Business Resilience: A More Compelling Argument for Information Security
Transcript

Part 1: Bridging the Business – INFOSEC Language Gap

Stephanie Losi: 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 Stephanie Losi. I am a journalist and Carnegie Mellon graduate, working with the CERT Program. Today I am pleased to introduce Scott Dynes, a senior research fellow at the Center for Digital Strategies within Dartmouth College's Tuck School of Business. Scott's research and studies focus on organizational adoption of information security, and today we'll discuss why it's so often difficult for business leaders to understand the value of security and why they should pay attention. So, Scott, welcome.

Scott Dynes: Thank you, thank you very much. It's a pleasure to be here.

Stephanie Losi: Thank you. Let me just dive in right here and ask you: when you talk with business leaders, how do they view information security? What is their immediate reaction when you bring it up?

Scott Dynes: Well, that's a very interesting question. It seems that — we [at the Center for Digital Strategies] went and talked to Chief Information Security Officers as well as VPs of various business lines, at many companies and in many different fields, and there was a variety of reactions when we asked them about how they view information security. Some view it as a complete cost. It's just a cost center. They wish they didn't have to spend any money on it at all.

Stephanie Losi: Right, like [they wish] it would just go away.

Scott Dynes: They do wish it would just go away. They don't understand. Others, they see why they have to spend money on it, but they actually don't understand what it's doing for their business. And still others actually view it as a core part of what they need to assure that their business works well.

So it kind of spans the range. Some people just don't understand it, and others completely understand the value to their particular business of investing in information security.

Stephanie Losi: So if we turn to the people who really don't understand security or understand it but wish it would go away, what do you think is at the root of that image problem for information security?

Scott Dynes: That's something that we've been spending a fair amount of time on. My particular view is that information security is important for all businesses that use the information infrastructure to manage their businesses or manage their relationships with either their customers, their suppliers, or other extended and enterprise partners.

I think the disconnect in some businesses comes about because the Chief Information Security Officer or the person who's playing the role of Director of Information Security is not clearly articulating the consequence of poor information security to the business partner in terms that the business partner can understand. In some companies, the Director of Information Security will talk about information security as an IT thing and use geeky terms such as firewall and intrusion protection system, which mean nothing to a business manager; and vice versa. The IT manager will not understand the terms that the business manager is talking about.

So, essentially, what we think makes the distinction is, at companies that do this well, both the business manager as well as the information security manager understand the impact that vulnerabilities to the information systems will have on the business processes that enable the business to run.

Stephanie Losi: Right, and they're speaking the same language, so they can talk about that with each other. So what do you think — what is that language? What do business leaders really want to hear, and is there a way, do you think, to put security in those terms? How should the IT person be speaking to the business person, and vice versa?

Scott Dynes: Essentially, it seems that financial services do very well at this, and it's because, to them, most of the data that they have represents real money, and therefore everybody sees a very tangible benefit to making sure that they have good information security. So when the business manager and the information security manager talk about securing data, securing links to other banks, it's very clear to both of them that what they're talking about is the core business proposition of the entity.

In other fields, such as in manufacturing, it's not such a clear relationship. We interviewed an oil refiner. The manager of information security there was very insistent that they needed to increase the security of their SCADA [Supervisory Control and Data Acquisition] systems, their process control systems, but speaking to the vice president of refining there, he could not understand what the value proposition was for increasing information security. He could not understand how increasing SCADA security would help him make, as he put it, make better oil.

Stephanie Losi: Right, so what do you think he wanted to hear? Is there a way that that could have been fixed?

Scott Dynes: I think so. It's been our experience when we go in and talk to people that it's actually very hard to make an ROI business case. But what information managers, information security managers *can* do is talk about business continuity. They talk about investments in information security resulting in greater continuity for the business in the face of particular information security threats. The business manager will understand the business continuity argument, and they usually act upon that in an appropriate way.

Stephanie Losi: Okay, so in this case we're coming at it from kind of a point of view of resilience, really.

Scott Dynes: Exactly, exactly. All business managers want their company to be resilient in the face of various activities that can happen in the business landscape. And so if you can come to them and say, "Our business will be more resilient if we do this," then they will look at that very seriously. The best you can hope for, we think, is to give them a rational way to make a decision, and they may or may not act upon a particular threat from the business resiliency standpoint. But if you talk about that threat in terms of business resiliency, then you'll be talking a language which they will understand and which will get their attention much more than if you talked about a database server being at risk from some virus.

Everybody understands what happens if you can't communicate with your warehouse or you can't make shipments. Most people have experienced stuff like that, and it may not be due to information security breaches so much as backhoes digging up cables and stuff. But everybody does have some experience with that, so it's a fairly tangible thing. If they create a redundant communication path to their distribution center, say, they'll assume they have greater resiliency. If they have particular information security software so that their email server isn't going to be affected by a denial-of-service attack, that's of value to them as well, because lots of companies are actually judged upon sending emails out to their customers, advance shipment notices, and they're graded on just how reliable they are in sending out emails, and therefore that's a resiliency business.

Stephanie Losi: Right, exactly. So you can see the benefit is that we can increase resiliency by x, or you will be able to achieve this particular maximum degree of uptime.

Scott Dynes: Right. Another take is instead of investing against resiliency, you can invest in reputation. Reputation arguments are also very effective at enabling business managers to understand the value to the company of investments in information security.

Part 2: The Importance of Mutual Education

Stephanie Losi: Okay, great. And so what would you say — is there a need to educate business leaders about resiliency and about how security can help them achieve it, or can you just go in there and pitch it as such, without that education effort? Do you think education is really part of the solution?

Scott Dynes: Education is a core piece of the solution. The best environment is where both the manager of information security and the business manager are aware of the risks and the mapping of risks from the IT sector onto the business sector.

It turns out that we have actually used such a process at our oil refinery field study partner. It's a process that we call risk map, and essentially what it does is it maps IT risk onto business risk, starting with business risk. So what we did is we went into the oil refinery and with the VP of refining and the CI, or the Director of Information Security, we talked about: what are the top-level business objectives of this refinery? And it turns out they were: stay safe, treat the customers well, make money, stay within regulations.

And then we talked about business processes that actually supported these business goals, and it turns out there's about 17 business processes that support those goals. So for each of those business processes we would go down and we would ask, "So if this business process were to fail, could you still achieve the goal? Is there a workaround? Is there a degradation even if there is a workaround, or if you just can't achieve the goal at all?" And so in that way we kind of categorized the impact of losing each business process.

Well, it turns out that each business process depends upon information flows to work. And so we figured out what the information flows were for each of these business processes; and at this point you're into hundreds, so you actually have to do some level of abstraction. But once you have a manageable list, you go through and say, "Well, if this information flow goes away, can you achieve the business process, will the business –– is there a workaround, is it degraded, or you just can't complete the business process at all?" And so there we have a matrix of information flows to business process.

And lastly, we tie physical IT devices or networks to each of the information flows, and we go through this process where we say, "If this router were to go away or this database were to fail, would it have any impact on this information flow, is there a workaround, is it degraded?" blah, blah, blah.

And so in the end you have this large matrix, which actually allows you to see exactly where the greatest risk is to the business from your IT assets and allows you to – in a very quantitative manner, almost – say, "If we want to get rid of, if we want to mitigate the risk most effectively, where should we invest our money?" And it turns out, after going through this particular process, the Vice President of Refining understood why investing in more secure SCADA devices would be good for his company, because it would lead to his ability to make more oil –- not better oil so much, but it would increase the resiliency of his refinery and he would be able to make more oil.

Stephanie Losi: Okay, so something like this can really be kind of part of the education outreach and part of really giving business leaders what they really want to hear. I mean, that's really what happened here, is that he heard what he wanted to hear or what he needed to hear in order to really understand security.

Scott Dynes: Yes. Also, rather than talking about bits and bytes, they were actually talking about impact to the business. And it was a good experience for the manager of information security as well, because he actually got in and understood the business consequences of a particular thing. And they were very surprised at the things that would have the greatest impact on the business.

In the case of IT managers, the education there is to understand the business. The more closely they understand the business and the business processes and how the business processes are enabled by technology, then the better job they can do of explaining the business risks to the business manager. Educating the business manager as to the risks the business faces from the result of technology I think is very important. Not many managers completely understand how dependent businesses are on technology and what particular information security mechanisms and processes can be used to mitigate that risk.

It's becoming increasingly the case that education in corporations is extending all the way up to the board; so the board is becoming interested in the information security stance of companies as well, which is a very effective mechanism for driving information security awareness down within the organization.

Stephanie Losi: Right. I would imagine that makes it a lot easier to achieve buy-in. If the board is saying, "Do this," then there's really no reason not to.

Scott Dynes: Well, that's true, as long as the board understands particularly what they should be investing against.

Stephanie Losi: Do you think it's hard to help them gain that understanding, or is this part of the education effort?

Scott Dynes: I think that's part of the education effort. Companies come in a variety of – they take a variety of approaches to information security, and it ranges from what we call the sore-thumb approach, where if a machine gets a virus, well, you'll put an antivirus suite on that particular machine; through more IT-centric approaches where you're specifically going out and trying to protect devices, networks against information security; to more enlightened approaches where you're trying to protect business processes. But it's explicitly an information security effort to protect a particular machine against an attack because it runs a particular business process.

Companies that do very well at this actually take a completely different approach where they look at the systemic viewpoint. There are no separate information security efforts, but they're always embedded in a business process effort such that when you kick off a new business process effort, the Director of Information Security is there talking to the people around, "Well, if we use this particular information application then we're going to suffer this kind of risk, but we can mitigate this by doing this."

So, in this way, information security becomes baked into the business process, and as such there's no separate budget for information security because it's just part of the budget for implementing this business process. And as people who program know, it's much easier to correct errors at design time than it is after processes are released. And it's the case here as well.

So just like twenty years ago most businesses were going through kind of quality programs to increase the quality of their products by designing in quality, we think the case is the same here with information security. If businesses take the approach where they design in information security from the start of a business process, it will lower the cost and it'll increase their resiliency. As well, they won't have to make the arguments about information security, because everybody will understand that it's necessary for this business process to work as envisioned.

Stephanie Losi: That would be great, that would really be a successful reframing of the issue, and in that way it would become part of the business process and just part of the way business is done.

Scott Dynes: If you look at people out of the financial sector, they tend to take this viewpoint already. But there are other enlightened individuals in industries even as diverse as the retail grocery industry that take this view as well. So the question — one of the questions we're looking at now is, what is it in these people — is it education, is it just a particular viewpoint they bring to the job — that enables them to build this stuff in from the start rather than bolting it on later?

Part 3: Motivating Business Leaders to Tackle Security Proactively

Stephanie Losi: Right, and what do you think that is? What goes right in those organizations, the ones that really have shifted successfully toward viewing security as part of the business process and as part of just the way things work? But what have they done right?

Scott Dynes: That's a tough question. I don't know the answer to that one quite yet, but I think it has to do with organizations being agile, being open-minded to different ways of doing things. I think there are large organizations that have lots of institutional inertia where things have always been done a particular way.

For instance, we did a study at a healthcare organization, a hospital, where you would think that hospitals would be very attuned to their reliance on information security, on the information infrastructure, and therefore pay a lot of attention to making sure that they had resiliency in the face of things like viruses. But this particular organization did not. It was rather shocking. And I think they've learned their lesson, because they were hit by a worm a year and a half ago and —.

Stephanie Losi: It did not go well.

Scott Dynes: They had a big wakeup call. But it's still very surprising, just very surprising to see the disconnect between the IT organization and the business organization as to what constituted redundancy and continuity in their business processes.

Stephanie Losi: Okay, so one thing that really can jolt someone into action clearly is, as you said, something going wrong like a worm or a virus or a crash. Is there a way, do you think, to sort of provide that spark without having to have a disaster first?

Scott Dynes: Yes. I think one of the keys to enabling multiple businesses to pay attention to this now rather than after the fact, after they experience something firsthand to their detriment, is to share information amongst businesses in a way that enables one business to hear kind of the horror stories of other businesses. Sharing information within particular sectors is very difficult, as firms are very — they don't want to share their horror stories with competitors for fear that the competitors will gain a competitive advantage by bad-mouthing their particular IT operations.

So if we can find a way to provide information — to share information anonymously or in a way that there is no competitive disadvantage, I think that would go a long way to incenting companies to take a rational approach to information security. I think one of the best things that's come about in the past two years has been the series of state laws regarding data breach notification, like starting with California in 2003.

Stephanie Losi: Yes, I think that's right. It was the Senate Bill 1386.

Scott Dynes: Yes, also known as Assembly Bill 700. But I think -- what, 34, 38? — there's a lot of states now that have enacted these laws. And if you actually look at the number of newspaper articles about data breaches, naturally as data breaches became more publicized there were many more articles about these data breaches. But there has also been an increase in the number of technologies to encrypt data on laptops as a result of these data breaches, we think. So it's just — by sharing this information, essentially what you're doing is you're creating market incentives for companies to do better with respect to their information security in this particular arena.

Stephanie Losi: So how do you think the evolving security and business landscapes will really change business leaders' relationship to information security in the next couple of years, based on the things that we've discussed?

Scott Dynes: That's a very good question, that's a very good question. I think in the future businesses will become ever more dependent upon the information infrastructure. Businesses will also become much more integrated with each other. Today you can still find businesses where they primarily communicate with their supply chains via phone and fax. In a few years, that will not be the case. Today you can probably find some businesses that can effectively function if their information infrastructure goes down, but I think in the future that will not be the case either. I think business managers will have to become much more attuned to the landscape that they face, and I think we're still in the early days of the information security age.

Information security, the viruses, the threats, phishing — who knows what's going to come next? But we do know that something is going to come that's not expected today. As a result, rather than protecting against particular things, managers, I think, are going to have to take the stance that they're going to have to protect against outcomes of possible information security events — which is again why resiliency, I think, is a good approach. I think lots of commentators have made the comment that you have to protect against everything, but the attacker just has to find one weakness. Here if you're actually trying to make sure that your business is resilient, then you've only tried to manage the outcomes rather than manage the vulnerabilities, which I think is a very difficult thing to do.

Stephanie Losi: Okay, so how would you say security managers can really proactively prepare to talk to business leaders in that new environment? I mean, what is the biggest challenge that faces them?

Scott Dynes: Security managers need to become very involved in the business. Looking at it from a larger perspective, the IT organizations, the businesses, are in a very good position to understand how information technologies are enabling business processes. If the information security manager can actually go out and place people kind of as relationship managers within particular business units so that they understand very well the risks that business is exposing itself to through the use of particular information technologies, then the information security manager will be able to go and talk about the possible consequences, the risks, the impacts, the resiliency that business has for particular business processes, for existing business processes, as well as working hand in hand with business managers to assure that new business processes are effectively managed from a risk standpoint.

So I think the big thing that information security managers can do is to go around and learn the business by working hand in hand with business managers and the IT folks who support them currently.

Stephanie Losi: Great. Okay, so thank you very much, Scott. I have really enjoyed this conversation, and I think our listeners can learn a lot.

Scott Dynes: Well, thank you so very much, Stephanie, for giving me this opportunity. I hope I have provided some interesting thoughts and things for people to focus on that will help them in their quest for creating greater security and robustness for their firms.

Stephanie Losi: Thank you for being here.

Scott Dynes: Thank you very much.