Title: Making Information Security Policy Happen
Transcript

Part 1: Know Your Requirements; Make Sure Business Leaders Are Engaged

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 very pleased to introduce Paul Love, director of information security for The Standard. We'll be discussing how to put an effective, sustainable security policy program in place. So welcome, Paul. Glad to have you here today.

Paul Love: Great to be here Julia, thanks for inviting me.

Julia Allen: Oh you're welcome. So this should be fun. One of the most common pieces of advice for an effective security program is to have a security policy. We tell people to do that all the time. Why do you think this is such an important foundational practice for a good security program?

Paul Love: Julia, that's a great question, because policies are the underdog of information security. People generally look at those as a necessary evil, but really, it sets the tone of your entire information security program, and it sets the tone from the executive management level.

How I look at policies in our organization that I've worked in is that it's really senior management's voice to the organization on the minimum requirements for an information security program. So it takes it away from being our particular information security program or all the onus on the director of information security or the CISO, and really lets management own it, which is where it belongs. And then the information security practitioners become the consultants to the organization and help explain management's intent. So it really is a foundational element of any security program, because it really sets forth what senior management is expecting of the organization.

Julia Allen: So what are some of the most common sources of security policy requirements? Requirements can come from all kinds of places, but where do you typically look when you're building policy?

Paul Love: Well, you have multiple forces pulling at you when it comes from an information security standpoint. In the policy specifically, you have your regulatory, contractual, and legal requirements. So trying to navigate that myriad and trying to start something from scratch is often very difficult.

So what I like to do personally is to look at an Industry-recognized or an internationally-recognized standard that has been vetted through a large group of information security practitioners, and use that as a starting point. The benefit of that is it adds credibility to the initial sets of policies. And it really helps to insure that when you're creating the policies, you don't forget something. If you're trying to create them from scratch, you may not have remembered a specific element. So in my practice, I've actually used the ISO 17799 in the past, or the new version, the ISO 27001. This really allows the organization to use the vetted source of policies for creation of internal policies.

And then of course, this has to be reviewed and evaluated against your appropriate contractual, legal, and regulatory requirements that you have. Because the ISO 27001 is really just a base set. You really have to make sure it matches your business needs and your regulatory environment.

Julia Allen: So when you do have — I mean, I'm sure, being in the insurance business, you're subject to all kinds of legal, regulatory, contractual, other types of requirements that make their way into policy. How do you, if you use ISO 27001 as your base, how do you either do the mapping or how do you tailor kind of a base policy template or approach to the specific requirements yours needs to fulfill?

Paul Love: Well, a close collaboration with other groups within the organization, especially legal, really helps out with that. Giving them something to look at and to critique, I've found, instead of trying to create policies in a committee forum, is much more effective. So if you give them the base set, they can draw down or draw up as needed, as based off of your requirements or the regulatory environment. So a close collaboration with the key constituents within the organization is absolutely critical to an effective information security policy program.

Julia Allen: Okay, well you started down this path a little bit. How would you describe, in a little more detail, what a business leader's role and responsibility is with respect to security policy? What do you look for them to do?

Paul Love: Well, as business leader myself being in the organization, we all have a responsibility to insure that our staff understand their particular role in protecting the organization's information assets. So making sure that the individuals within the organization understand fully what their requirements are is my responsibility as a manager within the organization. And it's not just telling them this. It also includes modeling behavior that we expect our staff to emulate. So we adhere to the processes, as well as provide action support for the organization's objectives and policies. So actually living that and following it, and making sure we articulate it to our staff is very important.

And then when we see deviations from policies or processes, we as leaders must insure that the behavior is identified, corrected, and reported accordingly — and not from a punitive standpoint, but really just to make sure that the people involved understand fully what the expectations are of management.

Julia Allen: Well that makes a lot of sense, because like many things related to information security, it really does come down to the people and the behaviors and the actions. And so I suspect there are a number of ways in a senior leadership role that you kind of keep your eye on what's appropriate and actions you need to take if a corrective action is required. So can you maybe say a few things, say, give us a few ideas of some of the things that you do maybe on a day-to-day basis?

Paul Love: So for us, the people, process, technology, we look at the people and process more so than the technology. Technology is an important component, but specifically, we really focus on the people and processes to make sure that they are meeting the organization's objectives. So when I say people, we work with the organizational employees to make sure that they understand what the requirements are. So getting out there and getting out of our cubes and our offices and actually talking to people is very important to make sure that we expand on it. But also to work with the management to make sure that they're working with their teams to expand on their requirements as well.

Julia Allen: So for example, during like maybe the performance review cycle or during your annual planning processes, does the security policy come up in those kinds of forums?

Paul Love: Generally, if you can, yes. Typically, I've seen that it's not called out specifically, because it's really part of the organizational culture. When you have to call things out specifically, sometimes they lose their value. Some people may argue with that. But if it's generally accepted that this is behavior that's expected and it's part of the corporate values, it's not an event, it's more of a thing that you live. So the employees will follow it just because it's the right thing to do.

Julia Allen: Yeah, well, that makes good sense. I mean, I think the whole idea is to make security, if you will, invisible. Or stated another way, to just make it part of day-to-day practice, right?

Paul Love: Oh, absolutely. It's not anything that they should have to think about aggressively. But it is something hat should be on their mind. It should be integrated into the organization.

Part 2: Policy Structure and Life Cycle

Julia Allen: So let's turn our attention a little bit to the structure and the language around policy. So we hear about policies, procedures, standards, guidelines. All this terminology and structure can be, I think, a little bit confusing. So in your experience, what types of policy structures have you found to be the most effective, say from initial statement of policy to actually getting some traction in terms of action in the organization?

Paul Love: That's really a great question, because when I first started out in my information security career, there was a lot of conflicting information on the definitions of policy standards, guidelines, and procedures. And really setting that out, setting the initial what the documents are, even, was very difficult.

So in my career, I've used a simple set of definitions for an information security policy system. And this insures that I'm targeting the right particular document to the right internal customer. So we've broken down the differing documents into specific hierarchical sections. And I've generally used the policy standards, guidelines, and procedures that you had noted. And the definitions we use really help set the documents apart and help spell them out for the organization. So instead of having 150-page document that's supposed to cover all aspects of one particular technology or one particular process, you actually break it out into digestible chunks that the specific audience can adhere to.

Julia Allen: Isn't it the case the policy kind of at the very highest level should be kind of short, sweet, to the point and have a fairly lengthy shelf life?

Paul Love: Absolutely — 100% agree, because the policy should really be a simple statement from management — it's really management's intent. And when it's coming from management, you don't want to get into specific technologies or specific processes. You really want to keep it at a high level and identify the control objective.

So for instance, a high level statement that your most senior management can sign off on, for instance, "Information in transit or rest will be encrypted to prevent disclosure to unauthorized parties." This is really — it doesn't get into the specific technologies or how you're going to do it, but it really sets "Hey, this is management's intent, this is their requirements." And if you want them signed by the most senior management, you really have to keep it at a very high level and you can't change it every six months. Now of course, there has to be a process to modify as needed. But you want to keep it very high level, so that it has a long shelf life.

Julia Allen: Right. And with the example that you gave, often the underlying technology will change as it becomes more robust or more sophisticated and yet you are able to retain the same statement of policy.

Paul Love: Absolutely, and that identifies the management's intent, and that allows information security to play their role in consulting to the organization.

So some of the other definitions that we had, for instance are standards. We have standards as a supporting document set to policies. And these are documents that spell out the compulsory requirements that support the policies. They actually spell out the actionable requirements, not the step-by-step, but what the specific technologies, for instance, are. And they're interpreted usually by the information security team or the other subject matter experts. And that's really where you get to the more prescriptive part of the information security policies and standards program. So, for instance, on that policy that talked about information in transit or rest will be encrypted, the standard would actually start talking about specific types of encryption — that you would use AES, whatever, that are required to meet the objectives identified in the policies.

Julia Allen: And then do you have a kind of a companion example for either a procedure or a guideline following that same train of thought?

Paul Love: Absolutely, and generally what I've used is, the guidelines are generally noncompulsory but they're best practice recommendations, that if someone wants to exceed the minimum requirements — because standards and policies are the minimum requirements. The guidelines really tell you how to move forward if you want to be best-in-class or if you want to really excel what the general requirements are. And they're things that you do when they're feasible within business requirements.

And then procedures are really where the rubber meets the road, and these are the ones that should probably change fairly frequently and need to be updated and monitored. Because generally, these are where you have the step-by-step instructions on what activities must occur to meet the requirements and the standards and policies. So for instance, for the encryption part, if you were to use a specific type of encryption technology, you would start off with, "You install this on this system, then you press the start button, then you move here, you enter this information." So it's really very, very prescriptive and detail oriented.

Julia Allen: Okay. So I can see why those would change on a more recurring basis because those details vary from system to system.

Paul Love: Absolutely.

Julia Allen: So you've given us a real good framework to kind of understand some of the distinctions and differences and various roles. Do you actually have — in your experience, have you used something like a policy management life cycle approach, from maybe initial conception of a policy idea — perhaps building from ISO 27001, or coming from one of your legal or regulatory requirements — taking that through implementation and then kind of wrapping it back around to make sure that it actually continues to deliver value to the business?

Paul Love: Absolutely. That's a cycle I've gone through a couple of times. Usually for the initial phases, it's very important to either use your existing policies — if they've been updated and the organization feels pretty good about them — and identify gaps against an industry-recognized standard, such as the ISO. Another method is to start from scratch using an industry-recognized standard. Because again, trying to create policies in a committee forum I've found is very difficult

and it takes much longer. Whereas if you give the organization, or whoever is on your policy governance committee, if you give them a set of policies that have been vetted through another organization or are internationally recognized, such as the ISO, it really helps them focus on the things that are gaps or that they want to change, and not so much arguing the points that aren't necessarily as important.

So from there, close work with those affected by the policies, and the management that will approve the policies, is very important. Communications is probably the most important thing when working on policies, because if you haven't communicated it throughout the organization, it won't be effective.

So you really need to understand the risks associated with implementing or not implementing specific policies and communicate those risks to management, so that they can make an informed decision. In the end, they're the ones who are responsible to the shareholders or to the regulatory bodies, whatnot, for making sure that the information security program is effective.

So once a decision is made, we generally have communications across the organization, especially the key people that are impacted and the key stakeholders. So a policy that no one knows about is probably worse that no policy at all from an exposure standpoint. If you have a policy out there, now you've stated management's intent, but nobody knows about it. That's probably not a good situation, because management has expressed their intent, and you're being audited against it, but you may not have compliance. So communications again, I'll stress that again, is during the creation of the policy as well as after the policy is approved is crucial.

Another point is to consider what the role of information security should be within the policy life cycle. I've personally found that being an advisor and being in an advisory role in regards to policies is most effective. Because then you can have that open dialogue with people, with the employees of the organization to ensure that they are working within the confines that management has expressed, but that also you can consult and give them open and honest feedback. So that really means being available to answer questions about the nuances or the gray areas. And again, that builds a strong trusting relationship with your internal customers.

And then another thing is to always keep your business needs in focus while weighing risk tolerance levels. And the risk tolerance levels are defined by the information security policies if you've effectively communicated risks. So that's very important to the information security program.

And then some other aspects that you may want to consider is that after you have communicated, constant review and update of the policies is crucial to insuring your policy program is effective as well. And generally, you want to have this conducted on a scheduled basis. But you also want to make sure that you have a review when business conditions change or technologies change or some significant aspect of the organization has changed. So you really need to keep an eye on it. And I've generally found that six months is a good schedule time frame, But again, integration into the business is very important to insuring that you understand when business conditions change.

And then this is one that I've seen often overlooked is that a very important facet that is often overlooked is the creation of a process for exceptions. No policy is written in stone. Business conditions will change. You do have some regulatory requirements that probably can't change. But in general, some of the policies don't have regulatory or contractual requirements around them have to be able to bend according to management's requirements. So having an exception process for those instances is important for tracking and risk evaluation purposes. And these risk exceptions will allow you to present an overview to management of what exceptions they have allowed. So at the end of the year, whenever you report, they can see that they may have provided

exceptions for one particular policy element 20 times. So maybe the organization should change the policy or make sure to clarify what the intent is behind that.

Julia Allen: Well you know that policy exception process I think is really pivotal to all that you've described. Because if there's a business requirement or a business need that kind of supersedes, or if there's a risk situation that really requires you to take a departure, having a well-informed, communicated process for creating those kinds of exceptions I think is just essential.

Paul Love: And that's really key because it shows that you are working with the organization, you're not dictating what the requirements are. But you actually want to work with the organization in identifying when those business needs may require changes or modifications.

Part 3: Engage Users and Track Policy Performance

Julia Allen: So let's kind of go a little bit further with your communication emphasis because clearly, all of this requires people to be on board. What are some ways that you've found are effective for making sure all your users are adequately trained and kept up to date on their responsibilities with respect to policy compliance?

Paul Love: Constant, relevant, and engaging communications. Too often, information security professionals will rely on email or the non-personal engagements or posters or whatnot. Really engaging the end users and the employees is really important. So having an engaging dialog with users in multiple formats, not just email or whatnot, you can engage a customer and build a strong security awareness program.

And one technique I've personally used over the years and that I adhere to actually is to start by conducting training on a personal, non-work protection of information. So really show people how to protect themselves at home, for Instance, because most people will generally grab that and really want to understand. And they're interested in protecting their own information or their family's information. So that tends to pique their interest. And generally, employees will take the practices that you showed them for protecting their personal information at home and transfer those habits to the work environment. In fact, I've found that people will often embrace these to the point where someone who had little interest in security in the first place will begin openly identifying other security areas or bringing up concerns on their own work areas.

Another important component to a good security awareness program in my opinion is the engaging and interesting communications. Generally, the email, the chain that says "You will do this," we've found that people don't generally review those as regularly as we want, because they're getting those types of messages all the time. So you really need to change it up and keep it interesting. So you generally wouldn't want every employee to read every policy, for instance, as that typically will be an ineffective use of employees' time. So creating what I call digests of the policies that have specific information based on an employee's role, really allow the reader to target and gain information on what they want in a condensed form. So for instance, an example of this would be to create a subset of policies targeted at system administrators that would have policy standard statements for someone who administers a system, the things they would care about. Maybe one for developers, one for remote employees, etc. And then from there you'd create — I've found that creating banner ads for your internal website, yearly online multimedia training, some targeted emails with interesting messages, etc., to supplement these activities really help get the message across.

Julia Allen: Well when you think about how we all learn as individuals, a program like you've outlined that's targeted, relevant, germane to what it is I'm trying to do on an every day basis is something I'm going to pay attention to.

Paul Love: I would 100% agree. And especially that making it interesting to them, while as information security professionals, we're generally very interested in all aspects of information security, you really need to generally help your employees understand a little bit more and dig into the nuances. So personalizing it really helps, because they will get very engaged and very interested.

Julia Allen: Well Paul, this has been great. I have just a couple more questions that I would like to ask you as we bring our conversation to a close. I'm sure you're held accountable for the overall program. But what have you found are your measures of success for an effective security policy program, that part of your program?

Paul Love: Sure. Having an understanding of any deviations from policies and understanding the root causes of any deviations really help. As you evaluate if there's been a deviation from a policy that results in a security violation, understanding what the root cause — Did the end user know about the policy? Did they decide not to do it? Did their management support them not doing? — really getting to a deep understanding of exactly why there was a deviation. But also keeping good metrics across the board. So for instance, having an understanding of how many exceptions through your exception process were accepted by management, so that you can report to them at the end of the year. That'll tell you how effective. If you have a good set, a very well rounded set of exceptions, generally tells you that people are following your process.

And then having involvement in the organization, having people approach you. And not necessarily having them approach you in a concerned manner, but actually asking for your advice. That is a great way to tell if you are being a consultant or if you're more of a dictatorial, "This is what you will do." So having people engage you is probably a great measurement. But the hard measurements are the exceptions, understanding of deviations, and just generally how often people are actually reading your policies and asking you questions about them.

Julia Allen: Well that sounds very well advised. And I like your soft measures too because sometimes having people come up and make suggestions or ask you how to interpret a particular policy guideline they've been given is one of the best measures of success.

Paul Love: Absolutely.

Julia Allen: So where would you point our listeners for more information on information security policy? And do you have any sources that you recommend for perhaps sample policy language?

Paul Love: Well, of course, the CERT website has all kinds of great information in this regard. But also the SANS website has some interesting documentation on standards and policies. But the one I've really leaned on throughout my career is the ISO 27001 series. That really identifies some key areas and has a great building block for you to build upon. So those are primarily the resources I would recommend to people I talk to.

Julia Allen: Well Paul, I'm so appreciative of your time and your expertise. I think you've given our listeners a lot of things to think about and a lot of good resources. And I look forward to another conversation in the future.

Paul Love: It's really been great to be here, and I appreciate it.