

The Human Side of Security Trade-Offs Transcript

Part 1: Raising Awareness and Motivation

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 graduate student at Carnegie Mellon working with the CERT Program. Today I am pleased to introduce Greg Newby, Chief Scientist at the Arctic Region Supercomputing Center at the University of Alaska. We'll be discussing the human side of security and what that means for business leaders. So, Greg, you conducted research on the human factors of security, and you've given talks on this subject. Can you describe what that means and why this topic should be of interest to business leaders?

Greg Newby: Fundamentally, security is about people. It's not really computers that are breaking into different systems, it's people. It's your adversaries. It's often actually your insiders, people that work for you. So understanding the motivation of those people and, I believe, training your people – people you trust, people that work for you, yourself, your employees, your contractors – to be proactive about security is one of the very best paths you can take to maintaining a good security stance.

Stephanie Losi: And so what would you say are some ways to, within the company, get people to recognize security as an important issue across the board? I mean, maybe some employees may not see it as an issue and may not really be inclined to comply necessarily with a policy or a procedure. How can you motivate all your users to see the importance there and to kind of take action in their own behaviors?

Greg Newby: It's a difficult challenge because people have different levels and types of activities involving computers and various other things that we need to keep secure. And it's not always very clearly in their job profile to be diligent and very well informed about security. In the organizations where it really matters, I think, people do take steps to say, well, "Security is your business." You have to keep an eye on who's coming in after hours, who's following you behind the door, be conscious of things like social engineering or phishing on the telephone and of course be diligent with things like spam and viruses in your email.

For people that are more deeply involved with computing, certainly people in the technology, software development, people doing web and ecommerce, that sort of thing, these folks do need to make security a primary part of their business because the risks are so much greater. The exposure is so much greater.

So I think we need to consider a multi-pronged approach where people who are very deeply involved with the technologies or have the ability to sort of make or break the security profile, those technologies do need to be trained and that training needs to be diligent and refreshed and part of their position. For folks who are not in that type of sensitivity area, then probably it's okay just to do what you do for almost anything – safety in the workplace, give periodic updates and so forth, and then design your systems so that those folks that are less well informed, less well trained, can really do no harm.

Stephanie Losi: Okay, and then in terms of designing those systems, we're always talking about here, people, processes and technology that make up a system that you might call a security system. What would you say are some of the best ways to motivate the people so that they create the best systems?

Greg Newby: Well, awareness of course is key. But the other thing is that there's a certain element of freedom, of really fun for the system designer, if they can put themselves in their adversaries' shoes. And this is one of the very best practices that you can engage in, is to say, "Okay, well, I'm designing maybe some software. I'm designing a website. Let's give some thought to what could go wrong. Let's give some thought to illicit input that could be generated. Let's give some thought to what an attacker would do if they were trying to break into my system, get access to my secret data." This can be fun, and actually it is what the people that do war fighting would call a game. You're doing gaming, you're doing scenario planning and trying to anticipate the next move of that potential adversary.

So I think making that part of the design process: not just doing the sort of straight through "Here's what we hope will happen. Here's what we think will happen during legitimate use." But [rather], "Here's what could go wrong, and here's some of the unintended consequences of the problems that could be created by going somehow outside of the boundaries of the system."

Stephanie Losi: And so how can business leaders really support that process? How can they give the security personnel what they need in order to be successful and think outside the box like this?

Greg Newby: I think there's two approaches. One is to hire people or seek to hire people who have a profile similar to that of your potential adversaries. So really what that might mean is, if you're worried about hackers – people that have very good skills at circumventing systems who are out there and maybe attacking you – well, hire some of those folks with the same skills. And, of course, you're hiring people that are going to be ethical and onboard and very much a part of your team, not someone that's going to be a security risk. But you want people with those same skills so that they can game your system, so that they can try to think like that adversary. I think that makes a lot of sense for very many organizations. I also think that there is somewhat of a hesitation because maybe those folks won't fit quite as well in the corporate culture. The approach there is to outsource and to say, "Okay, we're going to go out on and go to a security firm. And we're going to hire people to test our software. We're going to hire people to try to penetrate our systems." And that could include, we hope, not just clicking around on the website, but also looking at things like dumpster diving and phishing and social engineering and all of the different potential areas. And I would not leave out from that plan, in either case, the corporate espionage and the insider risks. Having someone on your internal local area network is very often where the big danger, where the big damage comes from, as opposed to someone clicking around on your website.

Stephanie Losi: How can you identify those people? And you want to hire people who are going to help your organization and then not be insiders. So what would you say are some good ways that they can do that?

Greg Newby: Well, today's modern information systems are complex. They're seldom created and maintained just by one person, except in the smallest cases in relatively new businesses or small businesses. So when you're thinking of the composition of your team for a new product or maintenance of an existing product or upkeep or what have you, then really what you should look for is a variety on that team. Clearly you need people with good leadership skills. Clearly you need people with good communication skills. And I'm suggesting you include some people that

have much more of a creative and boundary testing or boundary spanning emphasis in that group. And presumably they'll also have the software skills, the communication skills and that sort of thing.

But I think having a mix of folks on your team so that you don't have, for example, just a bunch of people that can code and follow a software design. But you're also having some people on that team who are going to say, "Okay, let's take a look at that design and let's see if there are any weaknesses and think a little bit outside the box." I think that sort of mix is going to be effective for coming up with a secure product. But you have to do the whole thing.

There are a bunch of best practices out there, so don't stop with building the best team. Also go ahead and institutionalize some of those practices that I mentioned: (1) the code audit; (2) the unvalidated input; (3) the various failure conditions – if a disk drive goes bad, if an operating system fails to boot properly; (4) thinking in terms of physical security; (5) of what happens to that paper trail generated by a system; (6) also thinking in terms of communication security.

So these days, of course, computer systems are running most of the things that we're talking about today, and they're all connected in various ways within the organization and to other organizations. You only need to look at the data flow across that whole spectrum, including the people involved, to have a really good notion of how well things stand. And if you don't have a good notion of how well things stand, that's probably the riskiest position of all.

Stephanie Losi: What do you think the biggest roadblock has been in terms of that, in terms of kind of stopping effective interaction between business leaders and their information and security staff?

Greg Newby: Well, computers is really what we're talking about for the most part here. Most of the types of information systems that we deal with these days have a pretty strong computer basis, software interface, communication and all that sort of thing. And the thing is, computers are a pain to use. And people that might be very effective managers might not feel all that comfortable with all of these new ways of doing things.

And I think that's one of the biggest challenges is, there has to be a certain level of letting the, either the security organization or the IT organization manage its own affairs. And, as I said, trust them to do their job, but also give them the freedom that they need in order to do this sort of exploratory activity.

Stephanie Losi: Okay, so trust seems to be a big thing in terms of what the IT team needs from the business leaders in order to really do their job well. So in addition to that, how else would you say, how can the business leader really support security personnel to help them achieve maximum success? What are some good first steps? Say, if you're just starting to try to reach out to your IT department and first of all find out what's going on, and then give them the tools that they need to effectively do their jobs, and then to measure how well that job is being done.

Greg Newby: Well, I mentioned earlier that computers are used by a variety of personnel for a variety of purposes. In terms of the IT and the information security personnel, security really needs to be a big part of the mission, needs to be built in and wrapped in to essentially all of the activity and a high level of integration. Because if the IT security personnel are sending out reminders on how to change your password and why you should worry about certain phone calls that you get or worry about someone shoulder surfing in the cyber cafe, these types of things – if they're not really getting high-level organizational support, then there isn't really any particular reason for the rest of the organization to pay attention.

So putting the information security folks in a role where they can be successful, I think, is the most critical piece. And the risks of course can vary according to industry and according to what it is that you're doing out there. But the fact that most of our corporate identities, our corporate policies, our data, our finances, all of that is computer-based – it's hard to imagine a industry where this is not a very important and very high-profile need, to take care of information security.

Part 2: Building a Security Conscious Culture

Stephanie Losi: Okay, so in terms of measuring how you're doing, can you maybe provide an example of where you have seen a security-aware culture working well and what were the characteristics of that culture?

Greg Newby: Well, there are a couple of high profile internet-based companies that are making security end to end and making it everybody's business. And I think part of the reason is, without naming names, I think part of the reason is that they're concerned about their value if they have a highly publicized security breach (and we haven't had any too recently, which is good). But if one of these very big internet companies, brand names, has a highly publicized security breach, they could be looking at literally 50 to 80% of their market value go away overnight. And customers will leave for another service, comparable, one of their competitors, and possibly never come back. So I think that the stakes can be extremely high in some of those companies.

And what I'm talking about here really are the tech companies that survived the bubble, the bursting bubble. These are the ones that came out on top and are still doing well. They seem to really have a culture of security and not to leave nearly as much to chance and to make sure that really all personnel are aware at least of the stakes involved. They might not be aware of all the details. They might not be responsible for daily operation because they have jobs. Everyone has jobs, and you don't want to make the security department everybody's job, but you do have to have everyone with a baseline level of awareness and a very clearly understood responsibility for security across the organization.

Stephanie Losi: Right, I mean, including the business leaders. Everybody should be toeing the same line.

Greg Newby: It's top down. In the success stories, it's top down. I think in the stories of failure where something went wrong, it was where an IT department with a security department – maybe they're together, maybe they're separate – but those folks may have been very effective but they weren't getting the organizational support, and so where did the weakness occur? Well, weaknesses might have occurred due to insiders. That's, as I mentioned earlier, that's really where the big money tends to be lost, not due to people doing viruses and to people attacking your website with well-known types of exploits. But insiders who are able to circumvent internal intranet policy to your disadvantage, and that could be all kinds of disadvantages.

So I think the failure stories are where there's not really good top-down coverage. And it doesn't mean that everybody has to be doing the IT or security department's job. I think that's important to understand. It does mean that everyone has to be aware of and supportive of the importance of security in the organization and have a certain baseline of knowledge of good practices: what to do, what not to do. And that of course is going to differ by industry, that sometimes there's regulatory issues involved, and it's going to change quite a bit depending on the size of the organization as well.

Stephanie Losi: Okay, can you give some examples maybe of things to do versus things not to do?

Greg Newby: Well, I think for the business leaders, the main thing is to consider whether or not any of this is making sense to you, and if it's not, then that's probably an indication of a problem. Listening to the podcasts is a sign that maybe you're on top of things. And if so, then look at who it is in your organization that is responsible for some of these areas and see if they're appropriately empowered and see if they're appropriately trained. So I think just doing a fairly high-level, top-down sort of audit of what's going on is a very good first step.

The *next* thing that I would do is to see how well understood your adversaries are. See how well you understand the risks. Just sit down with a whiteboard, if you don't already have some kind of a document on this, sit down with a whiteboard and some of the technical staff and some of the non-technical staff and do some of these scenarios. And say, "What if, what would happen if so and so accidentally deleted this database? What would happen if one of our partners who does some sort of processing for us – say it's inventory, say it's credit card processing, billing, that sort of thing – what would happen if one of them had a security breach? Let's imagine scenarios where employees have corporate laptops or things like that and they get stolen or lost." So you do these different types of scenarios and you see how well you understand what the risks are, then see how well you are prepared to meet those risks. And I think chances are in almost every organization you'll immediately come up with areas of weakness. And then you just go ahead and work through that; give allocation of time and effort to those weaknesses.

I think the *third* thing that you can do, and this is something that I believe big businesses tend to be more diligent about than small businesses because small businesses tend to have a lot of immediate daily pressures, is go ahead and do an audit more formally. Hire a consultant or hire one of the consulting firms or maybe just task a subgroup within your organization and say, "Okay, we're going to do a bunch of stuff. We're going to work through a bunch of scenarios. We're going to try a number of things that we might be concerned about and see how it turns out."

The one warning I'll give about that is something called red teaming or penetration testing. This is where you actually try to break the system, and this is something that you need to be cautious about. Because if you get permission, because that's an excellent way of testing your system, except you don't want to do that without having the appropriate level of knowledge within the organization that it's going on. And the appropriate level of course can vary depending on the situation. But I don't want to have someone in an IT department say, "Oh, I listened to this podcast and I think the answer is I need to go and figure out all the weaknesses in my system. And I'm going to do that by running all these scripts, and breaking in, in all these different ways, and making all these phone calls, and digging through the trash, and jiggling all the doorknobs, and testing all the filing cabinets." And that might be an excellent approach to a security audit, but don't do it without having full disclosure to the level required within your organization.

Stephanie Losi: Right, I mean, especially at the points where I guess the corporate network touches a partner network, for example.

Greg Newby: Yeah, and actually the boundaries are where the danger tends to happen, by the way, so that's a great example. And, in fact, the companies that are doing a lot of acquisitions, the growing companies that are doing a lot of acquisitions, face the problem of course of clashing corporate cultures and dealing with finance systems and all these important things. But the IT aspects can be really important, and in fact some of the weaknesses that some large and well-known companies have suffered came not from their own corporate network but from fairly recent acquisitions that had weaknesses that were not fully identified. And yet that acquired company, which is often at a remote site – it's not going to be co-located typically – was brought into the intranet without being properly audited.

And being attuned to that type of problem is important, and making a decision – just a conscious decision, about when to treat a particular network or individual or system, or choose your level of granularity, as sort of a trusted peer – is a decision that should be made consciously, not by mistake.

Stephanie Losi: Right, because we're talking about trust. We're talking about having a security-conscious culture and making sure security is built in, and in that situation you may have security built in but suddenly you don't.

Greg Newby: Yeah, that's right, and this is what I mentioned with having an insider. A lot of people make the mistake of implicitly trusting anything on the inside. So if you are in a physical building and you trust anyone who's on the inside, well, what if that person works for you but has a grudge or bears you ill will or is maybe a spy of some sort for your competition? Well, you have to treat your digital networks the same exact way. Just because it's on the inside doesn't mean you should automatically trust it to any particular extent.

You have to be making that decision very consciously, and it might be that, or actually it's very likely that, the level of trust for a system on the inside is no different than a level of trust to a system on the outside. You simply have a few different barriers and a few different structural things like firewalls that you go through to get access to resources. Yeah, it's all about design.

Now this is, luckily, this is something that the top-level managers don't need to know in fantastic detail of course. There's a lot of books that have been written on things like demilitarized zones and intranets and firewalls and public key encryption, and there's a variety of products like USB (universal serial bus) tokens and hard drive encryption - all types of things that you can do to make your internal network just as robust as your external.

Part 3: Tackling Secure Software Development

Stephanie Losi: Right, and we're talking about building security and there is some growing evidence that addressing security early in the software development life cycle or in the network, I would say, development life cycle as you build things out, that reduces the number of vulnerabilities that you have in the end. So let's sort of switch tracks from networks to software here, and I'd like to ask you: What do you think is the biggest challenge in getting software architects and designers as well as their managers to tackle security during development?

Greg Newby: Well, I think the thing that you mentioned is something that we know really helps a lot, and that's to start out with security designed in, to make sure that's a part of it and thinking in terms of inputs and outputs and unintended consequences and so forth.

I think the *biggest challenge* is just complexity. Software is still at least partially an art – it's partially a science, but it's at least partially an art. And you end up with often medium to large teams working on these software products, and things can get complex. And you don't always know, for a given instance of software, you don't always know all the possible scenarios that it could be put through. Sometimes there are mistakes made, like changes made at the last moment or using an older version of the code by mistake. There are all sorts of things that can creep in. So I think the complexity of the software is really the biggest challenge.

I'd say the *second biggest challenge* is the complexity of the underlying systems. So if you're doing web services based on [Apache] Tomcat or IBM's products, something like that, WebSphere, well, that's very complex software. And there could be problems with that software or unintended or undocumented consequences with your software's interaction with that software. Ditto if you're

developing software for the Microsoft, Apple, Linux, what have you operating system. Well, that's also very complicated, and there might be all sorts of things that you don't or can't understand, or it might be that there's just variability in what goes on with those underlying operating systems – just the fact that my PC and your PC aren't exactly the same. We've made different decisions about configuration.

Stephanie Losi: So what does the business leader need to do to make sure that the software engineers are able to do what they need to do, to deal with that complexity and variability? Because I have a feeling some business leaders may be thinking, "Well, that costs a lot, and how do we know we're going to see a return on spending all of this time building in security and taking into account all of the variability between platforms?" How would you justify that to them?

Greg Newby: Well, you have to consider risks. So we know that every time you do a full, complete security audit, you cut the number of bugs in half approximately. So if you say, "All right, based on the number of lines of code and other factors, I have a thousand bugs in this program." And then you say, "Well, based on the profile, what I'm doing with this, there might be a hundred of those that have security implications and the other 900 are just various types of errors." So you can go through a security audit – well, not a security audit, but a code audit, a complete audit – and find half of those. Okay, so how much did that audit cost? Well, it's going to be proportional to the number of lines of code and other factors, right? So you can estimate really how much it's going to cost you to cut your number of bugs in half, and then when you're done with that, you can do it again and cut your number of bugs in half again. And in theory of course is that it's asymptotic. You never actually get to zero, even though you might extrapolate that line. So you can repeat this as many times as you want, spending as much money as it takes, and every time you'll have fewer bugs. So the question is, what's that worth to you?

Stephanie Losi: Right, when do you say, "Okay, we want to do it x times but no more?"

Greg Newby: Yeah, exactly, and I think that Microsoft and some of the bigger software developers actually have a more or less algorithmic approach. They're treating it more or less as a science. I think for more custom software development, say an in-house type of product, then that might be a harder decision to make because you don't have quite as good a model and you might not even realize, it might be hard to estimate what the real costs are of doing that audit. Doing it once is a good idea for probably any old product, but I think the decision as to how much money to be spent really has to be balanced with the risk if something goes wrong.

So if you're making, say, a computer game or you're making some document processing system and there's a serious problem, right, as long as you have a way of pushing out a patch for that serious problem to your customers then maybe that's okay, maybe that's acceptable.

If you are, on the other hand, doing a security-related product or if you're doing a product used for e-commerce, e-finance, if you're rolling out for example a complex website, then you say, "Okay, well, wait a minute. What's the risk if there's a serious security problem? How many customers or criminals, or what have you, might exploit or be victimized by that risk, and what's the dollar loss for that one incident?" And then probably more importantly, as I mentioned earlier, what's the dollar loss in terms of credibility to the company, which might mean a bottom-line stock number, a proportion of your stock value? Or it might be something a little less tangible like, are you going to get – if you're a consulting company or a small firm – are you going to get business next time as a result of what happened this time? So you have to balance that risk.

I think doing the audit is really important, keeping the complexity under control by following good software development practices, things like documentation and regression testing and checking all

the boundaries on your inputs and so forth. There's books full of good software coding practices. So I think that's probably the thing that you must do for any project. And then the question of how far do you want to work to really squash as many bugs, including security-related bugs, that's a question that's more of an economic question in most cases.

Stephanie Losi: All right, and where can our listeners learn more?

Greg Newby: Well, there's a lot of different sites. Of course CERT is the place for clearinghouses on the latest developments, and there are a couple of similar clearinghouses that work within different sectors, one for military and so forth. There's also a lot of conferences that happen with security. There's some that are much more technical. There's some that focus really on the hackers and the exploits and the software and the insides, there's some that are a little bit more general. There's also some certification programs.

I think the main thing is that, as I said, technology is hard, computers are hard. So you really do have to make an effort to keep on top of this and whether that's through a conference you attend once or a couple of times a year, or whether it's just reading a book or reading some journal articles, or whether it's actually going out there and diving into some source code and looking at some of the latest exploits, whatever are appropriate.

Stephanie Losi: Right, and that goes back to what you were saying about the type of employee that's good to have who is interested in learning and interested in making sure that they catch the mistake before the attacker does.

Greg Newby: Sure, so do security training within your organization, and some of these stories can be fun to tell. And just like in any sort of customer service situation, everyone has a story about the customer that had so and so and what you did and you have a good laugh about it. Or you can have some of that same type of organizational storytelling with information security and share some of the foibles and the outcomes and the best practices and so forth and make that part of what's acceptable to discuss.

Don't make it something that people are afraid of because maybe they feel they don't understand security or they understand some security but they really don't understand cryptography or something like that. Just go ahead and bring that out in the open and get people feeling comfortable about discussing the security problems and then sharing both some of the solutions and some of the latest developments or practices that they're aware of.

Stephanie Losi: Thank you very much, Greg. This has been great. I've really enjoyed having you here, and I think our listeners can learn a lot.

Greg Newby: It's been my pleasure to be with you.