The Legal Side of Global Security
Transcript

Part 1: The Complexity of Information Protection

Stephanie Losi: Welcome to the CERT 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 Stephanie Losi. I am a journalist and graduate student at Carnegie Mellon working with the CERT Program. I am pleased to introduce Jody Westby, president and CEO of Global Cyber Risk and Chair of the American Bar Association's Privacy and Computer Crime Committee. Today we'll be discussing cross-border data flows, outsourced operations, and compliance.

So, Jody, let's get started. In your publications and presentations, you highlight how complex the compliance, legal, and regulatory landscape has become when dealing with cross-border data flows and outsourced operations. What do you think are some of the most pressing issues in this area?

Jody Westby: Well, Stephanie, I think the first and foremost pressing issue is the wide variety of types of information that is protected and then how it's protected; different levels of protection. The term PII, Personally Identifiable Information, pertains to information that's typically within privacy protections like your name, your address, telephone number but it can also extend to employment history, your employer, your purchasing history, areas that a lot of people wouldn't consider PII. Then there's sensitive PII, or what I call super PII, which is what you would also expect which is sexual and religious preferences, ethnic origin, as well as things you wouldn't think about like trade union membership. So there are so many different types of information beyond financial, health, and medical information that is protected like cable TV records, insurance records, school records, arrest records, driver's information. It's just quite a wide array. And that's protected in the U.S. under state and federal law but then different protections in Canada, different protections for the 25 EU member countries, and then also there are countries that don't have any laws at all.

So certainly in the outsourcing context that creates a real issue, because you have a situation where your data is flowing from countries with some protections to countries without any to countries with different requirements. The second major area goes to: What do you do when something happens and that is that there are very inconsistent laws about cyber crimes, as well as economic espionage? And then there's a wide disparity in the skill level of law enforcement in helping to investigate cyber incidents, searching and seizure of electronic evidence. So, on a global basis, with 240 countries connected to the Internet and 1.1 billion online users, when you have 200-and-some countries that don't really have skilled law enforcement or smooth procedures for international cooperation, then we run into real issues and for global enterprises trying to do business around the globe or outsource operations to less expensive developing countries.

Stephanie Losi: Wow, so all of this sounds very complex. How has it changed and how will it change?

Jody Westby: Well, the bad news is that most of the developing countries have approached security, and privacy for that matter, as an afterthought. A lot of the donor organizations like USAID, the World Bank, some of the American development banks, have put a big emphasis on

electronic commerce and making sure they had electronic transaction laws, digital signature laws, but they never quite got around to supporting privacy and security legal frameworks. So we have a lot of problems that simply flow from the fact that many developing countries don't have adequate laws on the books. So that's the bad news.

The good news is security has now grown up and people are recognizing that it is an enterprise issue – that is, an issue that they have to address for governance purposes. And with operations outsourcing all over the world we're going to see that change. And one of the things that will happen, I'm disappointed it hasn't happened yet but I'm hopeful in the next two or three years something would happen, is multi-lateral discussions working toward a harmonized global framework. We have the Council of Europe Convention on Cyber Crime, and we have the EU Council framework decision on a tax against information systems.

Stephanie Losi: Okay, and could you sort of clarify a little bit, you know, what those are and how they differentiate from each other?

Jody Westby: Well, those are very similar in that since that the Council of Europe's Cyber Crime Convention, which the U.S. signed and we recently ratified. We are not a member of the Council of Europe, but we helped draft that convention, and it has been signed by, last I looked, 45 or 46 countries. But it's only been ratified by a handful, largely eastern European countries and now the U.S. But the EU took the provisions out of the Council of Europe Cyber Crime Convention, which had some very good international cooperation provisions, resolved a lot of the jurisdictional issues like dual criminality (meaning it had to be a crime in both countries before someone would give you assistance), extradition issues. It resolved a lot of the issues; it would help enormously.

But the irony here is that the Council of Europe Cyber Crime Convention is held up as, "Well, we have this, and so countries ought to sign this," and therefore it's created almost a lethargy in the discussions because people think, "Well, it's out there," so people could just sign it. It's actually pulled, I think, momentum away from the harmonization effort instead of enhancing it. Now the EU's basically mirrored those provisions, but it's going to get better. We at least have a good framework, we have a very good start, and that may move into a broader multi-national context. We'll have to wait and see.

Part 2: Challenges for Global Operations; Roles and Responsibilities

Stephanie Losi: All right. For due care with respect to privacy, what do you think is the biggest issue leaders need to consider when outsourcing some operations or when they have global supply chain partners?

Jody Westby: Well, now clearly the biggest issue they have is meeting their governance and compliance requirements in a global environment where you have such disparity between the legal frameworks. You can outsource a function, but you cannot outsource your compliance. And so it becomes critical that you have some assurances and knowledge that your provider is doing what's necessary through controls, through monitoring, through its own policies and procedures, to meet your compliance requirements. It's very important that you understand what the governance requirements are in a company so that you can monitor adequately your outsource vendor. And that's difficult for leaders because they very often think they will outsource a function, but they don't realize that it requires different governance on the client side. And that the governance issue and the communication issue between client and provider require close working relationship, early warning systems, collaboration, means to resolve problems, mitigate any damage. And those kinds of issues are pushing leaders to understanding that they just can't outsource a function,

maybe even send most of their people to the outsourced provider and keep two or three behind to kind of look over things. It requires a very different governance structure in the client company.

Now the other consideration that's a major problem is economic espionage and protection of intellectual property – the insider threat inside a vendor. You don't know how the employees are really acting inside a vendor. You don't really know what their security system is on a day-to-day or minute-to-minute basis. Certainly you do audits, you have contract provisions, you do the things that are required, but in this environment when we have so many business processes outsourced, so much that's IT-enabled with critical data, it's very, very important that companies take steps to identify their critical assets and make sure that they have protections around those in their outsourced provider.

Stephanie Losi: So what about global versus local considerations when dealing with cyber crime? I mean, we discussed a little bit insider threat, what about some other types of cyber crime?

Jody Westby: Well, it's very complicated because global versus local – local's where the rubber meets the road and what really happens is local jurisdictions, local customs, local cultures, the way entities do business can vary significantly from what could be a global security requirement in a major cooperation. Many of our global entities are now struggling with how to have some sort of consistent global parameters with flexibility points for compliance with local requirements or local situations. It is strictly jurisdiction by jurisdiction, dependent upon the kind of operations you have, how sensitive they are. If you have critical operational criteria, like 95% uptime or 98% uptime or certain number of transactions processed within a set period of time, then you get into some very different circumstances where you're trying to juggle global versus local. But it is complicated. It depends very much on the legal framework and again it depends very much on how the public and private sectors can cooperate and work together to resolve issues.

Stephanie Losi: It doesn't sound like an easy job.

Jody Westby: No.

Stephanie Losi: What roles are responsible for tackling these issues and making sure that the business is protected?

Jody Westby: Well, I basically would divide them into two main groups with a third group of players that come in and out of the scene. In the one major group at the top it's a board risk committee and the CEO and senior management. The next level of team is what team of people that I call the X team, which is a cross organizational team so X meaning for cross. And that would consist of representatives from general counsel, human resources, the chief security officer and chief information security officer (if it's divided into two), chief risk officer (if there is one), chief privacy officer, procurement, communications, public relations. And we need to get all of those people together regularly in a cross organizational team to address security issues on a regular basis, at least monthly, so that the security requirements can be woven into the fabric of the operations both horizontally and vertically.

The third group of incidental players that come in and out are operational personnel or owners of what we call digital assets. And digital assets is information, it's applications, including the operating platform, and networks. And so owners of those assets certainly are involved as you start protecting them and defining the criteria and the policies and procedures. So they come into play as you're making those determinations. And operational personnel, because it's critical, they are the ones who really handle the data, work through their day-to-day responsibilities. Involving them in the process of how you protect it in the policies and procedures (1) creates buy-in, and (2)

it's just smart because if it doesn't work for the way they do their job they're not going to do it. They're going to short circuit, they're going to find a way around it, and you're goings to end up with change management run amok because you're not going to have control over what's happening 'cause it never fit the work situation.

The worst thing that can happen in security is for technology to drive the business environment. The business environment has to drive the system architecture, not the other way around. And so often with security, people want to burden it down and say, "Here's how you have to operate and do your job." That's not a realistic approach.

Part 3: The Role of Legal Counsel in a Global Enterprise

Stephanie Losi: How would you describe the role of the legal counsel specifically in managing privacy and security risks in a global business climate?

Jody Westby: Let me first say that the person on the X team that is most centrally charged with the development of the security program would be the chief security officer or chief information security officer. But the general counsel plays a very important leading role, and most of them aren't aware today what their role should be. Or they don't have the right skills and training to know how to do this. They don't often convey contractual provisions that would require privacy or security measures to the technical team as well as the business operational team. There's not a clear communication. So general counsels today are having to assume a new role. And the learning curve is going to be high for them for a while. Because they need to learn how an enterprise security program is developed, and they need to take a leadership role in that because that's really, now with the plaintiff's bar filing lawsuits, it's real liability and risk management that's at stake. They also need to understand, though, the steps and the process because they need to be involved when you're categorizing digital assets on top secret, secret, or confidential. A lot of those categorizations are going to depend on the compliance requirements.

And thirdly, they need to understand how and when to use privilege. There's two kinds of privilege that goes along with general counsels or attorneys. One is attorney-client privilege, and then there's attorney-work-product privilege. And I recommend that areas that you want protected under one of the privileges, you're better to engage outside counsel because privilege does not hold up very well with in-counsel, you're part of the company. But for outside counsel, it's much harder to break that. And it's not a pure shield, but courts loathe breaking attorney-work product or attorney-client privilege without looking at it closely. So if you're looking at forensic investigation of an incident and the general counsel is the one hiring the security expert and having him conduct certain work for him and report to him or her, then you have something that's being done clearly in anticipation of litigation. It's work product to the attorney, helping him understand the case. You have a much better chance of protecting that. And when you have class-action lawsuits now being filed, it's just a matter of good risk management for companies to know when to use privilege to protect sensitive information that could very much impact their stock price, their market share, their brand. And attorneys are going to have to learn how to do this.

Stephanie Losi: Right. And so what are some of the pitfalls legal counsel should really strive to avoid?

Jody Westby: Well, I think that the hardest thing attorneys will find in doing this is it's new for them. So, attorneys are going to have to become pretty skilled at understanding the elements of an enterprise security program and how they can manage legal liabilities without interfering with business operations and without doing it in a way that turns people off. Attorneys typically like to

have some pretty definite provisions of what will take place or not take place. So, I think that will be the hardest thing is for them to just understand how to balance risk and reward.

Part 4: What Leaders Can Do

Stephanie Losi: And what do you think are some of the best ways for attorneys to work with operational people? What approaches have you seen work well?

Jody Westby: Well, the cross-organizational team works really well because when these people get in a room and they start talking about an issue, they suddenly see how Joe's issue is Sally's issue is Tom's issue is Mary's issue. And in the context of the broader organization everyone has a role to play and that they're all- and it helps reinforce the team concept that they're really a team working for a common goal. So I used to be a lobbyist and I would see wonderful things happen when people would get around a table and start working an issue. They could be coalition members that came in from very diverse points of view; they could be even opposing sides. But as you keep meeting and talking, then understanding develops, people start bending and giving. It was a very good lesson because I see that happen in cross organizational teams where people really start saying, "Oh, we really are working on a common goal here for the company," and the best thing for security is to have a unified agreement and approach and buy-in. And that is the best precursor to success.

So I would say the most important thing is getting the board risk committee, the cross-organizational team set up with the proper roles and responsibilities, and that includes appropriate segregation of duties. What we see so often is this chief security officer or chief information security officer reporting to the CIO. That is not good business practice. That is not proper segregation of duties.

Stephanie Losi: All right. So what are some good first steps for leaders to take toward this goal? I know that working in a cross-functional team is probably one of them. And also, what can they do to stay up-to-date with the field, because it does seem to be constantly changing?

Jody Westby: Making sure there is that list of critical assets and critical processes. A lot of companies when I ask "Let me see your list of critical assets and critical processes," they don't even know what I'm talking about.

Stephanie Losi: Right, let alone have it.

Jody Westby: Let alone have it. And they haven't stepped back enough to say, "Oh, these are the things that really go to our core functions. We really must protect these at all costs," or, "These are seriously critical to our business continuity or our profitability, our competitiveness." whatever. And so it's making sure that, in addition to setting up the structure, that they have also had the steps conducted that will identify those critical assets, that a risk management plan's been developed, and that they then take it the next step to business continuity, to crisis communications, to incident response. So they think things through. The worst thing that can happen is to have everyone flying by the seat of their pants when you have a major security breach. The newspapers are calling, the regulators are circling, the lawyers are preparing lawsuits, and the company hasn't worked out who's going to say what to employees, who's going to say what to the press, who's going to say what to the public or the families of the employees, and it's just very important to think all of those things through.

And, of course, hand-in-hand with that is providing the adequate resources. And I'm a bit upset that now some CISOs have been getting fired when there have been security breaches at companies,

when for years we've talked about, "Senior management needs to get involved in this issue, this is a board issue, it needs to be funded..."

Stephanie Losi: And learn from mistakes.

Jody Westby: Absolutely. And so the other thing that's happened though is CIOs and CISOs have not done a very good job at communicating in board-speak or executive-speak terms about what they needed and why it was important as an enterprise issue. And when you go in and start talking in too many technical terms to a board about these issues, their eyes glaze over, they don't get it, they don't want to get it many times. And so this is a whole new era. That's all changing.

But they have to allocate the right amount of resources on an ongoing basis because you can't check this box and think you're done. You can only check the box and then start preparing for the next review and audit. And in the meantime you're monitoring and enforcing and testing your controls and evaluating how efficient the program's really working.

And training the people. And the training has to be in targeted audiences. It can't just be security awareness training. It's training throughout the organization, including the board and senior management level, so they understand security and the evolving threats of security.

Stephanie Losi: Is there anything else that you think our listeners should know?

Jody Westby: Yes, I didn't answer your last question, which was how do leaders stay up to date? And I think looking at the CERT web site always is the first place people go because you have so much good information there. Second is the Department of Homeland Security's web site has a wealth of information. Other organizations like ISACA have a large collection of information they've worked through with their IT Governance Institute.

And then, lastly, my own ABA Privacy and Computer Crime Committee. We have written four books that were written by a multi-disciplinary team of people from everyone from attorneys, government officials, technical experts, policy people: *The International Guide to Privacy*, *International Guide to Cyber Security*, *International Guide to Combating Cyber Crime*, and then a smaller book that links them all together, *Roadmap to an Enterprise Security Program*. I mention those as resources because they are also free to people in developing countries. And so when you have outsourced operations, anyone who sends me an e-mail in a developing country and asks for these, I can provide a free electronic download to these books.

And in the [*Roadmap to an Enterprise*] *Security* book, we actually outline all the different questions boards have to think about, and ask broken out by categories. So there's a lot of good work that's been done by the Corporate Governance Task Force, by my committee, by DHS, by CERT, helping senior leaders now take on these challenges.

Stephanie Losi: All right. Well, we'll certainly provide links to those resources in our show notes as well. So, thank you very much.