IT Infrastructure: Tips for Navigating Tough Spots
Transcript

Part 1: Mastering Merger Hazards

Stephanie Losi: Welcome to the CERT podcast series, "Security for Business Leaders." The CERT Program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Stephanie Losi. I am a journalist and graduate student at Carnegie Mellon, working with the CERT Program. I am pleased to introduce the two Steves: Steve Huth, CERT's deputy director for operations and former I.T. manager for the Software Engineering Institute; and Steve Kalinowski, CERT's IT manager. Today we'll be discussing how to build and sustain a secure IT infrastructure. So I'd like to just jump in by asking: What are some of the most critical security issues that business leaders need to tackle when they are building a new I.T. infrastructure?

Steve Huth: I guess I'd first like to suggest: Do you really know what assets are involved? You're building this new infrastructure out, and almost by necessity there are going to be things brought in that maybe you haven't really thought through. So you might have considered part of putting your customers' information on the web to make it easier for them. But you also have to step back and say, "Okay, what does that do, putting that information out there, to my overall security profile?" So look at it from the assets that you're holding.

Stephanie Losi: And I would imagine that in a merger or an acquisition that would be another issue that you would have is you don't know everything that the other company has.

Steve Kalinowski: Exactly. And it's interesting, when you consider a merger, we go back to the assets. The combination of assets from two companies, especially if they were complementary or competitors, may be more valuable than each of the individual assets. So in order to afford yourself the best protection and actually direct your money and your resources in the early part of that acquisition or merger, where the most value occurs is where the asset is, because by definition that *is* where the value for the business is. The class of information that you have to share, and the mechanisms by which you do it, change your vulnerability profile.

Steve Huth: There're a lot of fun things that happen when you're bringing these new groups together. And I guess I would suggest this is a good opportunity to actually step back and look at a lot of different things. So, for example, your business processes – this has been true in the software world forever, where people know that they ought not to build software that just sort of codifies bad business practices. But there's a lot of push to get this software out the door and get these things out the door.

So when you're putting [together] two organizations or you're developing a new infrastructure in general, it's a good time to step back and say, "Do my business processes really work?" And, in fact, what we've seen a lot of is over time these odd little pieces get added for special cases. And so you have a business process that at one point might have been very streamlined that now becomes very cumbersome. And you have a lot of, for example, databases where things are scattered all over your organization and there might be valuable customer information in four or five, I've seen 18 or 20 different places. Not only is that really bad from the customer management point of view, but from the security point of view, each one of these now has its own things that you have to worry about.

So maybe this is an opportunity to look at what you're doing, consolidate some of that, streamline the business processes, and streamline the technology. So there's a lot to be said for, again, taking that step back before you just jump right in and start putting things together.

Stephanie Losi: Oh, go ahead.

Steve Kalinowski: I was going to say there's an interesting hook on the whole business awareness issue because in a merger, you have two separate IT organizations, and there's a whole lot of personnel management effort to try to get those to cooperate as one because, invariably, by efficiency, some people are going to be pushed out.

Steve was speaking earlier about the business processes. The combination of business processes may be handled very well at the, what'd you call the C level, but if the IT folks – most specifically the architecture people in that domain who are going to help you build those new processes and the technical underpinnings, I guess is a reasonable term for it – they need to be aware of the business process, because if they each come to the table with only the piece they knew from the old organization, you'll actually have three sets of ideas around the table, and that can't possibly work out well in the long run.

Steve Huth: You also said something that triggered one of the insider threat notions. It was found, from the work that we did with the Secret Service, that many of the insiders – their malicious activities were triggered by some sort of work-related event. And as you suggest, you're putting these two groups together, people are feeling threatened, and that –

Stephanie Losi: It's a pretty big event.

Steve Huth: It's definitely a big event. But also, you have people that had been granted access, and in a lot of cases you give system administrator access. But unfortunately, too many groups don't think about going back and taking it away. And so now here again, you're bringing together these people. They've had these levels of privilege for a long time and it's a good opportunity to go through and say, "Are these levels of privilege really required to do the job that you need to do now?" And so it's something that makes it a good time to have that conversation with people. But, again, you do have to be careful because people do sometimes react very badly to those sorts of things.

Steve Kalinowski: Well, it's a delicate process, and sometimes that message isn't delivered very well. I mean, if people don't understand that it's not a matter of whether I trust you as an individual, but it's whether it's reasonable for your role to be trusted or to be involved in that process as opposed to some other thing that might be even more interesting for that person. It's a big deal. I mean, the way you deliver that message has a lot to do with how many people you irritate. How many people you irritate may change your insider threat vulnerability, or it may make your problem a lot worse.

Stephanie Losi: So what do you think are some good ways to sort of deliver these messages that may not be welcomed by everyone? How can you sort of smooth things over and really ensure that you're going to have a good transition?

Steve Huth: Well, I try to send Steve in to deliver the message, and –

Steve Kalinowski: And then we count the arrows in my back, and then we know.

Steve Huth: Well, first of all, there may be opportunities before you get involved in any of this to lay some of the groundwork. So, for example, one of the things that we do is have standing practices that say, "When your role is changing, we're going to reexamine things." And that's true whether your job functions have changed or perhaps you're transitioning out of the organization. So maybe now is a good time to look at some of those issues before you're in a situation where you really need them. And then it's already in people's minds – "This is the way we normally behave" – and so it's no different when we're coming into this awkward sort of business situation.

But I think what Steve said, really, is key, the fact that this is not a personality-based thing. So, "You have to keep in mind that we're treating all of our employees the same way. We're reviewing my access just the same as we're reviewing your access." And then it starts to remove a little bit of that. And there's a real opportunity to lead by example. So, for example, there are places that Steve has access to that I don't. So when people look at our roles they say, "Well, Steve, you're here. You ought to have access to everything." Well, no, I actually don't need access to everything, and other Steve has more immediate needs, so he has accesses that I don't.

Steve Kalinowski: Right, and in truth, you do have access, but you have it by following a particular process. You need to go through the facilities security organization, have them grant you access so that you can do what you need to do. You would be escorted, that event would be logged, I would be aware of it. So the opportunity for you to do anything that would be untoward is minimized. And the way we would treat you that way, any – we treat you the same way in terms of our rigor with visitors and other folks. And you're right, it sets up a condition that we're trying to create processes that are efficient, and we're trying to create [processes] that are repeatable.

Steve Huth: And so now people when they look at us, they don't see me because of a particular position being able to do things and they say, "Well, what is that?" So, again, it tends to make those conversations just a little bit easier. Also, though, if you have a good HR department, getting them involved can be really beneficial because, again, they provide something of a different perspective, and they can provide you more of that employee-focused perspective. So you can say, "Okay, here's what we're planning to do. Here's the impact that it's likely to have." And they can say, "We've been through this a lot more than you have as a technologist. Here's how your people may react." And so there have been times when we've stepped back and said, "Hmm, okay, maybe we want to rethink how we're going to do this particular activity." So getting those folks involved is often a good thing.

Part 2: What to Do When You Inherit Trouble

Stephanie Losi: What if you go in and something – everything is just really messed up? What if you are given like a mess to start with? How would you– what are some good techniques for dealing with that?

Steve Huth: Well, let me suggest one of the first things that you'll want to do is listen. I've come into several organizations and been asked to make changes. And it is without a doubt the case that I have a very different perception after having gone through it, discussed things with people and understood at a level what was going on, much more so than I had going in. So I think the sort of bull-in-a-china-closet approach – it, at least, it doesn't work for me. It's – come into the organization, talk over things, not just with the management level, but with the people doing the actual work, and then you often have a better understanding of why things are. And oftentimes you'll be surprised. The folks working on the line, they usually know why these messes exist. And they're as upset about them a lot of times as you are. So all of the sudden you're in a situation of saying, "Hmm, so I don't like this. The people that brought me in don't like it. The people that are doing it don't like it. How did we get to this position?"

And so you approach it, again, not from a people-centric thing, but from a process-oriented thing and say, "Okay, the processes are broken. Let's sit down and try to work through them and decide how we can make it better."

But I will tell you that, again, some of the insider threat studies have shown somebody that is perhaps a bad actor in the organization will also use some of those same behaviors to protect the activities that they're doing that might not be on the up and up. So there are documented cases where somebody is acting like, "Well, you don't trust me. And how could you do this and this, and things are messed up but I'm working real hard," and really sort of pushing back in a way that is indistinguishable from somebody that is just nervous about their job. And so when you dig a little deeper, you find out that their pushback is the result of them trying to hide activities that they really shouldn't be engaged in. So you have to be kind of careful. People's motivations can vary pretty wildly in all of this.

Steve Kalinowski: Well, it's interesting, too, that your entry into both of those situations, whether the person is legitimately overloaded or hiding something, can be empathy. Because from your perspective, you don't want to assume that the person is guilty of some nefarious deal, and you just want to find out how can you make their situation better. If they're always turning their back to you when you're trying to do that, that should be a signal that there's something going on that they don't want you to see.

Steve Huth: Now, again, if you're handed a mess, a lot of times what you want to be very careful of is: You immediately put in place a good change management process. Because just going in and sort of willy-nilly saying, "Well, this is broken. We're going to throw it out and fix this," can introduce security vulnerabilities.

One of the things that I've seen in a lot of different places – for example, in router configurations – is they're not well documented and they've been put together for specific reasons that grow over time. So you can take the approach that, "Well, we're just going to go in here and clean house." But for everything that you've fixed, you may have introduced some new and unexpected vulnerabilities, that that router may have been your only line of defense. So, [implement] a very good change management process where you say, "Okay, I understand this piece of it, and if I make these changes, here are the things that will be affected."

Stephanie Losi: Okay. And what if you can't do everything you would like to do? Like you come into a situation, you can see that there are many things to be done, but you may not necessarily have the resources to do all of them. So how would you go about making those trade-off decisions and prioritizing security investments? Yes?

Steve Kalinowski: I think Steve wants to answer that.

Steve Huth: Well, Stephanie, that's always the case. And Steve and I can laugh because we've worked together for a long time and there has never been any situation where you have all the resources to do what you want. And, in fact, I've had some very savvy C-level people say, "And if you do have the resources to do everything you want, we're actually giving you too many resources." There's no company where that's the case.

So there are some very good structured methodologies at– looking at your particular situation and deciding – based on, again, what your assets are, what the threats might be, the vulnerabilities –

where you should go first. Here, I'm going to advertise a little bit the OCTAVE method that CERT has developed. We've used it both internally and externally and found it–

Stephanie Losi: For risk management.

Steve Huth: Yes, absolutely. And found it to be a very good way of focusing in on what the critical threats and vulnerabilities really are. And then we can say, "Okay, I'm willing to accept a risk in these areas because even in the worst case, if there's some damage done here, it's not going to affect me too badly. Whereas these other areas I really want to focus. Here's where I'm going to spend my time. Here's where I'm going to spend my money."

The other thing that I really like about it is it doesn't require a cast of thousands. So doing something like OCTAVE you can do it with a small number of people. You can really narrow it down and say, "Okay, I'm going to look at this subset of assets," and really, in a couple of days' worth of effort, come up with a pretty good plan for, "Here's what I've got. Here's what my risks are. Here's what I'm going to do to mitigate those risks." And then you can decide, you know, how much further you want to take that into the organization.

Part 3: Business-Side Buy-In and Tone from the Top

Stephanie Losi: When should [non-technical] business leaders really actively participate in infrastructure security actions versus delegating the responsibility to the CISO or the CIO or the IT manager and saying, "Well, this is your job. You go do it."

Steve Kalinowski: Well, I think that you definitely want to have [non-technical] folks at the C-level involved early in the process because these – the rules should be governed by the business processes you're trying to protect, which are governed by the assets that you're trying to manage. That has to be defined by the folks who have responsibility for it. There are actually, in some cases, regulatory requirements for that to be the case. Once there are reasonable rules set into place, though, general operations and implementation of the technology that's required to meet a policy can probably be safely delegated as long as you trust but verify. I don't know if you would want to extend that, Steve, at all.

Steve Huth: Well, there are a couple of things I believe, and I do believe that all of this works better if you have active participation from the business side of the house. And by that I mean whether you're doing risk assessment, whether you're building a budget, whether you're developing a plan, doing it in isolation never seems to work very well.

And, again, when you go through things like OCTAVE, one of the things that is required is that business perspective, and those are the people that say, "Here are the real assets that I care about." It's good as an IT professional to have an idea about that. But the bottom line is, that is somebody else's call as to how to rank and order these things.

Also, I think it's a good idea always, when you're working at the policy level, to have that business leader's perspective. And if that's done well, then the rest of the IT functions can go off and carry out what it is that you've defined in policy.

The problem is policy is hard. And it takes a long time to do, and it's something that we worked on for many, many years, and there seems to be no silver bullet that I'm aware of. There's some good places to start, like the Wood books on policy and some of the things available on the web. But you really have to sit down for your organization and, again, talk to the business leaders, talk to the technology folks, and really try to put together a policy that's going to work for everyone. And that's just time consuming.

Steve Kalinowski: You're right, and it's an iterative process, too, because if at time T-zero you can have the perfect policy, if your business is evolving either by growth or reduction in some cases, it's going to change. So it's a constant vigilance thing when it comes to managing the policy.

Steve Huth: So going back to your merger question that's, again, one of the things that people have to consider. A lot of times you'll see as an organization, for example, might be absorbing a smaller R&D group, and that group was probably running pretty fast and loose, nothing in the way of policy, relatively few computer controls, but producing wonderful things. And then suddenly they're going to be brought into this other organization that might have been around for centuries and they have a lot of things really solidified in the policy and process world. And it's not just a culture shock. It really is something that can potentially introduce new vulnerabilities as people are saying, "Well, I'm not going to do this. I never had to do it before, why should I do it now?" And whereas before what might have been exposed was some experimental code that was probably available on SourceForge anyway, what now might be exposed is some critical, patentable technologies that the parent corporation has and this person may have access to.

Stephanie Losi: Okay. And so how do you think that that can be successfully spanned, that period of time where people come in and they are not happy about it? They may be saying, "Well, no, we are not going to do that. This is the way we've always done it, and we're just going to continue to do it this way." How do you get from that to them feeling like part of the overall infrastructure and understanding why it's important to follow the policy?

Steve Kalinowski: That's a tough one. Organizations, even when you're not talking about policy, sometimes you have to change out certain of the leaders because they can't evolve to that next level. One would hope that you could avoid that by a bit of transparency and – again getting back to the trust building thing – "This is about us trying to do something at the next level."

Steve Huth: One thing that we have seen some success with is explaining a little bit of why the policy exists. The problem with a lot of policies is they really are – they're very dry. They really tell you what to do and what not to do, but they don't often go into the why. And so we've done things from time to time using cases to illustrate what it is that happens when this policy is not adhered to.

Stephanie Losi: Do you know where can our listeners learn more about this topic?

Steve Huth: Well, we have several things that we put together to give you to put into the transcript. Certainly, the CERT website, especially for things like OCTAVE, is a good place to look. So if you look at the evaluations and practices, you'll see all of this information that can be downloaded. So a good place to start. Looking at things like ISO-77–no, it's now 17799. And just doing a search on that on the web will give you a lot of good information.

One of the other things that I'd respond is the Information Security Forum has a standard of good practice for information security. And it's worthwhile reading it because they're just small snippets of things, and you can say, "These practices really are very germane to the kind of work that we're doing here." And so use that to take this whole world of information security and focus on the areas that you think might be worthwhile and then go from there.

Steve Kalinowski: CIO magazine is also interesting because they often include first-person accounts of situations that I've more than once read and had been given pause, because it really is a business of people. It's not a business of machines.

Stephanie Losi: Well, thank you very much. I appreciate your time, and I'm glad you both could come here today.

Steve Huth: Thank you.

Steve Kalinowski: Thank you.