through the metadata within the file itself but by who's been accessing and who's been using the data that we can attribute ownership of a file out on a file share by usage.

Greg Hughes: So when we think about whether it's Symantec's product or one of the other what I may think as major vendors out there, you know you hear people throwing around terms like data at rest and data in motion and data in use. Can you explain what those things are and kind of how those problems are solved in the marketplace?

Robert Hamilton: Sure. Those are the common terms that people have started to use to help describe the types of data that DLP can protect. So let me take them one by one. First is data in use, and by that we mean files that are actually going somewhere. They're going -- I think data in motion is files that are going somewhere, they're going on an email message. They're being copied to a DVD or a USB drive. They're being sent from one person to another, or being copied from one device to another. That's data in motion. Data at rest is files that are stored on file systems that, like we've just talked about a minute ago, files that are being stored and may or may not be accessing actively. Data in use is files that are actually being manipulated by users. So I have a spreadsheet of confidential information that's open or confidential let's say Microsoft Word document that I'm using and then I want to do something with it, maybe store it somewhere, copy it to a USB drive, attach it to an email. So data in use, information that's being used, data in motion, data that's flowing out over the network, and data at rest which is stored data.

Richard Campbell: If data is at rest -- I mean as soon as somebody tries to copy anything, it's effectively data in use. You've got blocks in place, it looks the same as somebody is editing the file.

Robert Hamilton: That's true, and Data Loss Prevention isn't designed to prevent people from using data.

Richard Campbell: Right.

Robert Hamilton: Certainly if I'm on an organization, I can open up a confidential file and manipulate it. Data Loss Prevention comes into play when I want to do something with it that may be an activity that could cause it to leak out of the organization.

Richard Campbell: Right.

Robert Hamilton: Also data at rest, the key use for Data Loss Prevention is actually define all of that amongst all the terabytes and terabytes of stored data. You want to find all of your confidential data at rest.

Greg Hughes: So if I'm scanning my file servers, that's a data at rest search I guess you would say.

Robert Hamilton: Exactly, right.

Greg Hughes: If I go out to a file server as a user and open a file or if I copy the file to my workstation, that's data in motion?

Robert Hamilton: Exactly.

Robert Hamilton: If I open the file and maybe start copying part of the Word document out and pasting it into another Word document, that's data in use.

Robert Hamilton: That's right.

Greg Hughes: Okay. So when people implement these systems, I mean do they really work very well and how do they do it? It sounds to me like you have the potential here to, you know, I think about things in terms of like business logic or business processes. The people need to be able to get their jobs done but if we're going to be doing preventing data loss, how do we do that in a way that doesn't kill, as you've mentioned you alluded to earlier, it doesn't sort of kill my ability to do my job.

Robert Hamilton: Right, and it can seem like potentially a daunting process but what's nice about Data Loss Prevention as a program is that you can take it and say that typically it's how it goes. People get the Data Loss Prevention product and they start assessing their areas of risk, okay. They start monitoring. They start monitoring email, they might start monitoring people's use of data at the endpoint, and they start understanding which departments are at greatest risk and then embark on an employee's education. So nothing more than a user's awareness through educational programs is developed because now they have visibility. So DLP initially helps you gain visibility. The next step really is to start implementing user notifications, that is you don't really block or you don't stop people from doing things. But when people send an email with confidential data in it, Data Loss Prevention product can kick back a message from the information security department telling people that, well, you may want to reconsider whether or not you should be doing this. That step alone leads to a massive reduction in risk. In fact, we see customers that implement end-user notifications and they see what we say about 80% to 90% risk reduction in a matter of weeks, and what we mean by that is if they have a thousand potential data loss incidence before they implemented user notification, that's gone down to maybe a hundred. Once you users understand what the policies are, they start rethinking how they're using confidential data. Finally for really, really critical data, some customers use Data Loss Prevention to actually, as we've talked about earlier, implement blocking. So you take it in phases. It's not hard to implement, but it's a security program that is enabled through this technology.

Greg Hughes: One of the things I'm picking up on here is there's an opportunity to use the DLP technology to educate people. I think about security in IT and how so often we have to say "no," or that's wrong, this is wrong. It sounds like maybe there's the opportunity to use the technology not to tell them necessarily so much you're doing something wrong, but maybe to tell them here's what you need to do that would be right. Is that something we can do?

Robert Hamilton: Exactly and that's how most customers used Data Loss Prevention. So here's an example. Someone sends their tax return to their wife over the company's email system. Data Loss Prevention will kick back a nice email to that employee telling him that you might want to reconsider sending your Social Security Number in the clear over an email system. You know, it protects sensitive data. That's just an education process that happens when an event like that occurs and that really is the key when you think about the key to reducing risk, because like I said earlier most data loss issues are cause by well-intentioned people just trying to do their job.

Richard Campbell: And just not realizing that they've done something hazardous like that, like sending a SIM number over -- or a Social Security Number, sorry, I'm a Canadian -- over a clear text email.

Robert Hamilton: Exactly.

Greg Hughes: You don't have to apologize for being a Canadian, Richard. It's okay. No apologies...

Richard Campbell: We have a slightly different words for these things.

Greg Hughes: That's right.

Robert Hamilton: Well, DLP recognizes those numbers as well.

Richard Campbell: What I think is interesting here is that the kind of mistakes you would make like leaving an Excel Spreadsheet where the second sheet has a bunch of customer information and you didn't even look at that, you're working on the first sheet.

Greg Hughes: Right.

Richard Campbell: DLP is going to pick that up when you email that.

Robert Hamilton: That's right.

Greg Hughes: Or the email thread that's like two miles down has a whole bunch of sensitive information that you wouldn't want to afford out but because you don't scroll down to read it all you might be sending it out to somebody outside the company that you work at. That might be a problem.

Richard Campbell: What a great example. Because you have this email going back and forth internally, back and forth internally and it's got sensitive data in it way down in the stack and then somebody forwards it out of the company.

Greg Hughes: Yeah, or you know, you use the Outlook auto-complete. I had this happen to me not too long ago. You start typing somebody's email address. Outlook completes it for you. You hit enter, and it's kind of like we said a few shows ago with Clippy, it tries to figure out what you wanted to do but it's really if you don't pay close attention it may not really be doing what you want it to do. You know, sending something outside instead of internally because you happen to just not pay close enough attention because you were in a hurry, again I guess you're just trying to get your job done and just an inadvertent mistake that the person makes.

Robert Hamilton: There you go, a perfect example.

Richard Campbell: Yeah. You know that when you're writing an email, the second most likely person for you to send that email to besides the person you intended to is the one you didn't want to send it to.

Greg Hughes: Exactly I think, yes.

Richard Campbell: So what I love about this is this idea that the meal goes out and you may or may not realize it and then some time later you get notified. How does that look, Robert, when an email gets intercepted by the DLP software in the backend? Is it just send the mail back saying you may not want to send this? I guess part of this is deciding do I still send it but send back a warning, or do I stop it from sending and say you shouldn't be doing it this way?

Robert Hamilton: You can have it work both ways. You can tell people after -- you know, don't stand in the way of letting them send email but let them know that the email that they sent may have confidential data in it and that notification happens immediately, or you could actually block the email and then have the user make a determination whether or not they really want that email to go out. There are a number of different levels of security that you can implement when it comes to blocking and notification.

Greg Hughes: Okay. So what if I need to send sensitive data to somebody, maybe like some other company that's a partner of mine and it is sensitive data and I need to send it to them and they have to receive it via email? I mean email, just plain old email is just not a very good thing. So sometimes companies will say, well, you have to zip it with a version of a Zip program, that will do 256-bit encryption, etc, etc, make sure you do that and send it out. But in the "I'm in a hurry trying to get my job done" thing, maybe I just sort of skip over that part or forgot to do it. I attached the document, or maybe like Richard says in Excel Spreadsheet and the second sheet in the workbook or what-have-you maybe does have sensitive data but I didn't realize it. Is there something that DLP can do to get the data to the people that need to get it outside the company but still protect it?

Robert Hamilton: Well, certainly you want to implement levels of encryption through your email system just as a best practice but the DLP, when I talk early on about policy, defining what is sensitive data, also a part of policy is where is the data coming from, who is it going to. You can always, by policy, make exceptions that say "If this file is going to one of these trusted partners, let it go through."

Greg Hughes: Got you.

Robert Hamilton: Or if this data is being copied to a USB by this group of trusted individuals, let them do it. So you can create those exceptions within the DLP policies as well.

Richard Campbell: Is it possible to be explicit, for example, to actually mark an email as this cannot be sent outside of the company?

Robert Hamilton: Well, that capability is -- certainly DLP can inspect the email and make a determination whether or not that email should or should not be sent outside of the company and it can be tagged on the email via what we commonly call X headers.

Richard Campbell: Right.

Robert Hamilton: And then some other device downstream of the mail server can read that X header and do something with it like encrypt it or put it in a queue for inspection by a security officer. So DLP can -- the value that the DLP adds is again we open up the email, we read the body, we read the contents of the attachment, and then we can stamp it with some sort of confidential flag or whatever the user determines as appropriate based on that content.

Greg Hughes: Okay. So then my message workflow could hit after being stamped. You could stamp it for example that says encrypt and then maybe I would have some other third party application that could encrypt the email before it goes out on the internet.

Robert Hamilton: Yeah. That's a pretty common usage particularly with healthcare. It's they do selective encryption based on the content. They rely on DLP to determine what the content is and then they rely on an encryption server after the DLP product has made a determination that the email needs to be encrypted. So yeah, that's a common application.

Greg Hughes: So ultimately DLP looks into the guts of some kind of any document or content or file or whatever it is, however you define the object, look inside of the content, analyze it, make some kind of evaluation which you can then use to -- what would the term be, to remediate the problem if there's a problem.

Robert Hamilton: Well, yeah. I think you've got it pretty much correct there. We net it out to calling it just Detection and Response. We look at what's inside the document or the email and then we do something about it, okay. We can look at a lot of different documents and interpret a lot of different content and we can do many different responses. So Detection and Response, that really is the core of what DLP is about.

Greg Hughes: Maybe before we finish up, just maybe a last thought. Obviously you can't state names but can you give a couple of examples of where a DLP technology being brought into some kind of organization has made a tangible difference?

Robert Hamilton: Oh, certainly. I think in almost every installation, DLP makes a big difference. A good example is an insurance company that was very concerned about the amount of personally identifiable information and account information that was flowing out to the email system, a lot of email correspondence with customers and what they did is again they did this notification implementation where the people that were sending email when they were enclosing or attaching confidential data to that email they were informed that they shouldn't be doing that. Two weeks after that, notification system was put in place. The number of potential data loss incidence decreased 90%, or like 88%, within a couple of weeks so a huge impact. Another example is an equipment manufacturer with concern about design documents flowing out their organization to personal Gmail account and they knew this because once they had put the Data Loss Prevention product in place in a monitoring mode, it was showing them that there were a lot of tab documents that were going out over the email system to Yahoo and Gmail accounts. So in that instance, they implemented blocking and they saw close to 95% reduction in the number of design documents that were leaving the organization.

Greg Hughes: What's the one thing that people need to know if they're thinking about doing a data loss prevention or a similar kind of project or initiative? What's the mistake that they need to make sure they don't make ahead of time?

Robert Hamilton: I think they need to make sure that the initiative for data loss prevention involves the business units that are going to be affected by it. It's not simply something that is brought in by the information security team, but there's a relatively broader task force that brings the business units into the formulation of policy and essentially the definition of the type of information that they want to protect and get input from those business units on the impact of potential data loss.

Richard Campbell: Robert Hamilton, thanks so much for coming on the show.

Robert Hamilton: Thank you.

Greg Hughes: Thanks, Robert.

Richard Campbell: And we'll talk to you next week on RunAs Radio.