Protecting Information Privacy: How To and Lessons Learned
Transcript

Part 1: Why Should Privacy Be on A Business Leader's Radar Screen?

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 web site.

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 Kim Hargraves, Director of Trustworthy Computing Strategy for Microsoft. Today we'll be discussing the growing importance of privacy and how to develop an effective privacy program. So welcome, Kim, glad to have you with us today.

Kim Hargraves: Thanks Julia. I'm glad to be here.

Julia Allen: So what has put privacy on the radar screen for business leaders, and what are some of the most challenging issues that you see facing organizations today?

Kim Hargraves: Well, I think that with the increases in digitization of personal data, and the globalization of economies, and how that information flows within and across borders and between organizations, privacy continues to really be a growing concern not only for businesses and governments but also for consumers as well. And I see that this topic really has been a focus within specialized parts of organizations for years just due to the need to comply with regulatory requirements and things like that.

But now we're starting to see the convergence of this topic really at the C-suite (chief executive) level. And I think the reason for that is that the implications of poor privacy practices can really directly lead to the erosion of trust and ultimately, potentially impact revenues of organizations. And so I think that much of the rise to the top for privacy is a result of a lot of these highly publicized data breaches that we're seeing. And if you look at some of the figures, more than a hundred million users have been affected, or individuals have been affected to date.

Julia Allen: So when you talk about globalization, and the fact that, and I'm sure this is true in your endeavors dealing with global supply chains, I suspect that has kind of also caused the whole privacy issue to be elevated, right, because everybody's got different concerns and requirements?

Kim Hargraves: Yes, absolutely. And I think one of the challenges that organizations face today is trying to reconcile the different privacy legal regimes across borders between the U.S. and Canada, Europe, certainly Asia. I think that that's a significant challenge to try to figure out what is the bar from a legal perspective because we're a global organization. But then you have to overlay on top of that, "Well, what are our customer's expectations," because while there may not be a legal requirement in a certain country, we're pretty certain that individuals in those countries still may expect some level of protection of their personal data.

Julia Allen: That makes sense. So you've got, obviously, you've got the legal and compliance issues, but probably more important what the market is going to do if you aren't handling their data properly.

Kim Hargraves: Absolutely.

Julia Allen: So clearly there are common concerns when you're addressing both information security and information privacy, and I hope we have some common solutions. But in your experience what makes privacy unique? The two topics tend to get brought together in a lot of different discussions, but privacy really is different, right?

Kim Hargraves: Yes. Yes. I'm sure many of you listening have heard that you can have good security without good privacy but you can't have privacy without good security. I think where the common intersection point then is that on the security side, of course, security vulnerabilities ultimately can lead to the breach or inappropriate disclosure of personal information, and, of course, that impacts the privacy of an individual.

But where they're really different is that from a privacy perspective, you have to consider a broad range of topic areas. How that customer's data or individual's data is used. And that more goes to the root of business practices, business processes, and the choices that individuals in organizations make when they're interacting and using personal data, respecting an individual's choice when they've provided that data to the organization — how they've told the organization they want that data used or not used. And so I think there's a lot of business process issues, particularly, say, in the marketing space, or with human resources and employee data that are broader than just securing an IT system.

Julia Allen: So would it be fair, or perhaps too simplistic, to say that when I think about security I think about controls of various types. But privacy, you have to think about the controls but you also have to think deeply about the content, right?

Kim Hargraves: Yes, absolutely. Controls, obviously, are essential, across not just the systems but the business processes, again, as I said. But it's, a lot of it goes to the intention of use, and what is the individual and the organization who's gathering this data, what is their intention of use. Is it consistent with the organization's privacy principles and privacy statements which in turn are generally aligned with legal and regulatory requirements? And so once you're following an organization's policies you can pretty much be assured that you're going to be in compliance with laws and regulations around the world. But it's a difficult thing, I think, to think about because there's much more of a human element involved and much more opportunity for error.

Part 2: The Benefits of a Privacy Risk Assessment

Julia Allen: So we know that most organizations don't have sufficient resources to ensure 100 percent privacy. So I know that you've done a lot of work in privacy risk assessments. So how could such an approach help sort out what risks to mitigate and what risks to accept?

Kim Hargraves: That's a great question, and I have to say I'm really excited about the risk assessment work that Microsoft has done in the privacy area. And I think that what we've seen is that a risk assessment program, as a part of a larger risk management strategy, when it's used appropriately can really be a fabulous tool to identify your risks, capture those, have a methodology in a way to prioritize those risks that makes sense to the organization.

And when I said, "When you do that appropriately," what I meant was that if you can do that in a collaborative manner, and you involve the right stakeholders from across the organization who are the ones that have control over the purse strings to reallocate their resources to take on the most important risks to their organization, and you align those with their business objectives, you can get

a long way towards coming up with a really comprehensive set of prioritized risks that reflects the needs of the organization. And then the organization can take action on those things.

And once you have that organizational ownership even though maybe a central group, like in Microsoft our Trustworthy Computing Group, facilitates this risk assessment program and strategy, when there's business ownership, that's when the impacts can really get made in the organization. That's when change can really be effective and be made, and you can see the results of that through great risk mitigation strategies.

Julia Allen: So how have you been able to get business leaders, and owners, and information owners to enthusiastically engage with the risk assessment process?

Kim Hargraves: That's an area where we have had to, through trial and error, find ways that work. And in an organization like Microsoft where there's diverse business groups, and you have differences between what I would call shared services organizations like HR (Human Resources) and Finance that sort of serve the whole company versus individual business units that vary — business practices vary differently — where you have organizations developing software that gets sold in a boxed product versus online services versus consumer products like Xbox. You have to really spend some time understanding the organization, knowing the differences in cultures within the pockets and how they work, and be willing to adjust your risk assessment program because one size doesn't fit all.

And so I think one of the ways we were successful in getting folks to enthusiastically accept this program and get onboard is, again, to be willing to understand their business, tie their business objectives with the value that the risk assessment will bring to them, and then work with them in a collaborative way to tailor the action plans that would fit within how their business operates. I think those were really the key elements for success for us.

Julia Allen: So it sounds like you've really gone the extra distance to make sure that the privacy issues and concerns, and actions that need to be taken are really framed in business terms.

Kim Hargraves: Absolutely.

Julia Allen: So here's one I'm kind of curious to hear what you have to say. We hear about all kinds of risk assessments – financial, capital, operational, obviously, information security and now we're talking about, some would say, yet another risk assessment for privacy. Have you found effective ways to either tackle all of these in some integrated way or deal with the fact that there's many dimensions to assessing risk at the enterprise level?

Kim Hargraves: There are very many dimensions and I think that from my perspective Microsoft as an organization is starting to mature in this area. But one of the things we've done is adopt an ERM strategy or an Enterprise Risk Management strategy. And what that has done for us has allowed us to really place the right risk assessment activities with the right level and the right areas in the company. And so for those of you who are familiar with ERM which comes from a COSO framework, there's really four areas. There's financial reporting risks, operational risks, legal and regulatory risks, and strategic risks. So what that does is it allows the organization to kind of break those things up into meaningful pieces that can be looked at at different levels.

And so if you think about privacy risk assessments then really what my goal is as the owner of that program for the company is to be able to define, "Okay, there's some strategic privacy risks. Clearly there's a lot of operational risks and there's also some legal and regulatory risks." So I view

it as my role to have that information available in a way that then those risk pillar owners can take that and input that and add that to their assessment program.

Julia Allen: Okay. So then those all get rolled up at some level as they move up and through the organization so that, again, they're framed in a common business way.

Kim Hargraves: Right. And one of the things I'm really excited about as I watch Microsoft mature in this area is that, in a longer term view what you'd be able to do is for an individual business owner, let's say HR, you would be able to go to one place and see, "Okay, I have a bunch of risks that I need to manage as a leader in the company, and some of them are going to be strategic and some of them are going to be operational, etcetera." But you can look at them all in the context of "This is my risk universe. Now what's the most important to me?" Versus having individual domain experts – security, privacy, employment law, whatever it might be – coming to you and saying, "Well hey, the sky is falling. This is my top risk of the day." As a business owner you want to be able to look at those things much more holistically and be able to prioritize across those different domains and disciplines. And I think that ERM is one way that would allow an organization to do that.

Julia Allen: Well and it sounds like have confidence then, as you said, that their entire risk universe is described in a common place. And so if they tackle that, they don't have to worry about something being missing.

Kim Hargraves: Right, right, right. And like as a company, I mean, we're not there yet. ERM is a tough thing to do but we're on the right track and I can see this vision for the future where this is really impactful. It's already impactful today and the more robust we get at this the more impactful it will be for business owners to make decisions.

Part 3: Lessons Learned

Julia Allen: So based on your privacy risk assessment results, and others that you've seen use privacy risk assessments successfully, what have you found to be the most effective approaches for putting a program in place that you can sustain? And maybe throw in some lessons learned or pitfalls to avoid.

Kim Hargraves: Sure. I think that, as I mentioned earlier, one of the things that I've found that we have to be in our program as we're implementing it, is that we have to be flexible because there's different business units that operate differently. And then there's shared services organizations that support the whole company. And so we have to figure out kind of the best way to implement privacy practices across those varying organizations.

And so I think some of the lessons that we've learned that are really important that hopefully are applicable for other organizations as well, is that you have to start off with a basis. And people have to understand the domain and the subject to some extent. And if we talk about privacy explicitly, training employees and others in the organization is really important.

And so one of the key success factors I believe that we've had is that we've developed some role-based training, so that we have a Privacy 101 that any employee in the company can take. But we also have a fair degree of more specialized training courses so that if you're somebody in product development, if you're somebody in marketing, if you're somebody who handles databases with a lot of personal information, there's specialized training courses for you so that it makes it much more relevant for that employee in their job and what does privacy mean for them. So that's one area where I think it's just shown that it's absolutely critical to have that.

The other thing I think is using this risk-based approach to define our privacy strategy in the company and then aligning that with the businesses' objectives has been really critical. But then further taking that down to say, "Okay, where there's privacy functions throughout the company that support a specific business area, we also want to make sure that their goals and objectives are aligned with the corporate strategy." So I think the alignment piece is also really key.

Julia Allen: And would it be fair to say that some of the pitfalls or challenges are not having some of those connections made and some of those tailored training programs in place, or would there be some other challenges you'd want to mention?

Kim Hargraves: I think that some of the other challenges - yes, absolutely to the question. That's a pitfall to avoid – would be not aligning, going out and saying, "Okay, we're going to do privacy because we have this legal and regulatory compliance issue to deal with and this is what we're going to do." It just doesn't work effectively that way.

Another pitfall I think that's important to avoid is not trying to do this in a silo. There are so many other organizations in the company that you have to partner with and deal with on a regular basis that will help you implement and sustain your program. If I think about information security, network security, internal audit, there's some folks out there who can be really great partners from a privacy perspective – that if you are not working with those groups today you may not be as effective in your programs as you could be if you've got deep collaboration, and kind of day-to-day consulting and working together on common projects and programs.

Julia Allen: Well, that's great information and great input to others who are struggling with trying to put a privacy program in place. As we bring our conversation to a close I'm reading that, and you mentioned some of your role-based work in training and outreach, that you've done some work, some survey work and collected some pretty interesting information on the different role perspectives when people are collaborating to protect personal information. Would you like to just touch on that briefly?

Kim Hargraves: Sure. In October (2007), we released the results of a study that we did with the Ponemon Institute, looking at the different roles between marketing organizations, privacy organizations and security organizations across a company, and trying to find out how collaborative are those organizations. And when there is collaboration in an organization, is it valuable? Does it result in some return to the organization? And what we found was really interesting – that there's really a very strong correlation between the level of collaboration between those three groups and the incidence of data breaches within an organization. So what I mean by that is that in organizations where collaboration between marketing, security, and privacy are really strong, those organizations are much less likely to suffer a data breach than organizations where the collaboration is poor. And so that was very interesting.

The other interesting element that I wanted to bring out, while there are many interesting things about the study, the other piece that I thought particularly relevant was that if you talk to marketing people in organizations, they're more likely to tell you there's no collaboration even if the privacy and security groups are saying, "Oh, yeah. They're collaborating with us." And so I think that really speaks to what we talked about in many of the areas which is if you don't understand the business, and if you don't have close alignment of your objectives to businesses' objectives, the impact on your organization is real. Data breaches are much more likely to happen. Other things are, other bad things are more likely to happen when you don't have these things in place.

Julia Allen: Well, we'll make sure to include some links to that work in our show notes. And I think, again, you've reinforced this notion and this key element of success, which some might want to

avoid because it takes time, which is to get all the shareholders and stakeholders onboard. Create the collaboration structures. Create the relationship networks, and how critical that is to the foundation of the success of the program.

Kim Hargraves: Right, absolutely.

Julia Allen: So do you have any other references or resources that you would like to point our listeners to for more information on the subject?

Kim Hargraves: You can find more information on our Trustworthy Computing Program that include information on security and privacy among other things at miscrosoft.com/twc.

Julia Allen: Okay. Well, Kim, I'm so appreciative of your time and your expertise. I think you've provided great guidance and information and starting points for our listeners. And I hope we have an opportunity to talk again in the future.

Kim Hargraves: I'm sure we will. Thanks very much Julia for this.