Using Standards to Build an Information Security Program
Transcript

Part 1: An Introduction to the Leading Standards: ISO 17799 and ISO 27001

Julia Allen: Welcome to CERT's podcast series: Security for Business Leaders. The CERT Program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT, working on security governance and executive outreach. Today I'm pleased to introduce Bill Wilson, the manager of CERT's Survivable Enterprise Management Team. We'll be discussing how business leaders can use international standards to help them build an enterprise security program. So, Bill, great to be in Pittsburgh with you. We don't often get in the same place at the same time.

Bill Wilson: Good afternoon, pleasure to be here.

Julia Allen: Great. Well, obviously from our joint research and efforts [we know about] ISO 17799, – an international standard called the Code of Practice for Information Security Management – and one of its companion standards, 27001, which describes an information security management system. By most measures, they're considered the leading international standards for information security. So, for our listeners, would you briefly describe what these are and what leaders should know about them?

Bill Wilson: Okay, well, let's start with 17799. And I think you used the word appropriately that I would direct everyone to, and that is to consider them practice guidelines. Another way to think of them is a handbook of controls.

Julia Allen: Oh, okay.

Bill Wilson: And really they are general principles – in some cases very general principles and guidelines – for, as the standard itself would say, initiating, implementing, monitoring, and improving information security management practices within organizations. And they're driven at commonly accepted goals. You have to keep in mind that 17799 or its origins have been around since 1992-93.

Julia Allen: I didn't realize they'd been around that long.

Bill Wilson: So they're tracking to the types of controls that we think of traditionally when we're thinking about confidentiality, integrity, and availability. And that (17799) had been out there for some time, and it's still an effective handbook of controls. It did undergo an update in the 2005 time frame, but that was really more of a reformatting, re-categorization.

Julia Allen: So some of the major sections – I know there's policy, there's authentication, access control. What are some of the major topic categories?

Bill Wilson: There are actually eleven, what they call control categories. But yes, compliance, policy, access control, risk management...

Copyright 2007 by Carnegie Mellon University

Julia Allen: We can include those in the show notes just to give folks a notional example. And then, this whole 27000 series, 27001, which describes the information security management system, which is basically the cycle that you go through to put practices in place — again, say, maybe say a little bit more about that and what business leaders should know about it.

Bill Wilson: It really can be boiled down, and in fact is organized and structured around a plan, do, check, act (PDCA) cycle.

Julia Allen: That makes good sense. So, based on your work and the various experiences that you've had, what are the advantages of using, whether it's these standards or other standards, the standards-based approach to security versus some other method? And kind of what's the cost, and any notions about the cost-benefit of taking a standards-based approach?

Bill Wilson: I'll start with the first question in terms of the advantages. As I said, the 7799 handbook of controls has been around for some time. I would say in ninety percent of the cases these are controls and categories that should be familiar to information security, even [to] some extent information technology professionals. So there is familiarity there. It's also in a common language, and more importantly, I think, over time in the roughly fifteen years since the standard has been in existence, those are fairly — they have a good track record, proven and tested within organizations and by practitioners. When you combine that handbook of controls with 27001 as the process-based approach, I think for an organization, looking for (lacking a better term) a recipe of perhaps how to build an effective security management program, it's an excellent starting point.

Julia Allen: Would it be fair to say, based on this kind of this legacy and history, that — would you go so far as to say that it's possible to benchmark yourself against others in the community who have also adopted that set of standards?

Bill Wilson: Yes, there's certainly a benefit in that it's an international standard. The amount of practitioners both by number as well as across industry sectors is very broad, so there's an opportunity for an organization to compare itself against its peers; to use 27001 perhaps to look at its supply chain, upstream and downstream; perhaps in using it to require conformance and approach it that way. As well as, over time, and certainly over the last two years, 27001 has built a fairly large community of practice that a practitioner can tap into.

Julia Allen: Okay.

Bill Wilson: And then the last advantage, I would characterize as a support system. As it is an international standard, as there is an auditable component, as there is a certification process, there are a number of resources both in the public and private domain that organizations can draw on for reference or assistance in using 27001 or 17799.

Julia Allen: So quite a rich set of resources to draw upon to help inform and educate?

Bill Wilson: Correct.

Part 2: Getting Started

Julia Allen: So when a business leader is considering using these standards to put their program in place or maybe to benchmark their current program, what are some of the key roles that need to be involved, and what are some of the first steps to take?

Bill Wilson: Well, let me actually answer that by pointing you to a negative example, and that's because I feel there's a need to keep one standard, or actually the handbook of controls, in the context of the larger 27001 standard. We, in our experience, continually run into organizations who are following what I would call the Nike model: "Just do it." And they're gravitating towards the "do" part of the plan, do, check, act [process], without having done sufficient planning. And those are organizations that are starting with the handbook of controls and are using that as reference. And when you've approached them or they answer the question of how are they proceeding with their 27001 or 17799 approach, they're saying, "Well, we've chosen a particular control group where we feel there's a need, and we're just marching through that in a checklist fashion." As a place to start for an organization that perhaps is in its infancy, not a bad tack to take. But really, it's [about] needing to put those controls, and the risk-based selection and then treatment, into the context of the organization and the information security management system that it's trying to build, which is where 27001 comes into play.

So my first argument would be the first step is to start with 27001, versus 17799. An important component, since you are talking about an organizational-based improvement activity, is obviously to have sponsorship — right? – and awareness. Know what you're getting into, because this is going to take time. It's a process-based approach, which is going to require care and feeding to sustain it. And so you really need to appreciate what the investment's going to be internally in terms of resources and cost, as well as what might be required externally.

Another critical issue is scoping, in terms of whether you're going to build a management system that looks across the organization or perhaps [is] relegated initially to selected business units.

Julia Allen: Right, because you might actually want to pilot it or do a trial balloon before you commit the whole organization.

Bill Wilson: Right, what systems or business processes might you choose to include or exclude? A large number of decisions are required by the organization to properly scope it, (1) so it meets their needs, (2) also so, treating it like a project, that you're building towards a successful pilot or implementation from the first instantiation.

Julia Allen: Okay, well those are good places and good considerations for getting started. So, is it best to build this capability in-house from what you've seen, kind of build up your own core competence, or is it better to use an outside service provider? What are some of the pros and cons?

Bill Wilson: There are advantages and disadvantages to each. I think one of the things I'd want listeners to know is, in my mind, one of the hallmarks of success is being able to put 27001, as well as the standards or controls prescribed in 17799, in the context of the business environment. That's not going to come easily to an outsider.

And so whether you decide you use a lot of outside resources or do it in-house, I think organizations need to understand what their commitment will be in terms of providing and mining that information in terms of, really, what assets are under the purview of this approach? What really are the business goals and needs that you're looking for security to buttress or help assist you in?

And so while a lot of this and a lot of services are available to outsource or leave this to an experienced service provider, the need to provide that context and guidance from an organizational perspective will always be critical. So there'll always be a need for a collaborative approach and involvement by the organization, if they choose to do some of the activities outside.

But in terms of going in-house, it helps for the organization to have a familiarity with process improvement concepts, certainly if they have similar experience with ISO 9001 or, in the SEI vernacular, Capability Maturity Model, things like that. They're aware of some of the opportunities and pitfalls that they may find as they undertake such an organizational-level activity. And there is a lot of resources in terms of the standards themselves, guidance, [and] community experience that are available to no or little cost to the organization if it wants to do this itself. However, as I mentioned, there's a fairly robust cottage industry in terms of outside consultants, outside evaluators.

Julia Allen: Okay, so it sounds like much of the same thinking that you would want to apply to any kind of make or buy decision, you would want to apply to this process as well.

Bill Wilson: Right.

Part 3: Implementation Challenges, Barriers, & Key Roles

Julia Allen: Okay, so this sounds like, I mean, you've got this body of knowledge, you've got a community, you've got various approaches, specifications, certifications. I mean, this sounds like kind of a no-brainer in terms of, “Why wouldn't I march down this path?” So, based on your observations and experience, what have you found to be some of the challenges, or maybe the barriers, in building a standards-based security program?

Bill Wilson: I think the challenges — well, first you have to recognize that this is a process-based approach, driven by risk assessment or risk management. At the end of the day, the bridge between 27001 and 17799 is the risk assessment that is practiced and the results and how they're acted upon, which really serves as the gap analysis by which the organization determines what from this cookbook or collection or handbook of controls is applicable to my organization and its assets.

Julia Allen: So the risk assessment basically being, or the risk assessment results being what guides you in determining what actions to take?

Bill Wilson: Correct. And not just being there to guide you, but also that the assessment is undertaken and documented in such a way that, for lack of a better word, those results are defensible. One of the critical elements of 27001 is the creation or documentation of an SOA, a Statement Of Applicability, and that's the filter through which an organization looks at the list of controls, or categories of controls, in 17799. Which is to say, "We've looked at our critical business processes, deemed and determined which assets are critical, undertaken a rigorous approach to identify the relevant risks to those assets, and have come up with these required mitigation steps or risk treatment options." Those risk treatment options drive the control selection decision and determine which of those controls in 17799 are appropriate and which are not.

In terms of whether or not an organization is compliant with 27001, it really comes down to, “Was the risk assessment undertaken completely and effectively such that the risk treatment plans address the high-priority risks and have led to effective risk-based and cost-based decision-making on the part of management as to which of those controls are applicable and which are not?”

Julia Allen: So, then, that is what you mean by defensible, in other words – that you can take that whole set of process steps and you can relate the conclusions for the controls that you selected all the way back to your risk assessment and the critical assets that you're trying to protect.

Copyright 2007 by Carnegie Mellon University

Bill Wilson: Right, and going so far in documentation that you're not just doing it to say, "I have followed the steps advocated in the standard," but, "I've followed the steps advocated in the standard, and I've produced results that tie back to my business needs and the organization's assets." So I can say that I made these decisions based on the risks and needs of the organization, not necessarily the mechanics or the process that's advocated in either of the guidelines or standard.

Julia Allen: I mean, the way you've described this it seems very rational, it seems very straightforward, and yet a lot of organizations are not undertaking this kind of rigorous approach. I know that leaders have many, many considerations for their time, for their attention, for their investment dollars, so what do you think has been a barrier perhaps to more wider spread adoption of such a standard-based approach?

Bill Wilson: The easy answer for me is that the devil, as they say, is in the details. And in many cases, when I'm giving you a high-level description, I'm not giving you much more than what is in the 27001 standard. I mean, the document itself is roughly 45 to 48 pages and, again, does an effective, high-level job of describing what needs to be done. But there are a number of processes, a number of practices, a number of tools that are required to populate that for an organization to efficiently and effectively get to the position where they can be making those risk-based, control selection decisions. And I think that is the point where oftentimes a lot of organizations struggle.

Julia Allen: Kind of lose their collective will.

Bill Wilson: Right, they don't have the experience, or perhaps they aren't being pointed to a solution that is effective or applicable to their organization. Or, oftentimes they may jump over that and go right into a non-defensible selection of controls, or return to where their comfort level is, being driven more by the technology than a lot of the business context and information that's captured in the early stages of 27001.

Julia Allen: Yeah, well, that makes sense. I mean, sometimes you get into something like this, as you talked earlier, you know, do your planning and do your strategy, do your thinking up-front. But you get into this and then you realize it's a much larger undertaking than you originally planned for.

Bill Wilson: Right. I think another Achilles heel for organizations is relegating this to the information technology or information security program. I mean oftentimes that's the source of the original onus to pursue 27001 or the sponsorship. But hopefully I've given you appreciation, at least in the early stages of defining and implementing the ISMS, that a lot of context and information is required from the business units and the business areas, and so without their involvement, without their information and buy-in, you're not going to get the benefits or be able to pursue the holistic approach that the 27001 advocates.

Julia Allen: I'd asked you a little bit earlier about roles. Are there some key roles that need to be participants? You mentioned the business unit leaders, you want to obviously get advocacy and support from the key stakeholders, but what would you say are kind of the handful of key roles that you've seen really make this a go in an organization?

Bill Wilson: First of all – they may not have this title – I think a key role is the project manager. I think one of the elements of success for 27001, or any initiative of this type, is for the organization to treat it like the fairly broad-encompassing project that it is, and to make sure that they are doing the requisite planning in the style and using the tools and approaches that the organization is familiar with, not just to satisfy 27001, but to run this like a project, to staff it, communicate it, track

Copyright 2007 by Carnegie Mellon University

it like they would any similarly sized initiative within the organization. So it may not be the leader or sponsor of the activity, but you really need to have somebody managing the day-to-day details of the rollout of this activity.

Obviously, there is a need for, initially, some level of outreach and awareness. So somebody should be given responsibility for communicating the background on the process, preparing the organization and informing it of what it's going to be going through, what the information [is] that is required, and what the level of involvement will be from various aspects, be it business units, administrative areas like HR (human resources), and certainly the information technology and information security department.

And then there are the roles in terms of the sponsor, the leader. I mean, traditionally a multi-dimensional project team is created to lead the organization through a 27001 activity, and 27001 itself as well as some of the common references go into this in much more detail. I would refer organizations to those to learn more about specific roles.

Obviously, if you're looking at 27001 from a certification aspect, the internal audit group plays a role. The certification process is actually two-tiered. It involves an internal audit, preceded by a third-party external audit. And so, obviously, if that is a goal of the organization in 27001, you would want to involve that group from the beginning, not just for what they bring to the table in terms of an improvement initiative in their involvement just to help with gap analysis control selection, but also to have them prepare to present the defensible results to that third-party auditor.

Part 4: Sustaining a Standards-Based Security Program

Julia Allen: I just want to emphasize that point you mentioned about making it a legitimized project within the organization, because I know [in] so many of the efforts I've seen, you get all the key stakeholders in the room and you somehow expect them to add this to their existing set of roles and responsibilities with no additional resource, no additional time, just something additional that the organization has to take on. And so the notion of creating it as a legitimized project like any other acquisition, any new product line, any new service, any new IT initiative, with the same reporting structures and requirements, I think is, as you say, kind of key to success. What about sustainability? So [let’s say] you've put a program in place, you do have some good definitions, you've done your risk assessment. Do you find any nuances or special requirements in terms of actual continuous improvement or sustainment of this type of program?

Bill Wilson: We've talked about some of the generic benefits for organizations, but [at] the end of the day, that organization's unique operating environment must be considered. And so it may be pursuing 27001 for regulatory and compliance reasons, but it's certainly, particularly in today's business climate, not going to be the only piece of legislation or regulation that says something about how that organization needs to approach information security or information protection. And so enough flexibility has to be introduced into the approach that you can make that translation to show where 27001 activity is supporting, or in some cases may not be completely supporting, the compliance activities of the organization.

I think another issue of sustainability is recognizing that 27001 and 17799 are a starting point, and just that. They're giving you a logical bridge to effectively guide you to control selections when considering those controls within 7799, in those eleven categories and the 130- or 140- odd controls. All the controls an organization needs, particularly perhaps for some of its most unique and critical assets, are not going to be in that –

Julia Allen: In that list.

Copyright 2007 by Carnegie Mellon University

Bill Wilson: In that handbook, right. They may come up with a recipe where the ingredients that they're looking for are not to be found in 17799. So they need to be prepared to go beyond what's advocated and recognize that at times they may need to go outside the rigor – the discipline of the standard — to really meet with their security requirements.

Julia Allen: Right, but would it be fair to say that if there are additional controls or practices or activities that need to be included for compliance or other reasons, that the information security management system that 27001 lays out could be used for the insertion of those additional practices and controls? In other words, you can still have your same plan, do, check, act improvement cycle and just enrich the set of controls beyond what's in 17799?

Bill Wilson: Yes, conceptually that is how it works and how it should work, but, again, keeping in mind that 27001 is focusing on the what. It is not giving organizations that much on the how, and so there's a need to seek additional guidance, perhaps seek other references, to help put in place the effective practices will allow you to realize just that outcome, Julia.

Julia Allen: Okay, so this may not be a fair question to ask, but if I do —

Bill Wilson: That's fine. Those are the kinds I like.

Julia Allen: So if I, as an organizational leader, adopt these standards, will I keep myself out of the headlines, with respect to security breaches or other types of things that would put me above the fold, with respect to security?

Bill Wilson: It represents a significant starting point and first effort. I think it gives you — it lays, or can lay for the organization, the blueprint for effective protection. But that sustainment is key, right? We know — and looking at a house building analogy, right? — the importance of the foundation, and how we build upon all those aspects to get to the details of where we will put the locks, where the doors will be. That architecture will come from pursuing 27001, but it's the day-to-day management of operational activities and making sure that the right people are in the right place at the right time to make sure that the controls are not just implemented, but are in the end effective and can be traced back to managing the risks. If the organization adopts the process improvement and process-based strategic view of security that's advocated by 27001, it will allow itself to realize some of the flexibility so that as its risk environment changes, as its available controls on both the operational, management, and technical side change, it has begun to put in place that process and therefore that discipline by which it can adapt, which I think is key to being able to adequately protect the organization and hopefully keep the right folks out of the headlines.

Julia Allen: And maybe out of jail.

Bill Wilson: Yes.

Julia Allen: So, just to close, I know that there are some future plans for the whole 27000 series of standards. Can you say a little bit about a preview of coming attractions there?

Bill Wilson: The first thing is the simplest one, and that's to bring the numbering scheme in line. I think one of the initial parts or initial places where folks get confused is 27001 versus 17799, and the fact that the handbook of controls (17799) actually preceded the auditable standard (27001). So 27001 is the definition or requirement specification for the ISMS. Down the road, 17799 will convert to 27002, which brings the numbering scheme into line and also speaks to the

Copyright 2007 by Carnegie Mellon University

progression. Consider 27001 in the process and framework first as a bridge to the selection of controls in the handbook.

And then there are plans out of ISO to produce at least three more in that series: 27003, 27004, and 27005. 27003 have been deemed the implementation guidelines, so they will begin at a high level to get to some of the hows that are prescribed in 27001, and will begin to speak to: What should organizations consider in the policy space? How can they link some of these things to their activities in, at least, security governance? What type of approaches in more detail are advocated or recommended in risk assessment? So that's 27003. 27004 will be their first attempt to get into the metrics and measurement space. And then 27005 will actually expand on 27003 by specifically making recommendations in the risk assessment space, as they recognize that that really is the crucial tool or process, that it's the engine or it greases the wheel of the 27001 standards-based approach in this context.

Julia Allen: Well, I'm so appreciative of your expertise and comments and thoughts on this. We'll include links to a lot of the references that you've called out in our show notes. In closing, are there any kind of final thoughts or remarks that you'd like to share, or have we pretty much covered it?

Bill Wilson: There is a large community out there. There are conferences, publications just around each of the handbooks. There are more resources where individuals and organizations can learn. And again, as long as you keep 27001 in context as a place to start to begin to pursue a process-based approach to information security, I think more organizations than not will find 27001 and some of its principles and guidelines to be a very applicable one in putting them and keeping them on the road to effective information security management.

Julia Allen: Well great Bill, thanks very much, and I look forward to talking with you again.

Bill Wilson: Thank you.

Copyright 2007 by Carnegie Mellon University