The ROI of Security
Transcript

Part 1: ROI and Risk Assessment

Julia Allen: Welcome to the CERT Executive Podcast Series. 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. Before we begin, I'd like to let you know that show notes and other supporting materials for today's conversation are available at the podcast website. These include an integrated video and audio version of this conversation in Macromedia Breeze. Please take a few minutes to look these over

My name is Julia Allen. I'm a senior researcher at CERT, working on security governance and executive outreach. I'm pleased today to introduce Stephanie Losi, a journalist and graduate student at Carnegie Mellon in the Information Security Policy and Management Program. Stephanie also works with CERT. We'll be discussing the ROI of security.

So, Stephanie, we've seen a lot in the press and in various publications about ROI, return on investment, and whether or not this is useful to consider for security, which is why we're here today to try and explore that subject a little bit. So how will you be using the term ROI, as we talk today?

Stephanie Losi: Okay, well first of all Julia, I'm glad you referred to it as a useful tool because I'd like to elaborate a little bit and say that it's a useful tool because it enables comparison among investments in a consistent way, and that's really a message that we'll come back to several times throughout this conversation.

Julia Allen: This notion of being able to compare.

Stephanie Losi: Right, compare, and compare consistently. So I'll be using the term to describe the comparison between any expected improvement, such as a decrease in security breaches, for example, after you install a new firewall, versus the cost required to achieve that improvement.

Julia Allen: Okay, so we're going to compare the fact that we don't experience as many breaches once we put the firewall in place, and compare and contrast that with what it actually cost us to both purchase the firewall, but also maintain it.

Stephanie Losi: Right. Because this is security, we won't be measuring this as a concrete gain; it'll more be expressed as a reduction in risk.

Julia Allen: Okay, so risk is obviously one of the key concepts. And so how do I know what to measure, and how do I know if a security investment is really going to help me reduce my risk? That seems to be really fundamental. A lot of times it just seems like we're guessing or using someone's opinion or some market survey. So how can I relate this all back to risk?

Stephanie Losi: Okay. This does relate closely to risk assessment, and basically your risk assessment will depend on your individual company or industry. You'll need to take a look at, well, what are my risk factors, and how will I prioritize them? If

you're Coca-Cola, your top risk is probably leak of a trade secret; if you're eBay, your top risk may be downtime because that would cause so much lost revenue. So the quality of your risk assessment will really determine the quality of your ROI analysis.

Julia Allen: Okay, so it sounds like I really need to think about what's important to me and what kind of risks or threats or consequences could occur. Is that kind of what you mean by a quality risk assessment?

Stephanie Losi: Exactly. And I'll go into a little bit more detail. A high quality risk assessment, there are several points about one. One, it's sponsored at the enterprise or business-unit level. It's a high-level thing; it's really got some top-down support. Two, it identifies the most critical information assets and where those assets are most at risk. For example, like I said, it might be trade secrets; it might also be customer data or a custom application that your company has written. It depends on what is your business, what do you do, what is critical?

Julia Allen: So it's basically those kinds of assets that the underlying most critical business processes, the services that I offer, the customers that I service, it's the things that provide that value to the market -- those are the things I'm trying to tease out and understand in my risk assessment.

Stephanie Losi: Right. Number three, it prioritizes protection action that needs to be taken. So that's a necessary thing for a high-quality risk assessment. And number four, it does so on a recurring basis. You can't just do it once, you have to come back to it again and again, over time, at periodic intervals.

Julia Allen: So, for example, if I discovered in my risk assessment today that my customer database was my most critical asset, based on some new product offering or services that I was putting out there, you're saying that might not necessarily be the case six months or twelve months from now, based on changing landscape?

Stephanie Losi: It might not be that your most important risk factor changes, but maybe number 8 becomes number 10 and number 11 becomes number 7, and that's important to know.

Julia Allen: So that would change where I'd want to invest my security dollars and what protection actions I'd want to take, based on that shifting risk assessment result.

Stephanie Losi: Right, yes.

Julia Allen: Okay, so I've got- clearly risk assessment and its findings are going to be the foundation for my ROI calculations. So what are some of the risk factors or what are some of the things that I might want to consider measuring? You've mentioned a couple already.

Stephanie Losi: Okay, there can be many; you could choose just to measure 100 risk factors. I'm just going to name a few here to kind of kick off some thoughts, and also these are some that are probably pretty widespread across companies and across industries. One is lost productivity from downtime. For example, if your system administrator suddenly has to run and put out a fire because you've had a security breach, they're not doing the mission focused work that they were doing before. So I would call that lost productivity.

Julia Allen: So you basically have a double hit because they're being taken away from mainstream work and they're having to attend to something that they hadn't planned to.

Stephanie Losi: Right. And there are a few others that I'll just run through really quickly. One is, as I said earlier, with the eBay example, lost revenue from downtime. Another might be loss of data through downtime, corruption or destruction. Another is compromise of data through disclosure or modification. You might have repair costs after a breach if hardware or software has been damaged, or you could lose some reputation if the breach becomes publicly known. We've seen that recently with the VA.

Julia Allen: Right, there are lots of cases of stolen laptops and other types of data getting into the hands of parties unknown and not knowing if that will result in cases of identity theft or identity fraud. People are really concerned about that.

Stephanie Losi: Right, and that can be devastating, based on the theft of one laptop.

Julia Allen: I understand. So it seems like we could go quite the distance on all of these different risk factors. As you said earlier, there could be 100 of them or there might be just a critical few, based on the assets. So how do I know when I'm done, how far to take this?

Stephanie Losi: Well, that is up to you. This is where the risk assessment portion really comes in. You have to say, "How far do I want to go in measuring my various risk factors?" You might choose to measure 20 or 30 risk factors, or you might choose to measure 100, but you'll be the one who has to decide.

Julia Allen: So it really just comes down to what's most important to me.

Stephanie Losi: Right.

Part 2: ROI Methods

Julia Allen: So, Stephanie, we've talked about risk assessment, we've talked about risk factors, we've talked about various ways to think about how we might calculate ROI. So let's get a little more in-depth and talk about some of the methods. So are there some methods that you can summarize for us that we could use to measure ROI?

Stephanie Losi: Sure, I just want to talk about two here. One is called payback, and one is called net present value. I won't go into too much detail because we have examples of each of these methods, in the show notes, with all the detailed calculations. So you can look there to find out more.

Julia Allen: Yes, right, and sometimes when you're listening it's a little hard to grasp all the numbers, so I'm glad that we can look somewhere else to see some concrete examples. Well, then, let's take the first one, let's talk about payback. What is it, and how might I use it to help me come up with a return on investment?

Stephanie Losi: Okay, payback is a fairly simple calculation. What it does is it compares something called the annualized loss expectancy with the expected

savings as a result of some security investment, and if the savings are greater, the ROI is positive.

Julia Allen: Okay, so annualized loss expectancy, that's kind of a new term. Can you define that for us?

Stephanie Losi: I certainly can. Annualized loss expectancy is equivalent to the probability of some negative event happening, multiplied by the cost of the negative event, if it happens. So we might look at, for example, the probability of a password compromise happening. And so let's say expected savings are expressed as a reduction in the chance of that. So if, for example, the company has a 90% chance of a password compromise in the next year -- and it might have come up with that figure through its risk assessment, as we discussed earlier --

Julia Allen: Okay, its risk assessment or maybe historically they had some password compromises and so they've got some historical data…

Stephanie Losi: Some data.

Julia Allen: …data to draw from -- okay.

Stephanie Losi: Right. So you would take the probability of the negative event, which would -- which they've determined to be .9, and they would just multiply it by the cost of that negative event, if it happens.

Julia Allen: Okay, and again the cost might be something that I either know from my own experience or maybe benchmark data or market surveys.

Stephanie Losi: Right. And then expected savings would reduce the probability of that event happening. So for example, a vendor might come to them and say, "Well, we have this security awareness training program that will teach your employees to really use strong passwords." So if the company signs on with that, the vendor might say, "Well, our historical data at other companies with this program shows that we can reduce your chance of a password compromise to about 30% per year." So then you would do the annualized loss expectancy with the lower probability.

Julia Allen: Okay, so I'd be comparing the 90% likelihood of this password compromise occurring without any security investment to the -- at least the promised or the anticipated 30% if I did put the awareness program in place.

Stephanie Losi: Right.

Julia Allen: Okay, so likelihood or probability -- you're playing with that factor, but you mentioned in the payback calculation there's also the cost factor. So is there anything I can do about that?

Stephanie Losi: Sure, you can sometimes express savings as a reduction in the impact of some event happening. Let's take a look at an earthquake, for example. If your company is located in an earthquake-prone area, you really can't do anything about the chance that an earthquake may happen.

Julia Allen: Okay, so the probability will stay constant -- there's not much I can do about that.

Stephanie Losi: Right. So instead, what you would want to take a look at is reducing the impact, and that's sort of expressed as a reflection in the cost of the event. So you might say, well, instead of storing our backup tapes merely offsite, we're going to store our backup tapes offsite in a geographically distant area.

Julia Allen: Okay, so in that case again my probability would stay the same but my cost -- the cost of the negative event -- that would go down.

Stephanie Losi: Right, if you lose data in an earthquake disaster, you would find it easier to recover because your tapes would likely be safe.

Julia Allen: Okay, so in that case I could still do my annualized loss expectancy calculation, compare the before and after, before I took the action to move my tapes to another location, versus after I did that, and I would get the same net effect as what you described for the password compromise on the awareness class example.

Stephanie Losi: Right, it's like turning two dials, two knobs, you can turn either the probability knob or the cost of the negative event knob, and you can try to arrive at a level that works for you.

Julia Allen: Okay, well, that makes sense because like you said, there's some events that you can't change the probability on, it's basically a given.

Stephanie Losi: Right.

Julia Allen: Okay, so you said you'd tell us about two methods, and we've talked about payback. What about the second one?

Stephanie Losi: The second one is called net present value or NPV, and all this does is it takes into account something called the time value of money -- that's the only difference from payback. And what that means is that money tomorrow is worth less than money today. For example, I mean, you can see it in a salary cost-of-living increase- $50,000 that's made next year is worth less than the same $50,000 made this year. That's why you have a salary cost-of-living increase.

Julia Allen: Okay, so it's the same basic idea as inflation. If I buy something today versus I buy it a year from now, my dollars just aren't going to go as far next year as they did this year.

Stephanie Losi: Right. And the net present value effect applies to both savings and costs. So you can say -- for example, if you can push a constant to the future, $10,000 spent a year from now is worth less than $10,000 spent today. So you actually have saved some money.

Julia Allen: Okay, so this whole notion of the discount value or the future value of money I can apply to both my cost and my savings is what I hear you saying.

Stephanie Losi: Right, exactly. So it gives you basically a more accurate read on the value of all present and future savings and costs in today's dollars. That's really the value of NPV.

Julia Allen: Okay, so really this -- you've got payback and NPV as two examples that I can use to calculate ROI, and I'm going to make those calculations. But what's a reasonable period of time that I can actually find them useful or trust that they're going to inform me in any reasonable way?

Stephanie Losi: Longer than a year and shorter than five, I would say; and that may sound a little simple, but I'll explain what I mean. Basically, longer than a year because if you're using, for example, NPV, the whole benefit is that you want to basically look at the value of your present and future savings and costs. And so you can't do that if you don't have a long enough time horizon. If you go out five years or more, generally other business factors may change, the business environment may change, and so you may just find that you have a less accurate calculation. You're moving more toward just pure estimation.

Julia Allen: Right, the numbers were estimates and somewhat subjective to begin with; so the longer you try and play them out, probably the less accurate they are.

Stephanie Losi: Right.

Julia Allen: Okay, so I think I understand what you're saying. So you do either a payback or an NPV calculation and I find out that my ROI is positive; so, voila, I go ahead and make my security investment -- right?

Stephanie Losi: Not necessarily. There are some wrinkles, and one of the ones that I really want to point out, there are a couple of economists at the University of Maryland named Lawrence Gordon and Martin Loeb, and they've done a lot of studies on the ROI of security. And what they found is that a security investment is only worthwhile if the cost turns out to be 37% or less of the expected savings.

Julia Allen: So about a third.

Stephanie Losi: About a third. If you calculated, for example, with our training program example, that you would save $10,000 by implementing it, you actually should only invest, according to Gordon and Loeb, if the program cost $3700 or less.

Julia Allen: So I suspect that derives from, again, some of the estimated nature and the subjectivity and some of the numbers. So to really make it worthwhile, it's not just a net positive.

Stephanie Losi: Right.

Julia Allen: But it's really about a third of the value.

Stephanie Losi: Right. It should be significantly positive.

Part 3: Using ROI in the Real World

Julia Allen: Okay, so Stephanie, we've talked about -- we've laid the foundation with risk assessment and talked about being able to use things like probability and probability of an event and cost of an event and play with different variables to get a good either payback or net present value calculation. So let's talk about some more tangible applications.

Stephanie Losi: Okay.

Julia Allen: So let's say we've used net present value, we've got some good ballpark measures, but I get the feeling that it may be hard to get to the right numbers, or then I ask myself, or is having the right numbers even the main point in doing ROI?

Stephanie Losi: Right, well, you're actually right. The value is not necessarily the hard numbers themselves. I wouldn't say that. I would say the value is in two things. It's in first of all the quality of your risk assessment. As we discussed earlier, a good thorough risk assessment will lead to meaningful results, whereas a poor risk assessment will lead to misleading results. And the second important thing, and I actually think this is maybe the most important, is that you want to have consistency, you want to have consistent use of this same ROI measurement method across multiple projects, because that will provide a meaningful comparison among the alternatives.

Julia Allen: Okay, so when you talk about consistency, you want to make sure that you use -- if you're going to use payback that you stick with payback; you want to make sure that you're using comparable or similar risk factors.

Stephanie Losi: That's true, right. If you consider lost productivity for one investment but not for another, that comparison is going to be misleading no matter what ROI method you used.

Julia Allen: Okay, so let's say I used lost productivity as one basis for investment, but let's say I have another investment option coming up as a result of a customer database compromise. Are you saying that I really couldn't compare those two investments, or is there an instance where I could?

Stephanie Losi: Well what you'd want to do is you'd want to say -- if you have a customer database compromise and you consider lost productivity, and then you have a different kind of compromise, and you don't consider lost productivity, that's going to be misleading; whereas if you do consider the same risk factors for both, then you'll have a meaningful comparison.

Julia Allen: Okay, so I could have a variety of losses.

Stephanie Losi: Right.

Julia Allen: Based on a particular event. But if I'm looking at a security investment to help mitigate those losses, I have to make sure that the bases I'm using to compare are consistent.

Stephanie Losi: Right. You have to use a consistent basis based on a good risk assessment, and then you have to use the same method to measure them, be it payback, NPV or another method.

Julia Allen: Okay, so I got -- I think I understand what you're saying about consistency. Now can I just jump into an ROI calculation at any point in time? If I have -- like let's say we had an incident last week and we just learned that there is a vendor approach that would help us mitigate against that. Can I just jump in anytime and do ROI, or is there a particular point in either a project or investment lifecycle where it's more effective?

Stephanie Losi: Up-front is best, always up-front is best because that will give you a baseline to work off of. Now, if you haven't done an up-front calculation, you can jump in in the middle and you can say, well, let me get a handle on this and let's try to figure out where we are so that in the future we know where we were and where we want to go. So you can say, well, okay, we're going to do our ROI analysis right now; you might not have the clearest idea of what return you were supposed to get, necessarily, based on certain factors, because you may not have done a systematic measurement of all of those factors in a full ROI calculation before.

Julia Allen: So like let's say I had a breach now and I'm in the middle of some project lifecycle. You're saying that I may not have all the basis information that I need to do an effective ROI calculation, as if I had done it either earlier in the project or earlier, before I decided to buy the security technology.

Stephanie Losi: Right. It would have been better to do it before; however, that does not mean you can't do it now. You can do it now, and it will be useful to you, and it will especially be useful as you go forward and do additional ROI analyses in the future.

Julia Allen: Okay, might it make sense to use ROI as an instigating factor or as a catalyst for starting to collect some of this historical data that I need for future calculations. Would that be a positive benefit?

Stephanie Losi: You could do that, and you will gain historical data as you go forward because whatever you collect during your baseline ROI calculation, whether it's up-front, before you begin an investment, or when you just -- when you realize that you really should do an ROI calculation, then you jump in to do it -- either way you're collecting data that later will become part of your historical record and that you can use in future calculations as more of a concrete asset.

Julia Allen: Okay. So I can almost start to build a repository of information that I can use to draw from for subsequent analyses.

Stephanie Losi: Right.

Julia Allen: Okay. So I really get your point about consistency; it makes sense, I want to compare across similar methods, I want to compare across similar risk factors. But we've talked all about this recurring nature -- I want to do my risk assessment on a recurring basis. The marketplace is constantly shifting and changing, I may have a new partnership or a new product line. So in the face of a need for consistency, I've got all this dynamic change. How do I cope with that?

Stephanie Losi: One of the best tools is your security policy because once something is in policy, it's harder to change it. And so that's how you can use the policy to allow continuity beyond any one person's tenure, be it the CEO, the CIO, the CISO -- it doesn't matter. If it's in the policy, it's hard to change. And this is how the corporation does it, and they'll really have to make an effort if they want to overhaul that and do it a different way.

Julia Allen: And have it be a conscious decision?

Stephanie Losi: Right.

Julia Allen: So part of this dynamic environment is a change in senior personnel and so you're saying if -- one of the ways to help me kind of ride through those changes or have some consistency is to make sure I've got this established in policy.

Stephanie Losi: Right, because that will give you consistency and it also will make sure you have a rationale for any changes that are made.

Julia Allen: Okay, well, that makes sense. Is there -- if I wanted to pursue this further or find out more about it, are there some additional resources that I could go to?

Stephanie Losi: Sure, you can take a look at our show notes for the example of calculations, as we stated earlier, for payback and NPV, and you can really get into that, and we have some good mathematical examples of how those work. We also have an OCTAVE website at Cert.org, and you can get some information about risk assessment there, because we also talked a lot about risk assessment in this conversation, and you may have some questions about that. If you want to take a look at a security policy template, we have adapted one of SANS templates into a sample policy that deals with security ROI considerations.

Julia Allen: Oh, that'd be good to have, just to see something more tangible.

Stephanie Losi: And you're free to go to our podcast website and download that and use it as you wish. But keep in mind that it's only a starting point and not a binding document. You should definitely adapt it to your particular company or organization.

Julia Allen: Well, because every organization's going to have different risk factors, as you pointed out.

Stephanie Losi: Right.

Julia Allen: And different things that they're trying to protect, so they would need to interpret accordingly.

Stephanie Losi: Right.

Julia Allen: Well, thanks a lot Stephanie. This has been very interesting, and I look forward to more conversations.

Stephanie Losi: Thank you.