

Information Compliance: A Growing Challenge for Business Leaders Transcript

Part 1: Information Compliance Overload

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 Tom Smedinghoff, an attorney and partner in the Privacy, Data Security and Information Law Practice at the firm of Wildman Harrold in Chicago. Today we'll be discussing information compliance overload and how business leaders can deal with this growing challenge. So welcome Tom, good to have you here today.

Tom Smedinghoff: Thank you very much.

Julia Allen: In your work, you talk about the proliferation of information security and privacy laws, regulations and standards. You also identify a wide range of issues and concerns that business leaders need to pay attention to. Could you describe some of the dimensions of this growing challenge that everyone's having to deal with?

Tom Smedinghoff: Sure. I think that generally we've got some competing trends going on. If you look at the way businesses operate today they're increasingly global or certainly crossing jurisdictional lines with increasing frequency. At the same time information security regulation, laws, compliance obligations and so forth, are increasingly becoming local. Whether it's at the different country levels or at the state level or even at the city level, we're seeing quite a wide variety of new and sometimes conflicting laws and regulations.

And I think we also see that these obligations, if you will, come in a variety of different forms. They may be laws, they may be regulations, they may be common law obligations, they may come from contractual requirements, from standards that apply to particular transactions, from system's rules; in some cases they're even self-imposed by the parties, depending on how they run their business. But they're coming from many different forms and they're coming from many different jurisdictions, as I mentioned, state level in the U.S., the federal level, the international level. Sometimes they're pushed down by trading partners who want to impose security requirements and so forth.

And then I guess finally they cover an increasingly diverse set of issues that require some sort of compliance activity. You have obviously privacy concerns and regulations, security concerns. We see breach notification laws. We see the credit card processing requirements from the credit card industry, which some states are now starting to use as the basis for laws that they are enacting. We see laws governing the use of Social Security numbers, laws regulating the use of RFID (radio frequency identification) devices, spyware laws, laws governing record retention, record destruction, identity theft, pretexting, electronic transactions and so forth and so on. Just the number and amount and the breadth of the issues that we're starting to see regulated just keeps growing, almost at an exponential pace.

Julia Allen: It seems like a fairly daunting challenge just to get your head around what you're responsible for.

Tom Smedinghoff: It is. Just the sheer number of different regulations and rules that you might be subject to is a major problem. And I think it's also compounded by the fact that many of these laws and regulations are somewhat vague and it's not entirely clear what it is you have to do, and in some cases they conflict with one another. What one state may require may conflict with another, what the U.S. requires may conflict with what the EU requires and so forth and so on. And they keep coming at us at a fast pace, and so it makes it a very difficult challenge, to say the least.

Julia Allen: What in particular – and you mentioned international considerations – what do you see are some of the nuances or maybe some of the particular challenges when dealing with global supply chain or customers around the globe? Are there some special issues there?

Tom Smedinghoff: Well I think first and foremost is just the sheer quantity or volume of regulatory requirements that you may have to deal with. Privacy is perhaps a good example where the European Union regulates the use of personal data much more thoroughly than the U.S. does, and to the extent you're dealing on a global basis and you want to transfer that data back and forth, you've obviously got to deal with those issues.

We also run into a variety of conflicts. One that has perhaps gotten a lot of publicity recently is the conflict between the U.S. requirement under the Sarbanes-Oxley statutes that companies have to have a whistleblower, an anonymous whistleblower capability for employees to report on executives who might be doing something wrong, and the EU Privacy Directive and the country implementations of that directive, which basically prohibit such kind of conduct.

Now we've seen some movement in terms of reconciling those two, but that's just one example where complying with one set of rules may mean violating another. And it really does, I think, raise a lot of challenges for businesses that are trying to do business in a variety of jurisdictions, especially when they're transferring information across those jurisdictional borders.

Julia Allen: So given, if you can kind of for a moment set aside the conflicting requirements, what have you seen in your practice and in your interactions with your clients, some of the major risks and consequences of non-compliance?

Tom Smedinghoff: That is going to vary, I think, quite a bit from jurisdiction to jurisdiction. There seems to be an increase, however, in the level of enforcement in a variety of different areas. Some of the EU jurisdictions – and I want to say Italy, Spain and Germany come to mind – tend to, I think, do more in the way of enforcement on some of their privacy regulations than some of the other countries.

We're seeing the FTC (Federal Trade Commission) in the U.S. talking about stepping up its enforcement activities, particularly with respect to its current view that failing to provide adequate security for personal data is an unfair business practice and that companies are going to be held accountable for that kind of activity.

Also if you look at what's going on in the U.S., particularly in light of some of the recent high profile security breaches, we're starting to see a lot of litigation. Several class-action lawsuits were filed against the TJX companies, for example, in connection with their data breach. Same thing we saw with Choice Point following its data breach. And we're starting to see the courts recognize a common-law duty to provide security. And they're just starting, I think, to enforce that, and we've got a handful of cases at this point. But I think we're only going to see more as time goes on.

Part 2: Who's Accountable?: Board Directors and C-Level Executives

Julia Allen: That makes sense. So what have you seen in your client organizations as to the roles in the organizations who are responsible for tackling these issues and making sure that the business is adequately protected?

Tom Smedinghoff: Well I guess the first thing I would say there is that I think the trend in the way the law is developing here is to shift the responsibility basically to the Board of Directors. And what we're seeing is a change. What was typically thought of as an IT department issue is really becoming a corporate governance issue, and there's increasing recognition that information security is an issue that really needs to permeate the entire organization, with responsibility going all the way to the top.

So what you're starting to see, and I think we're going to see a lot more going forward, is Boards of Directors, as well as the C-level executives, taking a much more active role and responsibility for ensuring that the company has implemented adequate security. And I think we're going to see more and more that they'll be held accountable if they fail to do that.

But I think there's also – inherent in that is a recognition that every aspect of the corporation needs to be involved. Again you can't just delegate it to the IT folks. It's something that all the different lines of business, all the different departments need to really recognize as part of their obligation and that everybody is sort of in this whole thing together.

Julia Allen: So it sounds like, I know for those of us in the information security profession, it can sometimes be a fairly daunting undertaking to get top level executive and board attention to the issue. So would you say that this particular set of compliance requirements and laws and regulations is starting to heighten awareness at the senior level?

Tom Smedinghoff: I think we're starting to see that. In fact I just participated in a panel at the National Association of Corporate Directors where in fact that was the subject. And I think there is an increasing recognition that this has to be where the responsibility lies. And so, like I said, some of the laws are starting to do that.

But having said that, I think we've got a long way to go. I think there are a lot of boards where this really isn't on their radar screen yet. And there needs to be a change in thinking on this and there needs to be a more across the board recognition that this is a serious corporate governance issue. It's not just an IT issue.

Julia Allen: What would you say or what have you seen as the role that legal counsel can play in helping raise the awareness, raise the profile, help senior executives assess the risk in this area?

Tom Smedinghoff: Well I think fundamentally what we're seeing is that information security is now a legal issue. There's no question about it. It requires legal attention, it's a legal compliance issue, as well as obviously a liability issue, should a problem arise. And so from that perspective legal counsel absolutely needs to be involved in the process. Obviously legal counsel isn't going to necessarily be deciding what security measures need to be implemented or how the company needs to respond, but legal counsel needs to be actively involved, from the perspective of focusing on compliance, focusing on the legal risk that's inherent in this whole process, and sort of helping the company figure out what it's going to do and how that relates to its legal obligations to try to make sure obviously that the two mesh well and that the legal obligations are adequately addressed.

Julia Allen: One of the things we've really struggled with in our governance work is where does this set of issues – information security and privacy, risk and compliance issues – where do they fit, given all the things that, for example, that legal counsel needs to pay attention to, senior executives, boards of directors? They are clearly trying to run a business. So do you have a sense or kind of are you seeing any kind of rules of thumb for where this, if you had to rank and stack priorities, where this one shows up on the list?

Tom Smedinghoff: Well that's a tough question to answer, in part because I think it's going to vary from organization to organization. For example, businesses that are highly regulated in this area or that really depend very heavily on information as the lifeblood of their operations, for example, financial institutions, this has got to rank very, very high.

Other institutions, other businesses may find that it's not quite as critical. But on the other hand, I think today we're getting to the point where all businesses, regardless of what they do, are in a position where they really are totally dependent on information technology and networked communication systems and so forth. And if there's ever a problem it really creates a significant potential vulnerability.

The question I think each business has to focus on is how significant is that? And depending on the significance to the business that in part is going to depend on how they rank it in terms of its importance. But there's another dimension to it, which we're increasingly seeing, and that is that there's a focus on the stakeholders here, the investors, the shareholders, the employees, the customers, the suppliers, other third-parties who are increasingly impacted by a company's lack of security or breach of security. And so you really have to focus on what's the impact to those stakeholders, because the bottom line is that that's, I think, one of the key drivers here.

Julia Allen: Well information has become clearly the lifeblood and our infrastructure has become the transport mechanism for that. So we're all connected and we're all equally vulnerable I think to a greater or lesser extent.

Part 3: Effective Steps to Get Started

Julia Allen: Turning our attention to what business leaders can do perhaps to get their heads around this and to take constructive and diligent action, what have you seen are some of the first steps or some effective steps that they can take to address these requirements and risks and put a compliance program in place that will stick?

Tom Smedinghoff: Well I think first of all businesses need to recognize that information security compliance is a process. It's not satisfied by implementing a particular product. It's not something that you do once and you're done. It's a never-ending process that involves risk assessment and evaluation and response and re-evaluation and so forth.

Just to get the process off the ground you've really got to start with some very basic issues, what I call starting with the facts, which are basically identifying what kind of data do you have and how significant and sensitive is it, and who has it? Is it in your possession or is it the possession of a third party who might be a service provider for you? And what are you doing with it? Who owns it, who has access to it, where is it stored? Some very basic questions about your data.

From there I would ask as a second question what are you doing with that data? Look at its life cycle. How are you collecting it or acquiring it or creating it? How are you using it? Is it internal, is it used for marketing purposes, and so forth and so on. How are you communicating and storing it? What are you doing with it vis-a-vis litigation, for example? How are you destroying it? Sort of that

whole life cycle look at your data, because this is going to raise a lot of the issues that we see in the laws and regulations in terms of how you acquire, for example, personal data – where you can acquire it from, where you can transfer it to, what you can do with it, how you have to destroy it and so forth. But you can't really respond to those requirements until you know what you've got and what you're dealing with.

And then the third step in that process, this very initial process I would say, is okay, now that we know what data we have and how sensitive it is and what its life cycle is, from our perspective what laws apply to it? What laws apply to the data, what laws apply with respect to what I want to do with that data? For example, the Social Security number laws are going to restrict how I can use Social Security numbers. The Data Protection laws in a variety of countries are going to restrict how I transfer that data, and so forth and so on.

And then we've got to look at what's the likelihood of non-compliance, what's the penalty and the risk for non-compliance? And then we have to do some prioritizing. And I think it's important to recognize that especially for companies doing business in many different jurisdictions, it may well be impossible or prohibitively expensive to figure all of these questions out to the ultimate level of detail.

But I think you've got to start with those three basic questions: what data do we have, what are the attributes, what's the life cycle, what are we doing with that data, and then what laws apply to it and how do they affect our operations? You've got to start with those basic questions, at least at a high level, and maybe you focus on the jurisdictions – where you do the most business, for example – but you really have to start there and get a handle on what the situation is before you can decide how you need to respond.

Julia Allen: And what additional concerns might arise or steps might you take when you consider the fact that we all work with partners and collaborators and suppliers and vendors in our supply chain, where information is shared and flowed across that entire, if you will, virtual enterprise? Are there special steps or considerations there for information sharing?

Tom Smedinghoff: Well I guess in general I'd say you need to start with the understanding that if the data is yours or if it's your responsibility it doesn't make any difference who has it. You still have to protect it. You're still responsible for dealing with the legal requirements for that data. And I think with that view you've got to then, moving forward, when you're getting into situations where you're going to be sharing data, where you're going to be outsourcing data or whatever, you need to look carefully at who are you working with, how trustworthy are they, what kind of procedures do they have in place, what kind of contractual requirements might be appropriate, to make sure that they protect the data to a level that's appropriate for your needs, because if it's your data you're still responsible for it. And then you need to sort of monitor what's going on, making sure that people who are accessing your data or possessing and using and processing your data are in fact doing what they're obligated to do.

Julia Allen: Well that makes good sense. I think you've framed the issues very clearly and I know that our listeners will benefit from this discussion and hopefully if they aren't taking action this will help give them some ideas of ways to get started. Do you have some particular sources that you like, either websites or other sources, where our listeners can learn more about this issue?

Tom Smedinghoff: I know that CERT has a lot of materials on its website and they've been very helpful. I have an article that lays some of the framework issues out that's on our website at wildman.com. But other than that it's a matter of trying to keep up with what's happening and look at the big picture, I think.

What I find when you look at laws and regulations is that they often tend to follow a pattern, whether it's Social Security laws or breach notification laws or whatever. And so I tend to put, at least initially, I tend to put less emphasis on the differences of all the individual laws and more emphasis on understanding the framework of each type of regulatory scheme, because that will, I think, help you in the long run in terms of complying across the board. And that's the kind of thing that you get more from articles and analyses of the statutes than you do by reading 50 different state statutes, for example. So I don't know if that's helpful but I think sometimes that's a good way to approach it.

Julia Allen: Well again I'm very, very appreciative of your time and your expertise. This is a critical issue that I think most organizations are dealing with. So I really do appreciate your remarks.

Tom Smedinghoff: Okay, well thank you.