The Path from Information Security Risk Assessment to Compliance
Transcript

Part 1: Assessing Security Risk in a Business Context

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 risk assessment as an effective tool for achieving compliance. So, Bill, great to have you with us today.

Bill Wilson: Good afternoon, thank you.

Julia Allen: Risk assessment is regularly used by business leaders to manage all kinds of organizational risks. So why is risk assessment critical when you're talking about or trying to get your hands around information and cyber security?

Bill Wilson: Well, simply put, Julia, risk assessment allows us to put information security issues in the context of the business. As technical practitioners, often we talk about information security issues by referring to the components of risk – a particular threat, a particular vulnerability. But it's really until we combine those into the variable of the risk equation and discuss the potential impact to the organization, only then can we bring it into the context of what's important to the organization and answer what I like to call the "so-what" test.

So I can tell you potentially 20 ways that I could use a particular piece of technology to compromise a particular mission or business asset you might have in your organization. But until I can articulate what that compromise would mean in terms of lost productivity, lost revenue, potential interruption to the organization, I can't begin to prioritize it or put it in the context of the other operational risk issues that the organization is challenging. And so I need to be able to do that well so that I have the basis to analyze and prioritize those information security issues alongside the other operational risk management issues in an organization.

Julia Allen: So I know that we've really struggled with getting information security and other security aspects on the radar screen of business leaders, and I suspect most business leaders are familiar with using risk assessment for other parts of managing their business. So would it be fair to say that this is a way to get security to the table?

Bill Wilson: Yes. Yes, if you can do an adequate of job of, as I said, placing that security and risk information in the context, in tangible terms, of what a potential impact represents to the organization, much like you would discuss any other risk.

Julia Allen: Excellent, so framing it using similar language and similar measures of effectiveness and what have you.

Bill Wilson: Right, in the language that various components of the organization, not just IT, are familiar with speaking about those issues and terms in.

Julia Allen: Okay, so we all know that compliance is really a hot topic for business leaders today, compliance of all types. So how can risk assessment be used to help leaders address and prioritize all the growing compliance requirements, including all of the security compliance requirements?

Bill Wilson: In that instance, it really is a case of using the risk assessment practices that are often advocated by these compliance mechanisms or requirements correctly. Let's take three or four examples. FISMA, for federal/civilian agencies to comply with the Federal Information Security Management Act, that advocates a risk-based approach. So you'll have a risk assessment that drives much of your information security activities. If you're following something like we discussed in our previous podcast, [ISO] 27001, at the heart of establishing that information security management system and complying or seeking certification in 27001 is a risk assessment or risk-based approach. If I look at something more historical like HIPAA, Health Insurance Portability and Accountability Act, in terms of meeting those security and privacy requirements, [it's] ideally risk driven. If I start to look at things like ITIL, COBIT, COSO, all of those have or advocate in some manner a risk-based approach.

Oftentimes, unfortunately, organizations are overwhelmed by the sheer volume of control or requirements that might be contained in those mechanisms. For example, FISMA [has] over 200 minimum essential security controls. 27001, when linked to [ISO] 17799, [has] over 150 controls. HIPAA itself had 140-odd data and security and privacy requirements. An organization does not have to implement all of those, and an organization has options as to how it chooses to meet those requirements. And at the heart of all of those compliance mechanisms is the recognition that risk and risk assessment should drive that.

Julia Allen: So does the risk assessment then give you an ability to, if you will, rank and stack?

Bill Wilson: Yes. Yes, ultimately it's giving you the ability to analyze and prioritize in the context of business and then, based on that information, to decide whether or not those requirements within the compliance mechanism are truly applicable to you and your environment in the organization.

Julia Allen: And do you find, based on your observations and experiences, that using a risk-based approach, that [it] may cause you to eliminate certain controls from consideration? Either they're not applicable or they're lower priority. Will that pass muster in the face of either an internal or an external audit? Is it defensible?

Bill Wilson: Yes. And the risk assessment is featured in the compliance mechanism for just that reason. An organization really has no choice but [to] attempt to tackle and implement all of the security and data requirements contained in HIPAA; whereas with a risk-based approach and focusing on the assets and what truly is important to the organization and doing that rack and stack, as you referred to it, [the organization] really only had to address the higher-priority risk items and could be in a position to accept the remaining risk or residual risk as it's known, in a defensible way to say that, "We've covered our priority risks. Our budget limitations in terms of personnel and funding prevent us perhaps from implementing some of these controls that are contained within the compliance mechanism. But because we have gone through a complete risk assessment process, have captured the results in a defensible form, that's okay." That's the basis of risk mitigation. It's not risk elimination – get rid of all of them – but consider them in a prioritized fashion against what the constraints and limitations of the organization are.

Julia Allen: And, as you said, it gets back to well-informed decision making and having a basis for the security investment choices that you make.

Bill Wilson: Right.

Part 2: Zeroing in on a Risk Assessment Method

Julia Allen: Okay, so let's talk a little bit about what some of the common risk assessment methods are that might be available to a business leader that wants to embark on this approach if they don't already have a favorite one, and how can they compare? What are some ways to compare and contrast different methods and pick smartly?

Bill Wilson: I'll hit a couple of the more commonly known and widely used. Getting back to my example of compliance mechanisms, if you look at federal civilian agencies in terms of FISMA, NIST, the National Institute of Standards, is chartered with providing all the security guidance against those statutes. And so in their special publication, 800-30, they lay out a fairly flexible approach in a qualitative fashion to risk assessment.

If you look at [ISO] 27001, recalling that podcast, there is currently a British standard, 7799-3, about to become ISO 27003, which lays out the implementation details of an effective risk assessment approach as it's viewed by BSI (British Standards Institute) and ISO (International Organization for Standardization).

Some of the other more widely knowns include CRAMM, which is another – C-R-A-M-M, stands for –.

Julia Allen: Sounds like something I'd do in graduate school, right?

Bill Wilson: Yeah, it's actually a risk analysis and management method advocated by one of the UK ministries. You also have MEHARI – don't ask me to break down the acronym as it's in French – but again one that's seeing more use in the international space. Then you have things based here in the U.S. – FRAP, the Facilitated Risk Assessment Process, as well as STAR, which is a process out of Georgia Tech University.

Julia Allen: So, obviously, there are a number of methods and approaches. So how does a business leader make sense of all that and kind of navigate their way through to the one or two that might make most sense for their organization?

Bill Wilson: Well, there are some common elements to look for in a successful information security risk assessment, and hopefully we'll get to that in the conversation. But also because of the wide use of the number of instruments that I referenced, comparisons are out there. There are case studies and experiential data that organizations can refer to, testimonials in terms of what organizations have used successfully, the pros and cons of some of those approaches. One of the things that I would advocate that business leaders do is look internally at their own operational risk management activities. There may be, in fact, one that's more closely related in look and feel to other things the organization is already doing in the operational risk management space, or [an organization] certainly might want to be looking at the types of outputs and formats generated by a particular instrument or risk assessment method because it's more conducive to the presentation or analysis of data that they're already looking at in the operational risk assessment.

Julia Allen: Right, because we said early on that the whole – one of the major benefits of taking this approach is getting security into the same set of tradeoffs and conversations as other risks. So I know – I believe that most of the methods that you mentioned were specific for information security.

Bill Wilson: Correct.

Julia Allen: But it would seem to me that some type of an integrated approach where you take that selected method, as you're starting to say, but look at what you do for operational risk management, and there may actually be an extension to the one that you already have in place that would fit quite nicely –

Bill Wilson: Yes, and you may want to in effect create a hybrid. At the end of the day, in terms of the risk analysis, there's some level of evaluation and analysis, be it quantitative or qualitative.

It might be that, for example, if a risk matrix is used or if a 1 to 5 or 1 to 3 qualitative scale is used in other parts of the organization for risk analysis, we should bring those over because of the familiarity and use already in the organization and make that part of the approach by which you score and evaluate risks. Same with something like a risk evaluation criteria, where you're trying to, in as tangible terms as possible, talk about the potential impact to the organization in terms of lost reputation, financial losses.

Julia Allen: So you're saying put maybe the losses or the impacts in comparable language in terms of –.

Bill Wilson: Right. Put them in comparable language. Or, it might be in doing, in conducting operational risk management activities in the more traditional spaces, those artifacts already exist – those risk evaluation criteria exist, or those languages exist. Again, go out, do some investigation, bring them over.

For example, I've been doing some work very recently with the Air Force, who doesn't have a lot in terms of standards or regulations for information security risk assessment or risk management, but obviously because of their safety-critical nature in terms of flight operations have a wealth of information in operational risk management. Much of it in terms of the language and the context is transferable, taking some of the information security risk information and putting it in the context of what they're already doing and how they're already managing the risk to their larger mission.

Julia Allen: That makes good sense.

Bill Wilson: And that helps to bridge the gap.

Julia Allen: Well, sure, and it also helps with the entry and the integration process of bringing the leaders along because, as you say, it's something they're already familiar with. Well, you had alluded to elements of an effective or successful security risk assessment approach. Do you want to give us a little summary of what you think or what you've observed to be the key – [what] those key elements are?

Bill Wilson: Yes. I think first and foremost you need to choose an assessment methodology that recognizes its placement in the risk management life cycle and security management life cycle. So it recognizes that its position solely is a diagnostic to generate decision information that needs to be acted upon that leads to control selection. And that initial control selection and implementation is often where the risk assessment ends, but then following through, making sure the controls are implemented effectively, managing and tracking their effectiveness over time, and starting the whole cycle of periodic assessment recognizes a complete risk assessment cycle. And you need to make sure that the assessment acknowledges that and has the hooks that lends itself in terms of generation and quality of output to managing those items and tracking those decisions over time.

Julia Allen: Sure, because a risk assessment is a point-in-time event.

Bill Wilson: Right.

Julia Allen: And even as soon as the next day the world could change –

Bill Wilson: Right.

Julia Allen: And so what I hear you saying is that the risk assessment method has to be part of a continuous risk cycle.

Bill Wilson: Right. We've talked - you and I both keep coming back to operational risk. You want to make sure that your assessment is looking at the breadth of potential risks in those terms. So, what are potential failed internal processes? What would be inadvertent or deliberate actions by people? What problems or risk could arise from actual uses of a particular system or technology? And then you need to look at external events – acts of nature, weather, things of that ilk, looking across the spectrum, not just what might be a more traditional, well-known category of threat in the information security realm.

Julia Allen: I'm thinking back on your earlier statement about qualitative approaches and just kind of curious. Have you seen any great success yet at more quantitative approaches to valuing and assessing risk, or is that – or does this problem space really not lend itself to a quantitative approach?

Bill Wilson: In limited ways it does. The majority of the methods –.

Julia Allen: We know managers love numbers, right? We all love numbers.

Bill Wilson: Yes. But the majority of methods that I referenced earlier are qualitative. Some of them can be approached quantitatively. Where we're seeing more improvement and more comfort in the quantitative aspects is in characterizing impact. Organizations have gotten better at being able to say, "Well, if I lose this information or access to this information for a period of time or if it's destroyed, what does that mean in more tangible terms?" We have a long way to go, but organizations are getting better.

Where we're still not doing a very good job, but unfortunately these methods tend to become too fixated on quantitative approaches, is on characterizing threat or vulnerability. A lot of time and effort, in my opinion, is wasted by organizations who are paralyzed in terms of saying, "Well, there's a 70% chance of that threat versus an 80% chance of a[nother] threat," and losing a lot of cycles there when simply a qualitative approach of being able to rack and stack to high, medium, and low will suffice. Because, again, you want to eventually get to looking at both sides, that threat and vulnerability side in terms of condition, but equally important that impact side in terms of the consequence to say, "All right, I've looked at it in the context of the mission, and this is whether – as to whether or not I care..." really arguing qualitatively that 10% on the threat side usually is not going to break the tie or make a difference in terms of which of the high-priority risks bubble to the top.

Julia Allen: And I've also seen arguments that, given that the threat and vulnerability landscape is constantly shifting, constantly changing, and attackers are typically way ahead of the curve when compared with defenders, that really the most constructive place to focus is on impact. Regardless of how the impact was realized, what you care about is, "How badly does it hurt?" That may be a simplification, but is that a fair way to think about it, at least?

Bill Wilson: Yes, and I think that's a critical thing I think that the listeners need to take away because not only will that environment change, let's be honest, our compliance environment will change, the regulatory environment will change. But if I can ground my security activities in a risk-based approach – [if I can say,] "All right, what's important to the organization and its contribution to mission is probably less dynamic, and certainly the impact of a compromise, of whatever source or nature, can be characterized in terms of the organization"

If I can have that information available as ground truth, I'm better prepared to more quickly adapt to changing compliance mechanisms and consider new threat scenarios or new vulnerabilities that may manifest themselves on a daily basis, because I still at the core have: "What's important, and why do I care?"

Julia Allen: Yeah, you know what matters.

Bill Wilson: Right, I've really got that ground, that critical piece of information to move the risk assessment forward.

Julia Allen: That makes sense.

Part 3: Building a Risk-Based Compliance Program

Julia Allen: So if I was a business leader and I wanted to start building a risk-based compliance program, who would I want to have involved in that, and what might be some of my first steps?

Bill Wilson: Typically an organization starts by selecting an approach; again, going out, taking advantage of some of the resources, looking internally, looking externally as to what approach might be the best fit for the organization. Then the second step would be scoping the assessment. Typically, when we're talking information security risk assessment, it's not one instantiation of the assessment covers the whole organization.

Julia Allen: Right, you want to take a piece.

Bill Wilson: Right, I'll want to take a piece, and I might want to do that organizationally by looking at a particular business unit or area of a business unit, or I might want to look at a selected or a number of business processes that might weave their way through various parts of the organization, but still they allow me to bound, to some extent, the information assets and systems that I'll look at.

Julia Allen: And I could envision in that scoping process you could go a couple of different ways, one being: pick something that's hot or critical or needs immediate attention, but you also might want to pick something maybe less mainstream so you could pilot, kind of try things out, see how – walk before you run, see how it goes.

Bill Wilson: Right, exactly. And the key there is to keep it manageable. And as long as you're kind of taking the approach of having it being driven by priority in the critical assets, you should be okay. So as long as that's the focus. If you want to scope it down small, more success-oriented for a pilot, that's great, but try to keep it manageable. Then that allows you really to pick the team and participants. Traditionally, these are done — all of what I advocated involves some team. The team might be two people, the team might be five people.

Ideally, since we're looking to get to operational risk and risk in the context of the business mission, I want to go outside of IT. I want to bring in people from the business lines to be part of the team, because certainly they're going to have the best understanding of how to characterize that impact.

Or, I may need to go out to IT or information security specifically if I want to incorporate a vulnerability assessment, kind of a point-in-time snapshot of, "Where are the vulnerabilities within the technology, and what potential access would they allow for a threat of concern to gain access and compromise an asset of concern?" But really, a multi-disciplined approach or a team to collect the information that is used to identify the risk, perform preliminary analysis, but then that is taken to senior decision makers for action.

Where we've seen a lot of success [is] again making that bridge or link to existing operational risk management activities. The organization may have a risk committee, they may have — It may or may not be aligned with their audit function, but there obviously should be bodies or forums by which operational risk is considered or discussed in the organization. Again, as we try to integrate all these risk management activities under the umbrella of operational risk, to use those as a mechanism by which you funnel through some of this risk information for a decision. And then once judgment has been passed in terms of use of limited resources and funding to implement a particular mitigation control, it typically returns to IT or a business area to finalize and implement those plans. And then with oversight and monitoring by IT and others going forward to see that if in fact those choices (1) are implemented correctly, and then (2) most importantly, are actually having an impact in terms of reducing in some way the risk to the organization.

Julia Allen: So as we approach the end of our conversation, what have you seen as maybe some of the top maybe two or three challenges or barriers or things that really get in an organization's way who wants to make this happen, and how might those be addressed if they're encountered?

Bill Wilson: One of the biggest challenges I've seen, actually, I would characterize as a lack of patience. There's a lot of information gathering, documentation to do a thorough, defensible risk assessment. Along the way, as you involve others and collect pieces of information that will comprise risk information, you will stumble upon some problems, things that are currently issues within the organization. You also will identify some gaps. Oftentimes, particularly — and I'll raise my hand as a guilty party as an IT professional – you rush to solution mode.

Julia Allen: Right, you see something that you want to pay attention to right now.

Bill Wilson: Right. And that's particularly problematic for organizations that involve an extensive, or include an extensive vulnerability assessment within their risk assessment activity in that it becomes a speed bump to completion of the risk assessment. They're so overwhelmed by what they see in terms of deficiencies to the technology today that they lose sight of the larger goal, which is put it in context of the business and then implement controls in such a fashion that I'm looking to eliminate those types of problems or risks or vulnerabilities permanently in the future.

Julia Allen: Right, do root cause, not band-aid or symptom.

Bill Wilson: Correct. So that's one. Another is inability of organizations to spend the time getting that impact piece correct. And here's one [example]. An area of the organization that oftentimes does this very well are the folks working business continuity and disaster recovery. They tend to focus on the impact side in terms of business impact analysis but are kind of divorced from the condition side of the equation. They may have some information on the types of folks you may want to consult and bring in to help characterize impact. But all of these [standards-based approaches] – and FISMA in particular and [ISO] 27001 – offer very, very vague guidance in terms of how you categorize or stratify risk. FISMA in particular, well, it's a "high" [risk] if the impact would be catastrophic to the organization.

Julia Allen: Now what does that mean –?

Bill Wilson: It's "medium" if it would be a significant impact. The organization needs to be able to define, in its own terms, what is a catastrophic failure? What is a significant risk? And that might be a very different answer for organization A compared to organization B or an organization in one sector versus another.

So, another one of the elements that I'm alluding to now but didn't get to earlier is that need for a contextual risk evaluation criteria, putting forth a lot of effort there. And that really leads itself, if done well, to another deficiency, which is failure to involve the business line personnel appropriately. You're only going to be able to tackle some of those issues regarding impact in the evaluation criteria if you bring them in and involve them in the activity.

Julia Allen: Well, and when you get back to your notion of critical asset and information and key business process, they are truly the owners of those assets. They may not know that they are, but in terms of conducting their day-to-day business, they must be. And so if there are risks to those assets, then yes, I can see that you have to have them involved if you're going to carry out any kind of risk mitigation strategy.

Bill Wilson: And I think the last thing I would offer up is to tie this back to compliance, is recognizing the role of risk assessment and compliance – maybe not just in the compliance mechanism or item of concern for today, but recognizing that by putting the time in, laying the groundwork and foundation of effective risk assessment practice, you are again establishing the basis for the organization to be better prepared to deal with changes in that compliance mechanism as well as introduction of a new compliance mechanism; not to treat it as, "I'm doing the risk assessment to allow me to comply with regulation X." It's really "I'm doing the risk assessment because it is effective and smart information security practice," the foundation and benefits of which will be realized by any compliance activity I may have to undertake in the organization.

Julia Allen: Right. So, ideally, what we get to is a way of operating and a way of addressing risk in the organization that is sound, effective business practice, and ideally you get compliance as a byproduct.

Bill Wilson: Exactly.

Julia Allen: Well, thanks, Bill. It's been really wonderful talking with you and lots of great sources of information for our listeners, and I look forward to doing it again.

Bill Wilson: All right, thank you.