



RUNAS RADIO



<http://www.runasradio.com>



Richard
Campbell

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.



Greg
Hughes

Text Transcript of Show #004
(Transcription services provided by [PWOP Productions](#))



Simon Goldstein on Compliance
May 2, 2007



[Music Playing]

Carl Franklin: From runasradio.com you're listening to RunAs Radio – The weekly Internet Audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Carl Franklin, introducing show #4, with guest Simon Goldstein, recorded April 20th, 2007. RunAs Radio is produced each week by Pwop Productions – Offering professional media and Podcasting services, online at pwop.com.

Richard Campbell: Hey, this is Richard Campbell, and you are listening to RunAs Radio, and with me always is Greg Hughes.

Greg Hughes: Hello, everybody, hello Richard.

Richard Campbell: Well, are you ready to go again?

Greg Hughes: I think I am.

Richard Campbell: It seems like we've got the show worked out now. The website is up, the email is finally working, info@runasradio.com is working and I got us an email.

Greg Hughes: Yeah, they've started to flow in.

Richard Campbell: There you go, so this is from Alan Osbourne and it says, "Hi Richard and Greg, congratulations on the launch of RunAs Radio. I checked out your first show with Patrick Hynds on storage management and enjoyed the discussion as it's right up my alley. I have set up and deployed SAN infrastructures for clients and I am looking to get into an entry level iSCSI SAN using 500 gigabytes SATA drives for my own VMware based Hosting Service. Amazing that you can get up to 7 terabytes in a 2U space for about \$30,000. Your inaugural show raised some interesting questions about storage management and the present and future challenges that an exponentially growing amount of data presents in terms of management and disaster recovery. In particular, the examination of how user data can balloon, when the lack of policies and quotas exist on a per user basis was instructive as was the discussion on strategies for locking things down. As a VMware guy, I would have liked to have heard a discussion about the parallels between server virtualization and the virtualization of storage, where at the server level, the OS and software is divorced from the hardware details. For example, you can carve out a LUN and then abstract that LUN as a local disk to the server regardless of whether you employ iSCSI or fiber channel on the back end. In a similar fashion by employing virtual machines, you divorce the OS and software from the

underlying hardware and by doing so, provide standardization and then more importantly, portability. In effect, you make it possible to run that virtual machine as an application on almost any host server hardware with no driver issues, etcetera. In fact, the really interesting space is where the two technologies merge. For instance, a fully redundant SAN likely with RAID, which you can carve up and abstract as LUNS through a farm of host ECX servers, perhaps physically implemented as a BladeCenter, and Virtual Machines could be hundreds. CDAZ, the local disk, as SCSI virtual drives, that are in actuality encapsulated as a bunch of files on the SAN. The beauty of this is that the ability to take real time snapshots of the virtual server's dates and the SAN's dates, as a back up and disaster recovery methodology in addition to traditional file based back up. With virtual machines, given the fact that they are encapsulated as a few files, you replicate these files stored on the SAN to another LUN, then replicate the snapshot to a remote site via WAN links with no downtime and no performance hit. Then in the case of disaster, you can restore the virtual disks for the virtual machines at the remote site, make some changes to your writing tables and bring virtual machines back up on completely different host hardware as if nothing ever happened. For file and database restores, you mount the previous snapshot as a virtual disk and restore the files. I love this sort of topic and looking forward with anticipation to your future shows. Cheers, Alan Osbourne."

Greg Hughes: Wow!

Richard Campbell: Long email.

Greg Hughes: You get SAN and NAS type guys around or you know the other ones are the firewall guys, and they get started talking and the words just flow. And you know what's really interesting about that email is where I work, our IT department has really relied heavily on two time and cost saving technologies. One of them is server virtualization and the other one is SAN and NAS, and has done a lot of work in terms of, where did those two meet and how do you really work that? It's really very interesting to hear a lot of common threads between what our IT department has done here and what's being talked about in that email.

(00:04:52)

Richard Campbell: Well, and hugely powerful thinking around upgrading or failing over to asymmetrical gear. That has so much potential, I could actually upgrade the site this way, by taking snapshots, move it to the these bigger systems and I don't care about the changes, that I get a



whole totally new drive array, isolated from everything else, but running in that virtual mode, so that I don't have to deal with performance issues around them.

Greg Hughes: That's right and just the not dealing with downtime, the concept of as little downtime as possible or no downtime. The LUN or the logical unit and being able to basically point your card, that it sitting inside of your server if you will, which virtually points at the SAN disk array that you tell it to, and will simply leverage that, and the idea of doing what he referred to is syncs and splits. So, I can synchronize two disk arrays with each other. I can split one off and then I can perform an upgrade over there, or do whatever data management or backup, and then join it back up to the one that remained live and allow it to catch up if you will. The benefits of that, whether it's from a business continuity and disaster recovery, or high availability standpoint, flexibility in terms of managing downtime. There is a wide variety of benefits to going with that type of infrastructure especially in an environment where things have to remain up 24x7.

Richard Campbell: It's just happening more and more and more. I think we are getting closer to this theoretical world of the computing cloud, where I just buy performance as I need it, and can move my app anywhere I want to go.

Greg Hughes: Absolutely, that was a great email.

Richard Campbell: Thanks a lot Alan. All right Greg, let's get to our guest. Simon Goldstein is Corillian's Director of Security Operations, and a CISA. He has over 20 years of IT management and compliance experience. As principal of his own consulting company, Simon led business transformations for multinational manufacturers and is an expert in regulatory compliance assessments. He served as a senior eBusiness Architect for Sterling Commerce, and was instrumental in establishing their HIPAA compliance consulting service. Simon is a frequent speaker at Universities and Industry Conferences on business infrastructure, governance, and security. Simon worked in the financial services industry for over 20 years in a variety of technology management and planning positions with Citibank. He has also held Senior IT Management positions with PrePress Solutions, and at Norm Thompson Outfitters. Welcome, Simon.

Simon Goldstein: Well, thank you very much, appreciate being here today.

Greg Hughes: Simon, that's quite the list of past experience there.

Simon Goldstein: Well, if you live long enough and you keep moving, you wind up in a lot of different companies. Took me 20 years to figure out you don't have to stay put with one company for your whole career and I finally figured that out and so, the rest has all happened in the last 30 seconds.

Greg Hughes: Yeah, that's great. Richard, Simon is a good friend of mine. So, I can say honestly, that he is older than I am.

Simon Goldstein: I can actually say that if you presume I am reasonably precocious, I could qualify as to be old enough to be his father.

Greg Hughes: I have the benefit and the opportunity and really the honor of working with Simon for the last couple of years. The reason I asked Simon to join us, is because his background and his expertise and really just his general point of view is proving to be really valuable in terms of, the job that I have to do in a compliance and a regulatory standpoint, security standards and what not and I thought it would be great to maybe have him share some of his thoughts and ideas with our listening audience.

Richard Campbell: Yeah, we talked about getting into compliance issues, I know that's a major issue for a lot of folks and there is all kinds of different kinds of compliance. I mean, Sarbanes-Oxley I think is causing grief for all sorts of people and HIPAA, which you know Simon mentioned quite specifically, the big health care related one, but I think, you've also been involved in ISO as well.

Simon Goldstein: I have, ISO, HIPAA, Sarbanes-Oxley, actually the progression with HIPAA, Sarbanes-Oxley, ISO was specifically in my own experience, but I have to tell you, there is a tremendous amount of overlap across all of these compliance regulatory standards. You could add Gramm-Leach-Bliley into there and some of the regulation G and regulation E and like, all of them are surrounding, basic attempts to secure information, protect privacy, assure that people have access to information when they need to, and don't have access to them when they have no business reason to do so. It really is a lot of regulation and a lot of legislation surrounding practices that one would hope and expect businesses would embrace and adopt, simply because it's the right way to do things. Truth of the matter is, it always isn't the least expensive way to do it, and very often that gets in conflict with businesses that are trying to grow very quickly, they have limited resources or are



just not mindful of the regulations or the business benefits of being really safe and secure. A lot of people, if you walk up to them and you say, governance or compliance, or security, their immediate vision is some corporate equivalent of the Deathstar rising over the horizon and looming to lay waste to all their business plans and dreams for the future.

(00:10:16)

Richard Campbell: It's a kind of punishment for actually being successful.

Simon Goldstein: If you do your job really well, you work hard, security will come and damage you. Security should be thought of more as a shield, and to some extent there is an opportunity to strategically differentiate yourself in the marketplace. It's particularly true in financial services and healthcare, largely because there is more regulations, there is more oversight. But there is also more opportunity to have personal information. Information you wouldn't necessarily staple to a billboard or a tree or to sky write for everybody to read. You don't want your medical records all over the place, you don't want your finances, you don't want your pay statement disclosed as public information.

So industries that deal with those things have come to have more oversight, but the truth of the matter is, that the companies that do work with them are much better companies and do a much better job for their customers and represent more value to them, when they embrace security practices and the governance that enables and supports and monitors them, as they are going about the course of doing their business.

Greg Hughes: So, what does that mean in the real world, I mean the people that are listening to us right now, a lot of them are IT professionals. They run exchange servers, they manage IT departments, they work on the helpdesk, they administer servers and machines, desktop machines and what not. What does security and compliance and ISO standards or what not mean for the people who are feet on the ground and for those that are managing the day-to-day operations of say an IT department?

Simon Goldstein: Let me give you a simple model, that I've been using for years, that's kind of a four component cyclical model, and then within that we can talk to the specifics of all those, because they are all great points and it's worth doing some examples in specific. Almost any organization of enough size to have their own exchange server, as an example, probably has a body of policies. They may be security policies, they may be IP policies, they go by a

number of names, but they talk about how information ought to be treated and handled. If you have policies that describe what the right practices are, and you have procedures that describe how to do your work to embrace and to fulfill the promise of those policies. If you have evidence that you're in fact following those policies, and if you can demonstrate how you remediate non-conformities or violations of those policies against almost any set of regularizations, against almost any governance requirements and frankly, against any legal threat from the outside or challenge. You could arguably be in a defensible position, if you have policies, procedures, evidence and remediation, those four things. So, from a practical standpoint, you are looking at people on a helpdesk.

Well, they know that they are not supposed to just give passwords out over the phone without perhaps challenging some additional information, or providing some questions to get answers that are challenges to authenticate the person calling, is really the person who forgot their password and needs a new temporary one. If they follow that, they have a policy about protecting information like that. They have a procedure on how they do so, and authenticate the user. They follow that procedure, if there is a help to get or anything opened for that kind of a call, they have evidence of it and they're fine. When they have instances or calls of complaints, where that was done without it, they are not, and then you can hopefully have some kind of a management review process of tickets and or incoming calls or complaints to remediate, where people are not following rules or procedures. It's a very oversimplified example, but it's representative.

Greg Hughes: In the Sarbanes-Oxley world, we are talking about something that the term we hear quite often in a lot of these regulatory environments is controls?

Simon Goldstein: Controls are nothing more than steps in a process that tell you how do you know that the right thing is being done, and that the steps that preceded were in fact followed. So, for example, let's look at a change control process, you may have a half a dozen steps that say how the change control is received. It's reviewed preliminary by someone with a technical expertise. It's passed on for other people to be sized and/or scheduled, but at some point it passes to an approval phase, where someone in authority looks at this and applies not only some technical expertise, but some business expertise.

(00:15:12)

Is this a valid control? Has it been looked at from both a technical and perhaps a risk standpoint? Are there back out procedures, if we make this change, and it does not work, has it been tested? Someone with the visibility and scope for this particular instance, to approve and say, "Yes, we ought to proceed and execute this," that's a control point. Controls are not dials, they are not gauges, they are usually either approvals or signatures or reliance or referral to someone not - - who does not have the vested necessarily interest in the step getting done. Who will look at it from an oversight perspective and say, "Yeah, that's an appropriate thing to do here, all the steps have been followed, it's a checkpoint, we are ready to proceed."

Richard Campbell: I like the language you are using, because you really haven't focused in on any particular set of compliance rules. I mean, obviously controls was a term that Greg pulled from Sarbanes-Oxley but controls is generic as well, as an element of these four basic characteristics of compliance in general.

Simon Goldstein: When I first started doing compliance review work and the work that I did was really looking at companies, then helping them understand how far away their practices and documentation and behaviors were from being in a place, where they could say with some certainty, if an outside third party looks at what we do, they will agree that we are following the regulation, whether it be HIPAA or whatever. I struggled with controls, because I kept looking for dials and gauges and other stuff like that, and I grew up from a business standpoint, years and years at Citibank. They used to talk about doing transactions in control, and what that really wound up meaning was, that you knew what was really going on, and that some oversight was attending to the quality of the work, that it was complete, that it was accurate. That it made sense.

Richard Campbell: I think that's a very powerful point you made in there which is that, it's something that a third party can see, complies or that measures up to the standard. We always forget as we are inside of these companies, how much intrinsic knowledge we have about procedures that third parties aren't going to know about?

Simon Goldstein: There is a risk when you're really knowledgeable about what you do, and that risk is that you become complacent about all that you know and start to think that others will of course know all these things, because they're so obvious. When you then have to involve new people in the process, if you've had recent additions to staff or acquisitions or you involve

another partner or another player in the process, or it's a new hand-off or something like that.

Very often, there is an opportunity, and frankly an inclination to leak something out to that -- of course the other person would take care of, because they would know, that you can't do A without having also done B and C. Well, the other party may be coming from a different perspective, may be very rude in their manner, or may simply not know all of those things. If someone else isn't watching, who does know and who was not part of the initial change or the initial first steps that began the process, it can be a problem.

Think of it this way, let's keep it really simple. If you write a piece for publication or you write a piece for school, don't you usually try and find somebody else to do the proofreading? Not because you don't know how to write, not because you don't know how to spell, it's because you are going to read things the way you intended them to be, you are not going to catch your own errors. The person, who does not have that history, that knowledge of intent, looks at just what's been represented and that's why the third party editing service if you will, or proofreading service has a value.

Greg Hughes: You know, you take your analogy, I step back a little bit because one of the things that I've seen and maybe you can comment on this several times, is that quite often -- how do I know that my foundational approach to putting a security system or a program or a department or a set of controls in place, I can look at my company, I can look at my organization and I can say, "What I am doing, appears to be sufficient, but when it comes right down to it, I am looking at it through my own filter, through my set of glasses." What is out there, and maybe you can talk about some of the standards that are available to help and ensure that when a system is put in place or when a security program is implemented that, that it actually does cover those bases and that there is not gaps that maybe, I am not even aware of just because of my personal position or knowledge.

(00:20:19)

Simon Goldstein: Yeah, that's a great question and I am going to keep playing with analogies, because I think they will work in this case. I want you to imagine bifocals for a second, and maybe not necessarily the new modern ones with graduations, but pretty firm ones. You have two perspectives here, one are the specific sub-standards or regulations that, because of the business you are in, you are obligated to comply with, and the other might be international or generalized frameworks that have been put



together overtime by seasoned professionals like the ISO standard for security management, ISO 17799 for guidance on security management systems, the certification standard currently 27001, you could look at the COBIT standards for IT, the CASO standards.

All of these represent frameworks that you could say, "Well, if I can demonstrate to the satisfaction of somebody, I would be explaining what I do too. That I comply with all these concepts and steps, I have a sound security management program." You then have to look at the regulatory environment that applies to the business or the service that you are providing. If it's healthcare, you may have to look for things specific in HIPAA or in finance to Gramm-Leach-Bliley, and see if there is anything that's not covered in those frameworks, that might specifically be addressed or addressed in a unique way. For example, if you are in California, you have Senate Bill 1386, that's going to prescribe a specific timeframe by which you have to disclose a breach in or an event in your security system that may have resulted in disclosure of information about individuals. If you take that list, and you can put this in an Excel spreadsheet -- most tools start out that way.

So, here is all these things, now, here is the tricky part, and this is where you switch lenses. This is the thing that a lot of consulting companies do not do, and that you look at this, but you look at it each one, each step, each regulation. From the context of the risk and the scope of your own business, because someone says, you have to keep information secure. Well, if you are an individual contributor, if your company is a company you've won and you've worked out of the dedicated third bedroom in your home, that security may be a locked filing cabinet. That might be appropriate to the risk of disclosure. If you are a \$200 billion company, that is an enterprise across the country with a vast wide area network, and sophisticated IT and business process functions and automation, you are obviously going to need more than some locked file cabinets. So, you need to look at all of these amend kind of -- think of this from a risk management approach, what am I really doing? What's the real scope of my business? What's the real scope of this particular requirement as it applies to my business and its size. Then formulate a counter measure or a compliance step that is appropriate to both. At the end of the day, there is an intent in each everyone of the statements, policies, regulations, requirements and your ability to craft one appropriate to the risk and scope of your business determines whether you wind up with a risk assessment that took four days and \$4000, or took 40 people for a month and \$400,000 whether or not you wind up with a

remediation or a gap list that has 10 items or 10,000.

Very, very often, there is a tendency in the consulting industry, and this has been a big complaint of mine for many years, to basically say, well the only way to do compliance is the 10,000 step \$400,000 way, and even if your mom and pop with three employees in one location, that's the only way we can do it and you are just going to have to find the means to do that, or you are going to be out of compliance, and organizations are going to come and they are going to harm your business and now we are back to the whole analogy, 'Security will hurt you.'

(00:24:54)

Greg Hughes: And I think, compliance is never for an average organization size, whether small, medium or large, is not necessarily the simple or easy undertaking, but Simon, I think both you and I know that it doesn't necessarily take a team of external consultants to do a good job of this.

Simon Goldstein: No, the value that's brought by third parties comes back to the comments I made about oversight by third parties earlier, because they are not in the midst of the forest all day long, they will identify the trees that are not well. The trees that are hanging outside the edge of the forest, the areas where it looks like there may be 10 trees that are sick at once, than the people who are in there working and living around it all day everyday.

That kind of -- I don't know what we would call it, totally abstracted or parochial or whatever kind of perspective that they have, but it is separated from any of the passion about the business, and solutions. People do become very attached to the solutions that they have to problems, and sometimes you do run into some pride of authorship that gets in the way of perhaps making a better decision or a change for the better that might even be easier to do, may even save money and time, but because it is not what was originally perceived, there is a reluctance to make the change. That's where third parties add value, when they just come in and produce these gargantuan projects or becomes a supplementary staff for aegis, under the aegis of providing all the additional oversight necessary to comply with this stuff, my eyebrow goes up and my skepticism rises.

Greg Hughes: So Simon, let's say, you are the manager of an IT department or an IT team, what are the top two or three things that you would say to somebody else in that role, that they should be thinking about or paying attention to, when it



comes to IT operations and security and compliance in general?

Simon Goldstein: A few things come to mind that I think if they do at least these, they are going to be well on their way to compliance with any set of regulations. First and foremost, is shoring the perimeter of their enterprise. They need to know who is getting in, and they need to know that the people that are coming in, are the ones that should be there, and have a reason to be there. Likewise, from the inside, people -- the access controls to technology and to information must be role based. Almost every regulation stipulates that people should have access to the information they need, nothing else. There is no reason to give them access to information that has -- especially if it's personally or customer or individually identifiable, that they do not need to perform the work that they are assigned to do.

If they do those things, if they have defined roles and by the way, those things have implications tied to them. You can't do role based access controls and securities, without having defined roles, which implies job descriptions, implies thinking about what people do. If they do those things, if they manage access to technology, access to the business, access to data, and they have done some reasonable amount of preserving the availability and the security of the data through backups and secured storage. They are doing those two or three things, there is a lot that they've just accomplished. They may have some other things that are going to go on, they may have regulations about distribution of reports, but they are foundationally and from a cultural perspective within their company, they are going to lift as instances or expressions of those foundational principles.

Richard Campbell: Again, we are still socking at the very broad strokes of how you are going to plan these things in, and obviously you need to define those roles to get a picture of your footprint. I was really thinking in terms of, before I even go after compliance, do I have an idea of what I'm impacting? How big my organization is? Wonder if we shouldn't get into maybe just exploring that what these different compliance rules really mean, HIPAA obviously is healthcare related.

Simon Goldstein: HIPAA is healthcare related, but in fact it is more. From a security standpoint, it is more about protecting individual information. It is so much like Gramm-Leach-Bliley that the crosswalks that get published on the internet in spreadsheets almost build these one to one maps between a HIPAA compliance regulation statement and one in GLB.

Greg Hughes: And GLB is the sort of Gramm-Leach-Bliley act, overreaching act for the financial services industry?

Simon Goldstein: Right.

(00:29:58)

Richard Campbell: Then there is Sarbanes-Oxley, which I think has huge ramifications for almost every company.

Simon Goldstein: Yeah, Sarbanes-Oxley otherwise known as the Accounting Firm for Employment Act. Well, I mean come on, this was -- you guys were already doing external audits. Now, we want you to come in and we want you to attest the fact that the internal process reviews and control reviews done by the organization are in fact valid and well done and useful, and it's kind of like such overkill.

Richard Campbell: Yeah, oversight of the oversight.

Simon Goldstein: It is such complete overkill against the risk. This was a reaction to corporations like Enron and others that did some things at a very senior level, and almost any public corporation probably with the compliance and cooperation of their senior most executives could behave in just that way today. How many public corporations are out there and how often has this really happened? As a result of implementing Sarbanes-Oxley, how many corporations have been found to be out of compliance and charged with any kind of misconduct, find or brought to justice if you will. I mean tens of billions of dollars have been spent on this oversight, and I'm not sure that isn't going back to a statement I made earlier, kind of taking a \$500 platinum plated hammer, because there is thumbtack on the wall, and it needs to be straightened.

Richard Campbell: Now, don't hold back Simon. Tell us how you really feel.

Simon Goldstein: You'll be getting me going on this one whole day.

Richard Campbell: I was really interested to hear you talking about ISO in the context of the financial industry or software industries in general. I always think of ISO around manufacturing.

Simon Goldstein: Well, that's right. If you think of ISO still as defined policies or practices, documentation or policies that describe the work processes that ought to go on to enable those foundational points to be solved and to exist in your organization. Then look at a means of



governance of reviewing that, and making sure that in fact the programs and policies and procedures are being followed. That there are processes in place to remediate where non-conformity exists. We are coming back to that cyclical model that I mentioned earlier, and that's exactly analysis to the Plan-Do-Check-Act model but is used for an ISO assessment. ISO has done nothing more in instance of 17799 and 27001, but taken that industrialized like approach and applied it to security management, as if that were just another business process set of systems. Again, that you have rules, that you have practices, that you have remediation and evidence, and that you have a continues improvement repair and revisit process embedded in it.

At its core level, ISO is nothing more than that. What makes it really challenging, is that the set of standards which are prescribed, are so comprehensive in terms of all the different aspects of information, physical and system security that are in place, that for a company to do all of those things, they need to be kind of at some critical size point, to be sophisticated enough to have all of those practices in place to have documentary evidence of formulated work rules or procedures against all of them, and evidence of compliance is often a level of documentation, that a lot of companies, unless they are fairly mature or aggressive about that in their culture, often don't have as completely enough in place as they need to, in order to be ISO certified.

Greg Hughes: The ISO standard, the 27001 certification and the 17799 standard that you are talking about. Sometimes people assume, well I'm not going to adopt that, because I can't afford to do all of it or it doesn't apply to my whole company or I'm really not interested in getting certified. You used a term 'foundational' a few minutes ago, and I think that's an important one to point out. Maybe you could touch on what do you mean by foundational, and what the real value is there in applying the international standard?

Simon Goldstein: The international standard describes a set of guidance's and rules, that are things that, if you were a company that involves dealing with information that needs to be protected, you would be doing these things as a well managed company anyway.

(00:35:07)

You would be looking at these things again, I need to communicate with my senior executives and I need to understand and make sure that they are aware of what things are going on in the

security management system, what issues we have, what remediation we are taking. Well, if you had financial issues, if you had manufacturing and operational issues, these same things would be discussed with senior executives on a regular basis. This just calls out security and says, "You ought to be addressing security as an important business process, as it applies to running the business." So, security is never about security for its own sake, it is always in the context of the business that is in operation. You do not run around and follow guidelines that are not applicable to the industry that you are in, unless there is a corollary standard that addresses those same concerns for the industry you are in.

So, that's foundational, because it's always starting out at what business are you in, what industry and market place are you in, what are the important business issues, what are the important security and information protection and compliance and handling issues? If you look at the ISO standard, in almost every instance you will see that the practices that they describe are generic enough to apply to them all. They will be flavored in your procedures to be specific to the business size and scope and the risk associated with your specific operation, but they are foundational, because they are like saying, "Well, we ought to have freedom of speech." Okay, well freedom of speech in a classroom means one thing, freedom of speech on a national level is another, freedom of speech in a religious organization is something else. They are all freedom of speech, but the specifics that are surrounding the tenants or the bylaws of the organization are going to be specifically and uniquely tailored in each of those examples.

Greg Hughes: The concept of security not being a project or an event, but rather a way of doing things that's really supported by this business process standard.

Simon Goldstein: All of this is about risk management. At the end of the day, you are looking at your business and saying, "If information that I am charged is part of my business for keeping safe and secure is exposed, I have a business risk." These frameworks, frameworks like the ISO standards, HIPAA regulation, GLB, number of the others. All point out practices that if followed, put a business in a position of mitigating that risk. The extent and specific implementation that they follow, should be appropriate to the size and scope of the risk.

Richard Campbell: That sounds like the real key-point to start of with is, getting a picture of what the scope of your risk is.



Simon Goldstein: It's vital, it's critical, and in fact the ISO standard is a risk based standard. If you were to participate tomorrow in a third party review to get you certified for the ISO 27001, it would start by a review of your risk assessment for your business. What are your big risks? Oh great, these four things? What have you done to mitigate those risks? Show me evidence of what policies, procedures, practices and steps you've taken. Show me evidence of how you govern them to make sure that they are in effect and in fact these things are being followed and executed as prescribed. Show me evidence of what you do when you find that practices aren't being followed. What you do to train and retrain people where necessary, and show us how you then go back to remediate and review the effectiveness of remediation to make sure that in fact, you are protecting that which you set out to protect to begin with.

It's really not rocket science and it's really not hard but very, very often business do not close the loop and keep the process as a cyclical, continual and ever improving process. In fact, I hate to keep pounding on the consulting world, but I think the consulting world has worked very hard to make security and governance look like a project, because they can bill for those.

Greg Hughes: One of the things that's also interesting, to point out about the ISO standard 17799 and then the certification standard 27001, there is nearly 3100 organizations that are certified under that standard or its predecessors, the British standard, what people may not realize is that, of those 3100 global organizations, 47 of them are in the United States.

(00:40:02)

Richard Campbell: Wow.

Simon Goldstein: That's it, only 47. And that's really not 47 companies, because the way the standard is managed, you can carve out pieces of your business and certified just those pieces. So for example, companies like Bechtel represent four of those 47 certifications. There are a couple of pieces of the Federal Reserve System that queue up three more. There are couple of other companies that also have multiple units of their enterprise certified, but not the entire enterprise.

Richard Campbell: I could see them wanting to break those units down, because it's easier to get a smaller piece certified.

Simon Goldstein: It's about managing scope and then managing that cyclical process to the

refinement necessary to achieve the certification. You are right; it is easier to chew the submarine sandwich one bite at a time. I don't care for elephant very much, but I really like submarine sandwiches.

Richard Campbell: Submarine sandwiches. Are we talking then about a competitive advantage for those 41 entities?

Simon Goldstein: Let me ask you a question. You work hard for your money, and you are going to go to a bank and you are going to deposit your pay and you are going to pay bills and perhaps make some investments, keep some other things. You have a choice between two banks, their fee structure is identical, their services, hours of operation everything identical. One of them has this international security certification, the other one promises they'll do a good job protecting your stuff. Where are you going to open your account?

Richard Campbell: Point well taken.

Simon Goldstein: The same thing would go between two hospitals. Let's assume the doctor's practice out of both. One promises that no one will get their hands on your medical records, the other one has an international standard for security management. Clearly, that's where you're going to go. It is an enormous competitive and strategic advantage for a company that it is in a highly regulated or competitive market place and has a certification like this.

Greg Hughes: And having a third party do the validation of that and come in and actually perform the actual examination, and then issue the certificate based on that standard, really seems it has quite a great value.

Simon Goldstein: There are very few organizations that can deal with, the process is fairly rigorous, and of all the certifications I am aware of, the ISO certification is the only one I know that requires a semi-annual audit review twice a year, and that I believe is unique in the industry, even the treasury department does not go anywhere twice a year.

Greg Hughes: That's one thing to say every six months, yes I'm doing what I'll say I am doing, but to have somebody else every six months come in and say, "Yes, this organization is in fact doing what it needs to be doing," is really a different story.

Simon Goldstein: The only way that can work for you is if you have made security management and security practices a part of the operating culture of your company, your organization. And I



think at the end of the day, the best way to express a concept, which I believe Greg mentioned earlier about security being a process, not event, is a continues unending process and that can only be expressed when it is a cultural attribute of the organization that you are working at.

Greg Hughes: Yeah, you really have to live it.

Richard Campbell: Alright, I think we are just about out of time. Any final words Simon, before we wrap up?

Simon Goldstein: Nothing else. I would like everybody to understand that it is a valuable and useful thing to embrace security practices, that they always need to be done in the scope and in the context of the risk that they are trying to mitigate, and it is a part of a regulatory environment that is only going to grow more complex and demanding as time progresses.

Richard Campbell: Can't argue with that. Simon, thanks very much for your time. We really appreciate your insight on compliance.

Greg Hughes: Thanks Simon.

Simon Goldstein: My pleasure, thank you for having me on.

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