Security: A Key Enabler of Business Innovation
Transcript

Part 1: The Security for Business Innovation Initiative and Council

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 software assurance. Today I'm pleased to welcome Roland Cloutier, Vice President and Chief Security Officer for EMC. Also joining us today is Laura Robinson of Robinson Insight, an industry analyst firm specializing in information security and compliance. Today Roland, Laura, and I will be discussing how security can serve as a critical enabler for business innovation. Our conversation today is based on two reports that Laura has written in concert with RSA's Security for Business Innovation Council, of which Roland is a member. So welcome Roland. Welcome Laura. Glad to have you with us today.

Roland Cloutier: Thank you for having me.

Laura Robinson: Thanks. It's great to be here.

Julia Allen: So Laura, to get the ball rolling, could you tell us a little bit about why RSA created the Security for Business Innovation Initiative?

Laura Robinson: Sure. Let me start by first defining business innovation. The way that we have defined it for this initiative is "enterprise strategies to enter new markets, launch new products or services, create new business models, establish new channels or partnerships, or achieve operational transformation."

So innovation today is really viewed that broadly in the enterprise and it has also become a top-level strategy. But RSA saw that there was a missing link in all of this. Even though it's a top-level strategy, efforts to protect the *information* involved in business innovation is not considered strategic. So RSA wanted to create an industry initiative to really help security become more strategic.

And so it's not like this concept is alien to security professionals. Actually for the past few years, most security professionals have really been striving to align their security programs with the business, but many are still struggling with that. So RSA formed this Council in order to create kind of a body of knowledge to offer to the industry in order to maybe move the needle forward, advance this whole idea of making security more strategic.

Julia Allen: Well that's a great start. So what is the profile of a typical Council member, so we can understand the perspectives that are being brought to this new area of research?

Laura Robinson: Sure. The Council is made up of about ten senior security executives — so chief security officers, chief information security officers – from global 1000 enterprises; so really some of the largest companies in the world. They're from a cross-section of industries, and there's a mix of companies from the States, as well as international. If you want to see the full list, it's available on the RSA website. And if you go to the RSA website, on the left-hand side you'll see a list of selections. Just select "Innovation" and that will take you right to the Security for Business Innovation site.

Julia Allen: Well I know you're embarked on a series of reports and we're going to talk about the first two. So your first report, which is titled "The Time is Now: Making Information Security Strategic to Business Innovation," identifies a series of seven strategies that kind of help us start to connect security to business innovation. So could you just briefly introduce each of those seven? And then we'll get Roland involved.

Laura Robinson: Sure. So first of all, the first recommendation obviously is to have the right mindset. So it's really important that security professionals have the idea that they are enabling business rather than inhibiting business. So beyond having that good foundational basis of the right mindset, and being supportive of the business, the other thing is to know the business and speak business. Another recommendation, recognize and seize opportunities to add value; build relationships and win influence; become a risk versus reward expert; build repeatable processes; and make time for strategic thinking.

Part 2: Security Must Speak the Business; Introducing Risk-Reward

Julia Allen: So Roland, picking up on one of those, what exactly from your vantage point does it mean to know the business and speak the business? We talk about security trying to get connected to the business. What does that really mean?

Roland Cloutier: Well Julia, it's pretty simple. I guess in one sentence it's your ability to understand what the company or entity that you're servicing delivers to their end-users. And it doesn't matter what industry or vertical you're in, whether you're public or non-public, governmental or not. The real discussion here is what's at the end of the Ethernet that you're protecting? Whether your company builds a widget, protects a nation, or ensures the safety of a patient in the health-care environment, your capability to drive a protection program to enable that business is solely based on your ability to understand the value chain in that business and how they deliver those services.

And I guess speaking the business is a very key component here. When I talk about speaking the business, it's not just about general business language. But it is about understanding the strategy that my company sets forth; understanding deeper than

the value chain, but within divisions themselves, the products and services that they drive; and being able to articulate risk and security initiatives to those specific businesses. And if you're a senior level security executive, your success, and the success of your business protection program, is going to rely on translating security needs and initiatives to business impact.

Julia Allen: So Roland, you kind of started us down this path. But as a CSO or a CISO, how have you found that you've been able to provide either a unique vantage point to recognize and act on opportunities for adding value?

Roland Cloutier: One of the best ways that we've driven at driving value into the business is understanding long-term strategy and short-term goals of the business. So whether it's the business needing to be more innovative and drive partnerships and understanding the security implications of that; like allowing third-party access and designing new connectivity technologies that allow access to intellectual property and trade secrets from outside the organization; or whether it's driving time to a new market and ensuring that our resources can provide the type of technical services faster, quicker, and cheaper in the markets that they want to go to; to unique areas such as globalization and ensuring that we had resources in the regions for which we going to operate.

And it just goes on and on and on. Understanding security impact and the risk impact to the business, and looking at each one of their initiatives before they start their initiatives, and making sure that we're prepared to meet their needs and act as their internal consultancy.

A very specific one for EMC that truly helped the business was our Theater Threat Management Program. We were concerned with the speed at which the business wanted to internationalize; so not just use third-parties and O&O (owned and operated) programs but really look at new countries and areas of opportunity to build out market share.

Traditionally the business had no place to go to say “What are my risks?” Whether it's geopolitical, economical infrastructure, or cyber, the business had no place to turn to. We quickly created a Theater Threat Management Program that looked at all of the countries of opportunity and the existing theaters which we worked in. And the business now has a place to go. If they want to go to Vietnam, or they want to go to South Asia, or Southwest Asia, or Eastern Europe, they have a very clear picture of each of the countries, our assets there, or even if we're not there, and the services that we can provide.

Because the business knows this, they often engage us early, to say, "We'd like to go to location X. Can you sit in on our team and help us get there?" Instead of saying, "How scary is it?" they know that our job is to make sure they can do their business anywhere, anytime, wherever they want. And so they invite us early and often, which is a big key place for security to be.

Julia Allen: Well and clearly you're making the point that security and business innovation go hand-in-hand.

Roland Cloutier: I don't think you can be an innovative global company without a security and risk program tied at the hip. You can certainly go somewhere and do something and build a program. But the problem is you're — what are you putting at risk? What are the downstream impacts of a bad security decision? And what is it going to take you to recover from that, either from a brand equity position, marketability of your products or your services in whatever region you're in, or a general liability cost, because of a negative impact issue? These things, when they happen after the fact if security wasn't planned, become a very expensive proposition.

Julia Allen: Well Laura, let's move on to the second report and probe into that one a little bit. This report is called "Mastering the Risk-Reward Equation: Optimizing Information Risks while Maximizing Business Innovation Rewards." And for our listeners, in the interest of full disclosure, I did serve as a guest contributor to this second report. So Laura, in this report, you talk about a step-by-step process for making a risk-reward calculation for new business initiatives. So what do you mean, or what did you describe in the report, that you meant by the risk-reward equation?

Laura Robinson: Any equation, it factors in many variables to arrive at a solution. So in information security the factors that you consider — and this is going to be really familiar to everybody listening because it's what you do n a risk assessment — but basically you look at the type of information; the level of sensitivity; protection requirements; how it's being stored, processed, or transmitted; the threats and vulnerabilities; the systems and applications; and the likelihood and the impact of compromising events.

So yes, as I mentioned, it's very familiar. That's how people do risk assessments. But the key is to not only look at the risk side of it but also to look at the reward side of it. So the focus of the risk-reward equation is determining the right level of controls to put in place, given an acceptable level of risk. So an acceptable level means that the owners of that risk are really willing to take responsibility for that amount in order to maximize rewards.

So I think what's happened historically is that information security has really been focused, singularly focused, on the risks. But if you're going to enable business innovation, you really have to also look at the rewards.

Part 3: Determining Risk Appetite; Using a Self-Service Model; Future Reports

Julia Allen: Well this is pretty interesting because you're right. We tend, particularly as security professionals, to think about the downside, cost and loss avoidance, and things of that nature. So Roland, in this discussion about risk-reward equation, we talk about risk appetite or risk threshold. So why is this an important factor and how do you capture and quantify it?

Roland Cloutier: Yeah, it's an interesting question. A lot of people don't get risk appetite and how risk appetite fits into the decision-making process. Because when you look at it — CISOs and CSOs — we don't make risk decisions. We don't accept risk. Our job is to be the internal consultant for the company and be able to provide them with a clear picture of their options: "Here's the problem. Here's how we fix it. And here's how you can remediate it, or here is how you can avoid it." And there's a lot of options that go into that.

One of the biggest ones is understanding what is an acceptable level of risk? And that's really what a risk appetite is. For the people that you're providing your business, your security services to, what is their acceptable level of risk?

So when it comes to capturing and quantifying it, it's actually pretty simple. I mean, you can go into detail, baseline risk assessments and adding in this as part of the denominator. But here's how I look at it. Although risk appetite and risks are fluid, as everything else is in the business, your baseline security and risk assessments are not. What you enter in as a potential risk impact to the business, impact to brand, all those quantifiers that you make your risk measurement out of, they always stay the same.

What's different is how the business accepts the risk. You'll see, during your tenure, that the business starts to accept a little bit more risk, and they say, "No that's fine, no that's fine," or, "That's okay." Well every time they do that, they're accepting risk at a different level. And basically you can trend it and give basic heuristics of at what level the business or a specific division is accepting it.

And the best way is to go back to them and say, "So I understand that you're okay with this type of risk, because for the last three months your risk appetite has gone up and you've accepted things at this level. Is this going to continue?" And basically you make that part of your decision-making process. So when my risk teams come to me, or our security teams come to me, and they say, "We have a very clearly defined process that says if it reaches a certain level of risk, we need to notify the business and sit down and have a discussion, and give them their options." Well we're not going to waste a lot of time with the business, arguing. If we already know what the risk level is, we're simply going to provide them with their options, at that risk appetite level. And simply monitoring that and checking in with them and saying, "Here's where your appetite has been over the last couple of months. Do you want to continue on this?" makes them understand that you do understand their business and you're making their time to delivery faster, because you're taking their context into what you do. And that's how we do it here at EMC.

Julia Allen: Well in the report also, the second report, one of the recommended steps is for business units to use a self-service model. Can you say a little bit about what this means from your point of view and how it works?

Roland Cloutier: Well we have a couple of different self-service models at EMC. The first one is we are embedded now within the CIO's technology program organization.

So the people that drive all enterprise projects within EMC now have risk as a check off, if you will, risk and security.

Right at the beginning of when they start to define what their project, their business project's going to be, we've provided them with some easy tools that say, "What type of information are you touching? Is it internal or external? Is there PCI (Payment Card Industry) or PII (Personally Identifiable Information)?" And we educate them on what that is. And if so, how much? And so on and so forth.

So as they enter in the self-service tool, basically they come out with a risk score, and they know what level of risk services they need. Do they need a full assessment? Will there be an application assessment? Is it just a security architecture technology review? Or is this a regulatory requirement? And do you need to budget an X number of hours for that into your project?

So it gives them a base understanding of the risks of the project right off the bat. It provides them with the level of, if you would, consulting or security services they're going to need on their program. And it gives us an immediate feed from these projects, keeps us at the table very early. And it's worked out well because we're setting expectations up front and there's no big surprises at the end if they follow the process.

And some of the other unique tools we've put in is self-scanning tools. Whether it's a technology system's solution or an applications solution, we've provided the IT organization with managed security tools to look at their products through different life cycles. So not just when we do a code review as a security entity, but through the entire SDLC, we have tools and technologies they can use to check on their projects without waiting in a queue for our limited resources to be able to review their project.

Julia Allen: And during that whole process, and some of the other processes you talked about with respect to risk appetite, risk thresholds, how do you determine, or how does EMC determine with your participation, who has the authority to make what level of risk decisions?

Roland Cloutier: Well that's well-documented. That was the first thing we did, is we said — we came to an agreement with the business and our Executive Security Council actually, which is made up — our Executive Security Council is our oversight committee. It involves the vice-chair, the CFO, the CIO, myself, general counsel, and a few other people. And we looked at what was an acceptable risk process and who could do that.

So when there is a certain level of risk, a vice-president can accept it, at a certain level, to say the division, a senior vice-president. And when it is a company-wide-affecting issue, that is actually solved at the Executive Security Council level. And so myself, I can never actually accept risk. I can only argue the point for or against, if you will, or let the business, if it's below a certain threshold, accept it on their own.

And then of course we have a mediation workflow that if I don't agree they should be able to accept it, and the business thinks they should and we can't reach an agreement, that also goes to the Executive Security Council, who's made up of other business members, where we have that decision.

Now interestingly enough, the program, in our opinion, works well enough that we've actually never have gone to the Executive Security Council because of the relations and being able to sit down at the same table and drive an appropriate remediation or agreement on how to protect the business. So our process we believe works well.

Julia Allen: Well this has been a fantastic summary of some of the key points in the second report. I thank you for all that great insight. So Laura, as we come to our close, could you give us a little preview of the topics that the council is tackling next?

Laura Robinson: Yes sure. Our next report is titled "Driving Fast and Forward: Managing Information Security for Strategic Advantage in Tough Economy." And what we're looking at is how do we keep going with this really important effort to make security more strategic and better aligned with the business, given everything that's happening and given the fact that organizations are going to probably have less budget. So it includes recommendations for driving efficiencies. And it covers things like: how do you determine priorities?; how do you get resourced?; rationalizing processes; how do you share costs with the business, what are some good formulas there?; and things like automation.

So the fourth report, which will come out probably at the end of Q1, the beginning of Q2, is going to be a bit of a visionary report. We're going to look at what would a new information security model look like, or what would a future model look like, given all these things that are happening in the enterprise: globalization and technology and all the things that are being thrown at information security officers? If we took a step back and kind of envisioned a new paradigm, what would it look like? So a bit of an ambitious one, but given the caliber of the people on the council, I think it's going to be a really exciting one.

Julia Allen: Well, in fact, when we were talking, I know you mentioned things like cloud computing, virtualization, social networking, the fact that we're both all becoming more mobile and our devices are exploding and becoming more mobile — that these might be some of the topics you touch on in this fourth report.

Laura Robinson: Exactly. Looking at the huge technology upheavals that are happening within the enterprise, but also some of the ways that organizations - - Roland talked a lot about how EMC is working more and more with global partners. So that's another aspect to it as well.

Julia Allen: Well where can our listeners learn more, Laura, from either you or Roland? Do you have any other sources or references that you'd like to point our listeners to? Laura, why don't you go first?

Laura Robinson: Yeah sure. Basically the website that I mentioned before is probably your best source because a lot of the information is consolidated right there for you. It's the Security for Business Innovation website and covers not only the reports — and we tend to come out with a report per quarter — but also some of the research that has been commissioned and some of the results of that research.

Julia Allen: And Roland, do you have anything you'd like to point our listeners to?

Roland Cloutier: You know, there's a couple of places that I get a lot of value from, from the rest of the industry sharing and some of the new work that DHS (Department of Homeland Security) is doing. So the first one would probably be the Corporate Executive Board's Information Risk Executive Council. They're a great resource in person, online, or participating in some of their programs. So I would encourage people to go to the DHS CERT site and get involved there as well.

Julia Allen: Well I can't thank you both enough for taking your time and sharing your insights and expertise with our listeners. I think this series of reports is a terrific gift that RSA has sponsored and made back to our community at large, making these publicly available. So I thank you very, very much for your time today.

Laura Robinson: Thank you.

Roland Cloutier: You've very welcome. Thank you for having us.