Dual Perspectives: A CIO's and CISO's Take on Security
Transcript

Part 1: Roles, Responsibilities, and Reporting

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 very pleased to introduce Patty Morrison, the Chief Information Officer for Motorola, and Bill Boni, Motorola's Chief Information Security Officer. We'll be discussing how to effectively position and address security from the vantage point of their two roles, the CIO and CISO role. So, Patty, if you'd get us started for our listeners: Would you please describe the scope of your responsibilities for Motorola, and then perhaps what your two to three most challenging issues are that you face on a regular basis?

Patty Morrison: Sure. Thanks, Julia. It's great to be here, and [I'm] happy to be participating in the program.

My responsibilities include all of the infrastructure applications that run the company on a global basis. I have over 5,000 in-sourced and outsourced resources that support Motorola in over 140 countries with approximately 70,000 Motorola and then contract employees. We have quite a diversity of applications and infrastructure around the world. It includes all, of course, the networks and the computing infrastructure and user computing, all of our transaction and enterprise information management applications, all of our ongoing business process transformation work across all of the different functions at Motorola.

So the challenges that I face are keeping up with demand for constant change in how we do our business, our customer demands, our need to continually drive improvements and operating earnings and gross margin. And in most cases, that requires support in some way, shape, or form from the information technology organization. Demand always exceeds supply, at least from a monetary standpoint, so a lot of what I spend my time on is prioritization and portfolio management. So that is always one of the challenges that we face. The challenge of keeping an organization that is spread across the world rowing in the same direction at all times, and that includes the need for constant communication for our strategy and our plan. And then supporting the business in other ways, which would include participating in strategic direction setting overall for the company and helping to solve the immediate business issues and challenges that Motorola has.

Julia Allen: Well, for such a large global enterprise with all of the members of your organization, all of your supply chain partners, I can imagine that there are some fairly daunting challenges to undertake. What — in that whole mix of things that you have to face, where would you place security on your radar screen?

Patty Morrison: Well, security's very high on my radar screen. I have Bill, who you've introduced, my Chief Information Security Officer. He reports directly to me. He's an ongoing part of my staff. We also, both of us, participate in steering committees that would be looking at broader security

issues. Bill would tell you that when I get up and speak in front of all of the officers at Motorola, I'm always talking about security. So I have to be quite a bit of an evangelist as well.

Julia Allen: Well, Bill, welcome to the podcast.

Bill Boni: Pleasure to be here.

Julia Allen: I'd be interested in knowing, from your vantage point, what types of issues tend to fall in your lap versus Patty's when it comes to addressing security?

Bill Boni: Well, as Patty has indicated, her role of leadership for the overall IT organization, a member of the executive leadership of the company, is to raise the awareness and to provide the resourcing. And my responsibilities are to focus the program on managing the risks that are most important to Motorola and that will add the most value, enabling us to achieve our strategic business initiatives, again with the minimum amount of acceptable risk.

So the partnership that we have relies on my team going deep into this particular subset of issues and raising those up with the business context fully developed, and well defined road maps, timelines, and priorities set for the overall program initiatives, so that Patty can then provide the support and the ongoing visibility of the benefits of those programs to the broader executive and managerial audiences and the external constituencies of Motorola.

Julia Allen: Okay, so some would say that having the Chief Information Security Officer report to the CIO or Chief Information Officer can create either a real or perceived conflict of interest. Do either of you agree or disagree with this? I mean, obviously you've worked it out for yourselves, but what do you think?

Patty Morrison: I don't think it's ever created a conflict of interest. I think that it depends – you have to be clear. Bill does an incredible job of being independent and objective. And he works very closely with our internal audit, our loss prevention organizations, our legal organizations, to get involved in efforts that I don't need to know about. And he does wear that hat extremely well. So I really do think it could very much depend upon the quality of the leadership of the individuals. I don't know, Bill, if you want to add any flavor to that?

Bill Boni: Yeah, I think the essential fundamental here is trust and responsibility of the leadership. Because what Motorola has developed is a very effective set of commitments on the part of senior leadership from Patty and the other members of the senior leadership. And the expectation that my team will be providing the contributions that help us manage the risk this way. So having – the reporting relationship, for me, I've never seen the conflict issue. I've seen the opportunity and the leverage that comes from having the sponsorship of an engaged, articulate executive who understands information, its value, its importance, and the many areas in which it impacts the business if the risks aren't managed effectively.

So I think that developing the trust and developing the partnership is really the most efficient and most effective way for security officers to gain the impact that they all seek in exercising their accountabilities for protecting the information assets.

Part 2: Selling Security and Pinpointing Acceptable Risk

Julia Allen: Well, that makes good sense. Thank you both for addressing that question. So what approaches have either of you found to be the most effective in presenting security's role to the

business, both as a business enabler or as a necessary cost of doing business? So, effective ways to position security to your senior leadership and even your Board of Directors.

Patty Morrison: Well, let me start, and then, Bill, you add in. Like anything in IT, you tend to have a phenomena where the only positives you get are the absence of negatives. So I think what we do is we've been very effective at attaining a vision for where we want to go with security and why it's important to do so.

For example, the world is not firewalls around the borders of Motorola. We don't operate that way. I would argue no enterprises operate within a four-wall boundary. We have suppliers and partners and customers, and we have people in and out of our facilities. And so the practice of security and what you need to secure and painting kind of how the work is done in the future, and where security needs to be practiced, is part of what we've built here at Motorola.

That vision then tends to drive how we invest. We can't get all the way to that vision overnight, we can't afford to. And so when we discuss issues like, why is it important to have business continuity planning? Why is it important to have e-zoning and some of the other capabilities that we want to put in place? We have to put it in the context of where we're headed. So that's one thing that I think has been very effective.

The second thing I would add is that you have to use opportunities that happen in the world to educate, again and again and again, as to why it's important to make the investments. So last Christmas, for example, we had an earthquake in Taiwan, and it brought down essentially the entire telecommunications infrastructure for Asia. It was the end of our quarter, the end of our fiscal year, our number-one production facility is in Tianjin, China. And we need to get orders and make product and ship product, and when you don't have communications it's a little hard. So the fact that we could execute quickly a response to that, have the backups in place, know exactly what to do, allowed us to not miss a beat in shipping product. And you use those examples. You can't prevent every possible thing that could happen. So why is it important to be able to respond quickly? Bill, you want to add anything?

Bill Boni: Sure. One additional element in working with Patty, as we've implemented the IT portfolio management protocols to prioritize our investment in the various strategic areas that are going to enable Motorola's business process, we and the security team have been working in parallel to begin to manage risk as a portfolio, to be able to articulate the consequences of various events in financial, business terms, and the appropriate controls to help manage those risks in a way that will make it very clear to management the consequences of a choice to manage or to accept a given set of risks. And I find that that kind of dialogue is much more effective in helping people make the choice to do or not to do something with their eyes open.

Julia Allen: Well, Bill, that's a real nice segue into an area I wanted to explore next, which is: How do you go about determining acceptable levels of risk for security? In other words, how do you determine how much security is enough at any given point or for any given opportunity?

Patty Morrison: Go ahead, Bill.

Bill Boni: Well, again, our emphasis is on achieving what I would call a commercially reasonable degree of protection, security. And effectively to know what's enough is to be able to articulate the benchmarking data that shows how comparable organizations are invested and positioned for a given portfolio of risk, and then do the comparison with Motorola as a company. And when we're able to demonstrate that we have a portfolio of risk management processes and investments in place that are comparable to equivalent organizations, absent any set of mandated regulatory

demands for a specific set of controls, that's the best available framework that demonstrates that you're exercising responsible diligence.

Julia Allen: So it sounds like you have a pretty effective relationship with maybe some of your peers in the marketplace or some other trusted organizations, and perhaps do some cross-benchmarking between organizations. Am I hearing that properly?

Bill Boni: Yes. That's an absolutely essential part of knowing, again, in a very dynamic area like information protection, whether you're keeping up with the changes in the environment. It also avoids the temptation to go for a fad or the latest and greatest just because a vendor is pushing a particular set of capabilities as being essential to support the organization's security. Understanding how others view the risk and making choices based on the value that it's going to bring to your particular organization is how we would approach it.

Julia Allen: That's great. Well, thank you. Patty, how do you make the necessary trade-off decisions when you're prioritizing across your entire set of opportunities and issues and concerns? But particularly with respect to security, what is kind of like the thought process or the decision-making process that you use to pick amongst — as you said, you can never do it all, but to pick the ones that are really most important?

Patty Morrison: Well, of course, Bill goes through the same annual cycles that all of my teams go through, which would include kind of a strategy planning session and then also an operating plan for the following year where he makes a budget request. And so one part of making those trade-offs is understanding the total horizon and picture of what he believes we need to accomplish. And that's what we talk about in the strategy reviews and the time that he and I spend together, and what he educates me on.

And the operating plan — what we really try to do is protect a constant level of investment in security. It's not a one-time thing. I think we've been able to say, "Here's the amount that we need to invest year over year. We also have to run the things we've invested in previously, and we're going to make those investments, and that's kind of a run rate going forward, and we're not going to touch it," okay?

Now if we have excess capacity in whatever way financially to be able to go faster and support more, I think those tend to be built up as investments related to enabling other things. Security doesn't have to be its own isolated thing. Bill's done a very good job of helping my entire team understand why the investments that he thinks are appropriate will enable work *they* want to accomplish, so they can fund more security investment based on business needs that they are addressing, either in applications or infrastructure. Occasionally, we get at least political capital from the help of our compliance and our auditing organizations that help us in a very objective way identify where risks and opportunities may be, and then help us to put pressure into the organization to fund getting them fixed. So those are three methods that we use.

Julia Allen: So would you say that the process by which your security investment decisions are made and justified is very comparable to the way other business investment decisions are made at Motorola?

Patty Morrison: Absolutely. Absolutely.

Julia Allen: So it's right there in the mix.

Patty Morrison: Absolutely. It's not, it's not separate or anything. It's out there front and center, completely transparent, here's what we're going to be doing, here's what we're not going to be doing, and why we feel it's important to make these investments.

Bill Boni: So by articulating our strategy, setting out the architecture to support that strategy, and then setting out the road map with a multi-year horizon and the estimated investments at any given point in time, we're able to present that ongoing road map and horizon as well, so that we can see what's planned for next. And if — let's say an experience develops in the external environment where something, the risk environment dramatically changes, typically there's something on the road map that was expected to address that. Sometimes you need to pull those things in. That's when we work with Patty and the finance team to say, "New risk has manifested itself earlier than we had anticipated. Therefore this is how we're going to control that risk going forward."

Patty Morrison: And likewise, there are business conditions in which funding needs to slow down, and we may say, "We need to slow these down." It's not a "no," it's just "not now." But keep them in front of us, and depending on when capacity frees up, whether it's people capacity or funding capacity, whatever, we push the money out again. And that's our — what we do as a leadership team in our portfolio management process is we make those trade-offs all the time.

Part 3: Role-Based Advice

Julia Allen: Excellent. Well, thank you, that's really, really helpful, and very consistent with some of our governance research in terms of organizations that are tackling this particularly well, where security is mainstreamed in with all the other kinds of disciplines and features that the organization has to contend with. You've got to have it all in the mix if you're going to deal with it equitably. So let's turn our attention to roles a little bit. Either of you, what roles do you find to be most essential to the success of your security program?

Patty Morrison: Well I would — I'll start with kind of the layer at that strategic discussion level. But we have a team that has representation from all of the major functions of concern, HR, legal, finance, which is in our auditing area. We even have marketing, because marketing plays such a huge role in protecting consumer, customer information, for example. And that team, that steering process, has helped us to bring what I would call issues that people may not be seeing. And we talk about them, we build plans, we get their sponsorship and engagement to get the resourcing to address them. And then Bill has a team that basically follows a service model that we have across our leveraged service functions. I'll let him tell you about kind of how he is structured.

Bill Boni: Again, within the construct that Patty's laid out there, the information protection team is focused on the contributions for planning, the overall road map, the architecture, the framework for this, and then ensuring that we have, in fact, compliance to that set of standards and controls that have been identified for the various applications, the environments, platforms, and so forth, the kinds of information. So my team is organized around governance, around data protection and privacy, around enterprise resiliency and disaster business continuity services, around security solutions engineering, and around risk management, which is essentially the measurement of the degree of compliance too. One of the benefits of being in a heavy engineering organization is we've found it very effective to apply the Six Sigma type of protocol, such as failure modes effects analysis, in order to help us identify and prioritize the various control areas that need to be executed. So then my team helps make certain that the appropriate capabilities exist and that in fact they're being applied where they should be applied within those various environments and areas.

Julia Allen: Great, thank you so much. So, turning our attention — and as we start to come to our close, the two of you have obviously been at this for quite a while and been quite successful. What advice might you give to those in your roles, in either a small to medium-sized organization or a large organization that is either trying to get their security program off the ground or may be struggling with having it be dealt with in a serious and effective way in the same way that other business processes are operating? What advice might you give to help someone kind of get the ball rolling or help them deal with some of their big challenges?

Patty Morrison: Well, utilize the resources available to you, like CyLab, for example. I mean, there are resources available to help you understand how to put a road map together. And that's probably a place I would start. Assess your situation, and you can get resource help to do those assessments if you want formal assessments done. As a matter of fact, Motorola actually does formal security assessments for many of our customers. But you could do that. If not, do your own assessment. And then lay out where you are and where you think you want to be in two to three years as your vision, your strategy, your road map. You've got to start there no matter what size company you are.

And then you build the case for each step along the way, and you fund your way to getting that end state established as your business situation allows. But I would say that whether you're the IT support person in a small company or the CIO of a larger company, you have to make this a priority. It is imperative to business success. And it's unfortunate for the many companies that do experience the issue where it actually hurts their trust and reputation from their customers. Those are very, very hard to recover from, and take much time, and I'm sure, Julia, you could give many examples of those situations in the market. So it's very important to make it a priority and, again, use the resources you have available to you. Now, Bill, what would you say?

Bill Boni: My words would be to the security practitioners or protection professionals out there, is to understand, we can't do it *to* the organization, and we can't do it *for* the organization. We have to do the protection program *with* the organization. And one of the lessons I've learned working closely with Patty is, to the extent that the business and the management team understands and therefore accepts their accountability for risks, their commitment will be dramatically improved. So the essential role that security professionals need to address is that outreach, that communication, that speaking in business language to the business leadership so that they really get the facts and they understand the need for [security], and the consequences of [its lack], is how the program will be most effectively supported and sustained going forward.

Julia Allen: Sounds good. So, when you're asked the question, "Are we secure?" how do you answer it?

Bill Boni: The focus is on what's commercially reasonable. I think sometimes as security professionals there's a tendency to want all possible risk, all possible controls, all possible protection in place, and then to say, "Now I'm done." And it really comes down to adopting that risk management framework that says, "Commercially reasonable security, have we done what's responsible under the circumstances?" And how you know that is, you do the benchmarking, you participate in things like CyLab, you get the reference documentation for best practices, you map your control frameworks and your risk areas, and you say, "Here's what we have in place, and it is equivalent to comparable organizations." At that point, I think in the private sector, you've done what you can do. And then you know where the gaps are or where the road map is, and you just consistently move ahead step by step. And as Patty said, when times are good, you may go faster and do more. When times aren't so good, you still maintain momentum because your eye is on the horizon. You know where you've got to go, you just may have to take a few steps longer to get there or take some more time to get there, but you'll get there.

Julia Allen: Yeah, well, it sounds like you make a very solid business case and use all the resources at your disposal to help present that.

Patty Morrison: Right.

Julia Allen: So is there anything that I should have asked either of you, or any closing comments that you'd like to add to our conversation?

Patty Morrison: No, I think that I would just say it's a journey, and there's always something new, and you're always learning. I mean, one of the challenges of this profession is that there's more technology introduced that creates unexpected disruptions, either blatantly, kind of subversive kinds of things, or accidental things that you always have to be on your toes, and you always have to be learning. And so making sure that you invest not only for your security organization but for all of your IT professionals, and constantly learning what they need to do, and how they design applications, how they implement infrastructure, how they design metadata, whatever they are doing, that they need to make security a part of their professional catalog of skills. And I think that it's not just about what happens in the CIO office or in the CISO's office that happens. It's all IT professions' responsibility to make security a priority.

Julia Allen: And Bill, any closing thoughts from you?

Bill Boni: One thought, which is that what we learned in the 20th century is still relevant in the 21st century. But to echo Patty's comments about the need to learn and adapt, we know that the malicious, deliberate, and willful attacks are increasing, and therefore the security professionals out there that are responsible for protection are going to have to adapt our programs to deal with the more skillful opponents that are targeting much more malicious outcomes as a consequence of their actions. So that's going to keep us all on our toes going forward.

Julia Allen: Well, I'm so appreciative of both of your times. I know you're both extremely busy people with a lot of demands for your attention, and appreciate your remarks and I know our listeners will benefit greatly from all of your advice and experience, so thank you very much.

Patty Morrison: You're welcome.

Bill Boni: You're welcome. Thank you.