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 #132
(Transcription services provided by PWOP Productions)

Simon Goldstein on what's IT Pros need to know about Audits!
October 28, 2009

[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 #132, with guest Simon Goldstein, recorded Thursday, October 8, 2009. 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. You're listening to RunAs Radio and with me as always, my co-host, Greg Hughes.

Greg Hughes: Hey everyone. What's up, Richard?

Richard Campbell: Ah. You know, no rest for the wicked but we're making our way through wintertime. It's now dark in the mornings.

Greg Hughes: Yeah. Is it dark where you're at right now?

Richard Campbell: Not too bad, but I've realized since we've built the house and we moved in in May we've never had to deal with the fact that it is dark in the morning so my programmable light system really isn't set up to turn on the lights in the kitchen from the bedroom. This is not a normal problem. I don't have all those problems.

Greg Hughes: Wait a minute. Your programmable light system is not turning the lights on the right time?

Richard Campbell: Well, I haven't actually set it up. I never thought that I would need to turn on the lights from the bedroom going into the kitchen because there's always been light.

Greg Hughes: Doesn't your programmable light system know what time the sun comes up?

Richard Campbell: Well, yeah. It's just a programming failure on my part. I haven't actually done the work.

Greg Hughes: Ah, user error. Got you. Well, the sun is shining in my face where I'm at, but I'm a few hours south of you.

Richard Campbell: There you go. All right, how about we do a show?

Greg Hughes: Yeah, let's talk to Simon.

Richard Campbell: All right, let's introduce Simon. Simon is Fiserv's Director of Risk Management, a CISA, and CISM. He assumed responsibilities for CheckFree's IT Risk and Compliance functions upon Corillian's acquisition by CheckFree in 2007, transitioning to Fiserv upon its acquisition of CheckFree later in 2007. That's a little acquisition mayhem there. Simon led the successful achievement of Corillian's ISMS certification first under BS7799-2, and then ISO27001. As principal of his own consulting company, Simon has led business transformations for multinational manufacturers managing HIPAA compliance assessments for private and public sector organizations, and led an online retail startup's operations. He also served as a Senior eBusiness Architect for Sterling Commerce, establishing their HIPAA compliance consulting service. Simon has over 20 years of IT management and compliance experience. He has served in numerous technology management roles at Citicorp, as the senior IT officer at PrePress Solutions, and the VP of IT at Norm Thompson Outfitters. Simon is an advisor to companies on ISO27001 compliance, and a frequent speaker at universities and industry conferences on business infrastructure, governance, and security, and a previous guest. Welcome back, Simon. It's great to talk to you.

Greg Hughes: Hey, Simon. You know, I have to add he's also been my colleague for several years and is a very good friend.

Simon Goldstein: Well, thank you very much, Greg. I appreciate that, and likewise. And you got it, for my weather report I have the sun coming in sideways to my window right now but I do have a beautiful view of one tree that is going rapidly from bright yellow to a kind of an orange color. Fall is my favorite season and I'm thoroughly enjoying getting something resembling vibrant foliage.

Richard Campbell: Yup, it's definitely Fall now.

Greg Hughes: It is.

Richard Campbell: So the last time we've talked to you, I think it was compliance related because that seems to be your life these days, isn't it?

Simon Goldstein: It is pretty much, Risk management, some amount of compliance, and the parts of security and in particular IT security that bleed their way specifically in.

Richard Campbell: Right. So where are we going to drill in today?

Greg Hughes: What do IT Pros need to know about audits. I mean, we've all seen IT departments cringe at the thought of here comes an auditor. So what do they really need to know?

Richard Campbell: Hey, I'm cringing now.

Greg Hughes: I cringe when I hear the word audit, you know.

Richard Campbell: Yeah, I think that's really the thing. So maybe we've got to start right in the beginning with what kind of audits are IT folks dealing with these days?

Simon Goldstein: Well, they deal with a variety of them and there's a fair amount of overlap. They deal with audits in compliance with sections of Sarbanes Oxley. If they're members of good size public companies, they're dealing with IT audits. If they're in the health-care industry and they're trying to demonstrate compliance with the IT component regulations within HIPAA, they're dealing with them in the financial services industry in compliance with Gramm-Leach-Bliley and the PATRIOT Act and others, no matter what industry you're in there seems to be at least some amount of audit requirement to demonstrate that there are good practices and sound security controls mostly surrounding the handling of your data, and my data, and everyone else's.

Richard Campbell: Yeah, losing data? Bad.

Simon Goldstein: We've seen many examples of both public and somewhat less so of what can happen to individuals and to corporations as a result of data breaches, data fest both in the inside and from the outside.

Greg Hughes: So what's the classic, maybe even cliché response, bad response by IT when they know an audit is coming?

Simon Goldstein: Once the panic is set aside and diminishes a little bit in their souls, the next reaction seems to be two things. Clean everything and hide everything.

Richard Campbell: Right.

Simon Goldstein: And neither of those really is particularly healthful. People tend to lose sight of why audits are performed. It is not a function that is done so that people can point fingers and say how bad you are, but it's an opportunity to do a few things. First of all, confirm that the hard work you've been doing to control your IT environment is in fact enforced, and it's effective, and it's doing its job. It's also a way to get an extra pair of eyes, ones that are not so familiar with the forest and the trees that you've planted within it to look at things and say, "You know there's some best practices here that you might want to implement that might make things better." There are some places where there are some holes you may not have noticed in your day-to-day excursions through the IT environment that you're managing. And the audits can really be a useful, helpful tool in helping you determine where you're going to go next and what your priorities in the coming months and years are going to be. So there's a positive aspect.

Richard Campbell: Isn't there an auditor essentially like a consultant? We have this advantage that we see so many different systems that we have a better sense of what you can and can't do reasonably? I think most folks working in the same shop everyday, they just don't have that breathe of the different ways that folks get things done.

Simon Goldstein: There's a yes and a no answer to that question. Certainly you're right in the fact that the auditor likely is traveling around seeing a variety of implementations within the same vertical industry as you're working and so they have a really, really clear sense of what best practices are, what works, what doesn't work, what's applicable to a domain of your size and scale and scope or not. The no part of the question is that in role as an auditor they're there to evaluate and identify and they're not suppose to, if they're good auditors, bleed over into the consulting side of this is what you ought to do.

Greg Hughes: Right. What's the difference between an audit and a risk assessment? This is a topic of conversation that I've run into a few times and there can often be some confusion.

Simon Goldstein: A risk assessment is identifying opportunities where there are threats and vulnerabilities in your environment. There are threats usually obviously from the inside or from the outside, but most people tend to pay attention mostly to external threats and evaluating, one, how vulnerable you are to those threats and as a result how likely those threats are to manifest themselves, understanding what the impact would be if they were to manifest themselves. A simple example is how likely are you to be subject to a storm so severe that your people can't get to work or your building maybe damaged or your power maybe cut, and if any of those things happen how prepared at you to deal with that, and if they happen in the things that you put in place to deal with it take effect and go into operation, what material loses or what material risks to assets that you have might materialize. That's the risk assessment part. An audit comes in and says, okay, you've determined all these risks and as a result you've set up these programs, and you've got back-up power, and you've got generators, and you've got a business continuity plan. Well, how well would those things work because they went into effect? Give me evidence that you've done the due diligence and testing to show that if that storm came that your power back-up system's been tested and in fact would go into effect, that your business continuity plan has been tested, and in fact people would know what to do and you would be able to continue operation through whatever means you've set up. So it's a difference between identifying what controls ought to be in place and the audit coming in and determining

whether or not those controls, one, are enforced, and two, whether they are likely to or are in fact effective at addressing the risk that have been identified. So many, many audits today and many control sets around them have taken the posture of being risk-based so they presume a risk assessment.

Greg Hughes: From the standpoint of maybe we could just call it surviving an IT audit process, what would you say are the practices that people working in IT should follow as a general rule to help them be successful, and by being successful I think we probably don't just mean get a good audit result but rather what we mean is have an outcome that is beneficial. So in other words, make improvements or get the overall best outcome of an audit. What do people maybe thinking about what they need to do?

Simon Goldstein: That's a great question, and the answer really is fairly straightforward and simple. Audits like everything else in businesses, in corporations, are process and there's a pretty simple straightforward plan to follow to understand how to participate in the audit, how to get the most benefit out of it, and how to do the best job of demonstrating the real situation and circumstances that your company is working from an IT perspective. First and foremost, every audit have some kind of a scope document associated with it, something that communicates to the organization being audited, what's in bound for this review and what is not and getting that from the audit group, whether it's an internal audit group or of it's an external organization, that's being brought in to perform a particular kind of audit. Getting that scope document upfront is vital because it puts clear boundaries in place for you in terms of which systems, which technologies, which departments, which operations are going to be reviewed and which ones are not. The reason that's important is that the steps that follow and the extent to which you size them and determine who's going to be involved or not are dependent on that scope. It's foundational. Once you have the scope, you then need to look at, and in most cases auditors will tell you this is the kind of documentation I would like to have access to in advance of coming onsite. It will usually be IT policies, procedure documents, they maybe looking for process flaws if you have them, and they'll prescribe a specific set of documents. When you look at those, there are a couple of things you need to do. One, you need to get a sense of have they describe a specific document, or have they describe content. For example, are they asking for my change control process documentation? That maybe spread across one to four or five different procedure documents, each of which calls out or describes a particular aspect of your change process management system. When you provide documentation, you always want to think in terms of responding to the control or to the specific evidence that they're looking for. Don't be caught up in looking for a document with the same name as indicated in the list. The list that the auditor provides is generic.

Greg Hughes: Right.

Simon Goldstein: Because they go to many places where things are named in a variety of ways so they're describing the kind of documentation they want. It's up to you to work with the auditor, clarify any issues and get the right documents in their hands.

Greg Hughes: Understanding the purposes, the purpose behind each question that the auditor is asking, whether it's onsite or ahead of time as you're saying, is really pretty important, being able to sort of evaluate the question and then understand in the context of your business what they're looking for.

Simon Goldstein: Very much so. It is a really good idea not to make assumptions about what in the world the auditor is asking and to get clarity, otherwise, you may be answering a question that will take them down, or rather go in a direction you don't particularly care to go and they had no intention of going before you brought it up. The other thing is again it may lead them to a different documentation. You want to make sure that you are giving them the answer to the question they are really asking and clarifying is very, very important. The other thing that comes as a result of that is understanding who auditors are going to need to speak with or interview when they come onsite. Again, going back to the scope document, going back to the documentation, those are clues as to which areas of your IT operation are going to be explored and that will give you an idea of who will be the best person to put in the room. It's not always necessarily the leader of that function. It maybe someone within that operation who can answer more detailed questions should the auditor have them. Ideally you like to have someone in the room who can approach an operation or function or process from an oversight or governance role, someone who's managing it, as well as someone who is deeply involved in the details so should a technical question come up it's clear there'd be enough brain power in the room, enough knowledge in the room to answer the questions accurately.

Richard Campbell: Do you see folks running into issues where they're just not committing sufficient resources to the auditors to be successful? Like most of the time those best minds, those guys are busy.

Simon Goldstein: They are busy and if your organization is subject to an audit, it's not being done because someone decided this would be a fun way to spend money. Their doing it because they either have a legal or a regulatory obligation to do so, or for competitive reasons it is a best practice they have to be able to demonstrate they've performed just as well as any of your competitors. It is as important to

process even though it's for discreet periods of time as your security controls, as making sure your versions are up-to-date in your applications, that you've got sound change management practices, all of those things that you would do to manage an IT operation. This is just one more. And because audits tend to be discreet for specific periods of time, you hit on something key here. The very worse thing you could do, the worst mistake you could make in an audit is to basically under resource the activity and blow it off.

Richard Campbell: Right.

Simon Goldstein: You will virtually always get an unsatisfactory result and often one that does not do justice to your operation.

Greg Hughes: Sure. An audit being a point in time sort of -- it's kind of like taking a test, isn't it? It's like you get a grade and then it's done a lot of the time. Do you see organizations treating audit events as sort of like, it's like the grade by which they evaluate their entire process, yet it is a point in time thing? There's no continuous improvement type of thing implied by an audit, not like risk management, and risk assessment, and general continuous improvement programs. So how do you look at audits as sort of their point in time process fitting into an overall quality management system?

Simon Goldstein: In every quality management system, there is some point of scrutiny that looks at the work product and examines it to a standard. If you were selling shirts and you have a warehouse, when the shirts came in from the manufacturer there would be stations somewhere in the warehouse where you would spot-check some of the shirts and make sure that there are no open seams or no missing buttons, there are no stains on them and the like. This is just like that. In the course of your operation, you're busy doing a lot of things to make an IT organization work. This is that station where they stop and look at how you're managing access controls. They look at whether or not you have logs identifying incidents and whether anyone is looking at them and doing anything about them. They look at whether or not you're applying patches in a timely manner to your servers. They look at all of these things and you don't get so much as a grade as this is acceptable and this is falling short of what we would expect for participants in your industry, in your business, or trying to achieve compliance, a sustain compliance, with this regulation or not.

Greg Hughes: Right.

Simon Goldstein: And so what you get is kind of an ongoing checklist. To render an audit, you're going to get one of two things. The unlikely perfect score which I think is actually almost always questionable, or you're going to get a short or long list of things minor or significant that need attention and those are useful because, one, a returning auditor can start with that list and your own management can start with that list and say what have we don't to strengthen these areas that were identified in the last audit, and how can we make those strengthening activities an integrated part of our overall quality program with respect to managing IT. So you have that as an ongoing part of continually improving your IT function, and also using the audit or that knowing the audit is a coming phenomenon to help reinforce and drive continued hearings to policies and procedures and practices. It's just another reason to do so, this one being a little more publicly visible in some cases than some others.

Richard Campbell: Yeah, it's nice to have that deadline to say we need to get this stuff in order so at least in the audit we can say, hey, we've done it wrong up until now but we know we did it and here's how we're fixing it.

Simon Goldstein: You're right, and in some instances those deadlines wind up being driven by changes in regulations. That certainly happens in the financial services industry, and frankly recently, in the health-care industry there were some recent changes in HIPAA regulations that I can almost assure everyone listening if they're involved or driving a significant amount of change in the data handling within their IT world especially if they were third party providers or peripheral providers of services in health-care industry. But really, there's another advantage in this too and that's one that most people don't see and there's a management development aspect to participating in audit. One of the things that is important in preparing for it, and one of the things which I think many companies fall down on or don't think about, in planning who's going to participate in the audit there's an opportunity to coach those people to help them understand how to answer questions asked by auditors and how not to. It goes back to something that Greg asked earlier when we were talking about challenging and asking questions to make sure you have clarity and understand the question. You want people in the room who have the knowledge to answer the question and have the skill to answer the question and not tell a story. So you don't want people telling an auditor 125% of what they know about that topic. You don't want them answering that question and then continuing on into a story about something else. You run the risk of leading the auditor in a direction outside of scope. You also run the risk of discussing things that are completely outside of the control that they were looking at and you want to do that. The other thing is that the people need to understand that auditors are not always ultimate omniscient omnipotent authorities. There are times when you need to challenge auditors. If they are asking for a document or an interview with someone or access to some process or even an area of the building, that seems to be genuinely out of

scope to what they said they were there to do. It is important to kind of stand up and say, "Tell me what control you're reviewing that requires you access to this asset, or access to this individual."

Greg Hughes: Right.

Simon Goldstein: And if they can't answer the question, invite them to move on.

Richard Campbell: That seems to be very reasonable.

Simon Goldstein: It's an important thing that a lot of them don't do.

Richard Campbell: Well, and it is this idea of challenging how is this in scope. That's why you want that scope documented in the first place so that you are able to preposition those resources and give them some fair warning. You're going to lose a certain amount of work time here to be available for this audit, and if they're going to go outside of that then there's obviously a misunderstanding from that document on either side.

Simon Goldstein: There's no reason why you shouldn't have a scope document in hand at the very least 30 days before any onsite review. In an organization, like in any other, there are people who are really good at what they do and sometimes not so good, or maybe new...

Richard Campbell: Right.

Simon Goldstein: And a little bit unskilled. And so sometimes their processes and their practices, however well intended, can fall off a bit. It is important, it is foundational to have this scope document in hand, and in hand with a reasonable amount of time so you can prepare to assist the auditor in performing their role and give them the most complete and accurate picture of the controls they're there to review. So 30 days, longer if possible. Some audits and some organizations will provide months of advance lead time, but as a barebones minimum of 30 days and there's an opportunity to push back if someone says, "Oh well, we forgot but we're coming next week." I think that's an opportunity for management to have a rescheduling discussion.

Richard Campbell: Well, and after all auditing is a business. I mean, these people are charging for the service. There had to be a quote somewhere. That's probably pretty close to the document you need.

Greg Hughes: On some cases there might be. There are also audits, and sometimes organizations maybe contractually bound to accept a surprise show up on the front doorstep point in time audit and there are a few regulatory in situations where that can happen. So you can't plan for it every time, but I can think of a lot of audits that I've never paid for. Somebody else is paying the auditor to come in and assess me as a third party provider for example.

Simon Goldstein: Sure, you're absolutely right. But if you're managing your controls on a day-to-day basis in a reasonable and consistent manner, the surprise audit when it is permissible, it maybe somewhat of a disruption in the day-to-day activity but it shouldn't be anything more than an indicator of whether you only take a shower when companies come in and clean the house or whether it's in good order all the time.

Greg Hughes: And isn't that really the point in auditing? It's that if auditing is the mechanism that is driving improvement, isn't that kind of a sign that the organization is already behind the eight ball? That audit should be a validation of what is already in place?

Simon Goldstein: It should be, you're absolutely correct, and if in fact an organization is doing the job it says it's doing and that it needs to do, then the audit that's performed whether on a spot basis without advance warning, or in a planned organized way with adequate lead time and the like, it should be getting pretty much the same result. If not, then again you've just cleaned the house for the event and need to now that too.

Greg Hughes: What about auditing standards? You've mentioned HIPAA, we've talked about PCI, there are all kinds of standards out there whether they're regulatory, private regulatory, public regulatory, that organizations are held to and my experience had been that quite often people look at like the PCI Data Security Standard or HIPAA or any other standard as like this huge mountain that they have to get to the top of and you struggle to the top and then once you're there; there is this I think artificial concept of I've made it to the top, when in reality quite often these standards are just the basics, the minimum necessary. How do you feel about that and how do you plan in the big picture, not just looking just at the regulatory concerns but looking at how those regulatory concerns fit into the overall environment, what's the way for doing that?

Simon Goldstein: Well, a couple of things there. First of all, you're right. There are lots of standards out there. They have a tremendous amount of overlap in terms of the specifics that they're exploring and examining, and there are these control matrices that are sitting out there that compare HIPAA, and Gramm-Leach-Bliley, and Sarbanes Oxley and the like and you'd see so much overlap in them that they point to something else that you just said and that is that they don't represent the pinnacle. They represent something of a baseline minimum. If nothing else, at the very least you should be doing everything that the standard says that you should be doing, or that the

piece of legislation or a resulting regulation says needs to be enforced. If you're not compliant with those things in your industry, you're not even at a minimum level of reasonable security for the business that you're in. That's what those guidelines all attempt to describe. At a very least minimum, you must be doing these things. So I look at all of those as the foundation for an overall IT quality management program and everything else that I do when I'm considering what is my security program, what's my quality program, how do I test to make sure that I'm running an effective IT organization. I look at the standards to help me build the foundation and to make sure that there isn't one control there or one set of controls that I might have thought less important that I still need to comply with and include because of a regulation or standard. But they certainly are nothing more than a departure point in the overall design of how I'm going to manage quality and assure compliance with my own policies and practices and procedures which I assume I've built because I need them in order to run an effective IT operation.

Greg Hughes: And that's, you know, simply being compliant with whichever standards apply to a business or organization. It doesn't necessarily mean that one is operating at the level one needs to operate. There could be gaps in between and it might also be necessary to operate at a level of protection or configuration or depending on what the standard covers that's above and beyond what the minimum compliance is.

Simon Goldstein: None of the standards are so specific and so detailed as to provide a complete set of things that you need to do in order to run an effective, safe, and secure operation. They only describe the fact that it will be a good idea if the door was lock when you went home at night, and it would be a good idea if you didn't let people run rampantly out with your customers' data and distributed in skywriting in the sky. They certainly don't provide the detailed level that you need to perform and you need to manage to make sure that in fact you are running a safe, secure operation up to your customers' expectations, their customers' expectations, your own expectations when you as a consumer or customer of other businesses provide them with your information to process transactions or to do business with them. These standards are meant as nothing more than to be foundational. They are the bottom, they should be the easiest hurdle for you to comply with and you should be building more appropriate ones to your business that are probably more detailed and more stringent on top of them. So yeah, achieving PCI certification, or complying with Gramm-Leach-Bliley, or meeting the HIPAA requirements, for the most part these are all describing if nothing else at the very least you must do these things.

Richard Campbell: Well, in the end PCI compliance is not just about the logo on the website. This is actually about trying to protect payment cards. I find it funny that the audit seems so adversarial when isn't an audit just a simulated version of you've had a crises, do you know what to do?

Simon Goldstein: Well, that's certainly true and in a payment card industry in particular, we've all seen the headlines and probably many of us have been blessed with some letters from credit card issuers saying, well, you know, there's been this breach here and there's been that breach there and as a result you're getting a new card issued, or as a result we're closing your account and reopening it under different numbers, and a variety of other things and there have been tremendous amounts of financial laws across the financial services and the retail industry resulting from those kinds of breaches, and in all cases when you look at them for the most part the kinds of things, the kinds of controls, the kinds of security activities and processes that most of your listeners would probably consider to be a basic, foundational, nothing extraordinary, you're finding in these investigations that in fact something didn't happen the way it was suppose to do.

Richard Campbell: Right.

Simon Goldstein: Or some risk to the operation was never attended to and as a result no controls were put in place. That particularly occurs to threats that can occur from the inside.

Richard Campbell: Yeah. The whole inside threat which I think is a whole other show. Simon, I think we're about out of time here. Any final words?

Simon Goldstein: In closing, I'd like people to start thinking about audits as an opportunity rather than an adversarial event. Look for what contributions the audit can make to their operation, to their management of their IT, and to the business overall, and I think when they do that they'll start seeing more opportunities to get more out of the audit and get a better result and participation in the process.

Richard Campbell: Simon Goldstein, thanks so much for coming on the show.

Greg Hughes: Thanks, Simon.

Simon Goldstein: You're welcome. Thank you for having me.

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