Why Leaders Should Care About Security
Transcript

Part 1: Why Should Leaders Care About Security?

Bill Pollak: Welcome to the CERT Executive Podcast Series. The CERT program is part of the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at Cert.org. Before we begin, I'd like to let you know that show notes and other supporting materials for today's conversation are available at the podcast website. Please take a few minutes to look these over.

My name is Bill Pollak and I'm the Manager of Communications for the SEI. Today, I'm pleased to introduce Julia Allen, a senior researcher at CERT and a recognized leader in security governance and executive outreach. We'll be discussing why security is an executive's problem. So, Julia, let's begin.

Julia Allen: Great, Bill, I'm looking forward to it.

Bill Pollak: Okay, so why should executives care about enterprise security?

Julia Allen: Well, if you take a look at what's happening to breaches, information security breaches in the press and the kinds of exposures that organizations are enjoying, if you will, information is really being viewed more and more as a critical asset in organizations -- almost like money. So some of the ways that we introduce the topic of enterprise and information security to executives is to ask them to think about situations such as what happens if their customer data is stolen or disclosed, and this is on the front page of the New York Times or the Washington Post? What happens in the case that their customers lose confidence because they've become aware of a security breach? What happens when strategic plans, key trade secrets or intellectual property get into the hands of their competitors? And of course the one we're all familiar with when we try and go and access a site or get to an organization is they're not available, their site's not available or they're having an instance of down time. All of those occasions as they occur and show up at the consumer or the customer end are one of the ways that executives seem to be able to grasp that this is something they should pay attention to.

Bill Pollak: Okay, so it sounds like you're talking about something beyond just compliance with the law.

Julia Allen: Right. Many organizations come to security through a compliance door; in other words, some regulation or law is imposed upon them and they take action and tend to approach it more like a checklist exercise: "If I pass my audit, I'll be fine." Organizations that are handling this problem much more robustly and much more from a strategic point of view are understanding the importance of information assets, their infrastructure, their customer databases, their trust, their reputation in the marketplace, and so instead of coming at this from a compliance point of view, they're understanding what kind of protection strategies they need to put in place and then almost as a fallout or as a result of that kind of attention, they're meeting their compliance requirements.

Bill Pollak: Oh, okay. So it goes beyond just the minimum.

Julia Allen: Right, right, at least the organizations who are doing it well and not struggling with or incurring the cost of every new set of regulation that comes down the pike.

Bill Pollak: Great. Well, let's talk about a specific instance. The incident with ChoicePoint was in the news in 2005. Can you tell us a little bit about that and why you think executives ought to pay attention to that whole situation?

Julia Allen: Sure. The ChoicePoint case was kind of a landmark case. What happened was that a new customer of theirs was able to fraudulently access information, customer data and other client information. And the reason that this was a particular landmark case -- over a hundred thousand customer records were exposed in this particular compromise -- is because this was the first visible case where California Senate Bill 1386 that requires organizations to notify residents of California when their information has been put at risk, that's what made this a particular landmark case. And so what ChoicePoint got to enjoy was basically being the first icebreaker, if you will, for the interpretation and prosecution by the Federal Trade Commission.

Bill Pollak: Perhaps enjoy is the wrong word.

Julia Allen: Yes, yes, enjoy at least in terms of, you know, probably more visibility and attention than you ever wanted. And what the FTC found was that they were really negligent in not doing appropriate background checks and due diligence on a client that contracted to do business with them before they actually gave away, if you will, the keys to the kingdom.

Bill Pollak: Okay. So are there other examples that you might want to cite?

Julia Allen: Well, it's really interesting. I just ran across a new -- new to me -- a new website this past couple of weeks called Privacy Rights Clearinghouse. And what they've done is they're actually tracking the chronology of all citizen information breaches since the ChoicePoint case. And they've documented over a hundred that occurred in 2005 after the ChoicePoint settlement and in this year alone just through June over ninety. And so some of the cases that they highlight … I think most of our listeners would be familiar with what's happened recently with the Veterans Administration, where over twenty-six million records of veterans since 1975 -- and an additional two million records of reservists and active duty personnel -- were unfortunately on a laptop that one of their employees took home to do good and legitimate work and that laptop and the hard drives were stolen. And so that case has certainly put the whole Washington…

Bill Pollak: So each of the folks whose names and information was exposed there had to be contacted, right?

Julia Allen: Well, they had to be contacted. I mean clearly, there's again more press than probably the VA ever wanted to experience, at least in this case, and now a large number of veterans groups have initiated a class action suit against the VA with all kinds of claims and ramifications. And one of the senior executives at the VA has been reported as saying that they think it's going to cost them over five hundred million dollars to recover from this particular incident.

Bill Pollak: And that's not to mention the reputational damage, which is difficult to quantify, but still extraordinary.

Julia Allen: Right. We talk about -- in some of our governance work we talk about this whole issue of trust and reputation and how difficult it is to build trust and how just in an instant, as evidenced in this case, how easy it is to lose.

Part 2: Why Is Security a Governance Issue?

Bill Pollak: So you talk in a lot of, you know, your written work that I've read, a lot about governance. And can you kind of make the connection for me between what, you know, most of us think of security on the one hand and governance on the other? What's the relationship and how would you define and characterize governance?

Julia Allen: Sure. Governance historically has come out of the financial side of an organization, governance over the financial reports and the financial records and the financial transactions. We're really trying, and actually, a lot of communities are trying to broaden the definition of governance to really talk about setting explicit expectations for the organization and then making sure those expectations are fulfilled, so oversight, directing and controlling, setting an appropriate tone at the top, helping establish the proper cultural norms, the ethics and the values of the organization. So the tie to security is that we, in the organizations that we've worked with and our observation of what's going on and who's doing security particularly well, is that it's a cultural norm. People understand what's expected of them, they understand they're going to be measured based on this, they understand that they are the custodians of the information that is given to them on behalf of their customers. And so where governance comes in is basically setting that oversight directing and controlling structure in place so that the business can conduct itself consistently with respect to protecting information.

Bill Pollak: And that becomes a matter of really managerial strategy beyond just, you know, compliance, right?

Julia Allen: Right, it becomes a question of strategy, business goals and objectives, critical success factors, identifying the critical -- in this case -- information assets, and then making sure that security is part of the normal day-to-day business flow, the processes, the conversations, the management and staff meetings, the quarterly reports. So that recognizing that executives have a great deal of demand for their time and attention, getting security into the mainstream of how they conduct business is really an act of governance.

Bill Pollak: So let's go back to ChoicePoint for a moment. Suppose that ChoicePoint had treated security as a governance concern. How would what happened to ChoicePoint have been prevented? What would that have looked like?

Julia Allen: Well, it's hard to say if it would have been prevented or not, but it certainly could have been mitigated in some regard. A particular case in point is the Chief Information Security Officer at ChoicePoint only felt that his responsibility was digital security and viewed this whole situation as a case of identity fraud because it had to do with somebody coming in fraudulently and establishing an account. So there was a disparity, a disconnect between what you normally might consider to be information security, more IT technology-based, and maybe more physical or fraud types of investigations which were really handled by the Chief Security Officer. So

where governance could have played a role, and one of the things we talk about in our practice's recommendations is this kind of integration or this convergence where you bring all the different parts of the organization together, in this case digital, physical, legal, human resources, or whatever part of the organization would do the necessary background checks, audit to make sure your particular controls were in place, and you actually integrate these and create forums where these different parts of the organization that all have a part to play can converse and interact and explore and examine. And chances are, you know, even if they didn't have the right controls in place on the front end, it might have helped them get through the pain process a little more effectively.

Part 3: Competitive Advantage, Duty of Care, and Who's Responsible?

Bill Pollak: Well, let's kind of turn it around. We've mostly been talking in the negative here up until now, but, you know, it's also the case that doing governance effectively could provide a competitive advantage to an organization, and maybe we could talk about that.

Julia Allen: Sure. Folks don't typically think about information security as a competitive advantage, but if you consider that fact that if you put particular security controls in place, you may be able to do global business more effectively because you've got a global supply chain. You may be able to access competencies in products and services in whatever you offer to your end customer that takes advantage of the fact that you can communicate twenty-four seven around the globe. There may be ways that you can, by being known as being a good custodian of your customers' information and that they feel safeguarded and protected and that they trust that you're going to handle them properly, that that in and of itself creates word of mouth if there are competitors in your particular market segment, but you're known as being particularly trustworthy or not having a significant number of cases of identity theft or putting your customer data at risk. So there is a variety of ways or perhaps new business transactions, new products and services that you can bring to market because you treat the information that those products and services handle and convey in a very effective and foolproof and demonstrable transparent manner so that the marketplace knows that you're going to take good care of them.

Bill Pollak: Yeah. What comes to mind for me is, you know, if you think of safety for an automobile company, immediately the word Volvo jumps into your mind, you know?

Julia Allen: Absolutely.

Bill Pollak: And so you can imagine that for an organization that's dealing with information that it could be a branding exercise for the organization to really try to brand itself effectively.

Julia Allen: Right. Well, for example, if you look at what eBay has done with PayPal, interestingly enough, PayPal or adding that as part of the eBay service suite was not part of their investment banking recommendations. It came from their customer base. They said we want an easy, foolproof, satisfactory way to be able to transact our auction business, and so eBay bought PayPal. And, you know, I don't have any numbers on this, but I would hazard to guess that a big part of what draws customers to eBay is because they know that their financial transactions are well protected.

Bill Pollak: Right. So I've seen the term in some of your written work, duty of care. Can you tell us what that means?

Julia Allen: Sure. In the regulatory and legal space, if you will, some of the compliance and liability areas this term comes up, duty of care, that which a reasonably prudent person would expect. So, for example, if you're in the healthcare sector and most of the leading organizations in the healthcare sector by example include information security as part of their business continuity plans. If you were a provider in the healthcare sector, you would be expected to do the same and demonstrate that if you ever found yourself in a legal proceeding. So it really means that you're just taking care of, you're doing what the norm, what would be minimally hopefully more than that, but minimally expected of others in your market sector, and you're actually getting back to this notion of custodianship of information. You're doing the right thing and you're doing it for that reason alone, not because you necessarily plan to make money from it, but that you know that that's the right corporate thing to be doing.

Bill Pollak: It's the corporate responsibility in a sense.

Julia Allen: Correct. Correct.

Bill Pollak: Okay, well one last question, Julia. Whose responsibility is it really to protect digital assets? The Sarbanes-Oxley Act, you know, might indicate that it's the CEO who has to sign off on company financial statements, but what are your thoughts on that?

Julia Allen: Well, as I mentioned, one of the big areas of best practice that we've seen is this notion of bringing all the parties to bear in appropriate forums so that audit and HR and legal and your risk management, your privacy organizations can play their part. Clearly, the buck stops at the top. The CEO has a critical role to play in terms of accountability for information security, and actually, the Board of Directors have a role to play in their oversight and making sure that proper policy and procedure is in place in the organization. But accountability doesn't necessarily mean all the implementation responsibility. So we would expect to see Chief Executive Officers turn to like if risk is a big issue or advantage in the organization, turn to their Chief Risk Officer or their Chief Privacy Officer. Certainly, the Chief Information Security Officer plays a significant role, and ultimately, the folks that run your IT organization and their security functions have "where the rubber meets the road" implementation responsibility for security controls. But in terms of making sure that it actually happens, that really lives at the top of the organization, or in terms of any kind of steering council or management group that the CEO might set up to help them orchestrate this through the organization.

Bill Pollak: Okay, and so what would be your one final message that you would want to leave our listeners with, and maybe if some of the things you have said have motivated them to make some changes, what steps would you suggest that they take first?

Julia Allen: Well, I think the real message that we're trying to communicate here is security-conscious leadership. In other words, whether leaders choose to take security action or not, at least have that be a conscious informed act, and in having the level of security in their cultural behavior and norms appropriate to whatever their risks and exposures are. So I would say that leaders really need to treat security, or

at least adequate security, whatever they defined adequate to be, as a nonnegotiable requirement of being in business and do what's necessary to look at this hard. In terms of next steps, do an effective risk assessment, take a look at what your critical assets are, where those assets are exposed, rank and stack the protection strategies to help mitigate the high-profile risks, create the councils to help manage and control and take the necessary action, and then measure, measure, measure. Don't just put the initial action in place, but put the follow-through in place so that you can know how you're doing. We've looked at various approaches like Balanced Scorecard and various types of management dashboards, which is probably another conversation, but where you can actually get some insight at a level that leaders can deal with it and integrate that with the other important success factors and objectives that the organization is trying to meet. We have a lot of materials on the governance portal on the CERT website, so I would point our listeners to that material.

Bill Pollak: Absolutely. There's a wealth of information on the CERT website so I would echo that thought. Well, thank you. I enjoyed the conversation very much.

Julia Allen: Okay, Bill. Thank you.