Evolving Business Models, Threats, and Technologies: A Conversation with CERT's Deputy Director for Technology
Transcript

Part 1: Evolving Business Models; Evolving Threats

Julia Allen: 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 more about us at CERT.org.

Show notes for today's conversation are available at the podcast website. My name is Julia Allen. I'm a senior researcher at CERT working on security governance and executive outreach. I'm very pleased today to introduce Tom Longstaff, CERT's Deputy Director for Technology. Today, we'll be discussing the threat and technology landscape and what business leaders need to know. Welcome, Tom. Glad to have you.

Tom Longstaff: I'm glad to be here.

Julia Allen: So let's jump right in. How would you advise business leaders to think about or determine the most critical security threats to their organizations and what they should do in the face of those threats? What are your thoughts about that?

Tom Longstaff: Well, I mean there are a lot of different things that a business leader has to consider today; many more things, perhaps, than even as little as five or ten years ago. Five or ten years ago, I would characterize the threat to business leaders as very overt, very in your face. So you could put a network together and attach to the Internet and start doing business on the Internet and really have to worry a lot about straightforward attacks through your firewall. Things that smack you right in the face, things that really came straight in.

The threat today has really started to go more subtle, more underground, more not quite so overt and obvious. The real ramification is there is no really good single point of protective technology or concern or something that a business leader has to think about today. They have to think about a whole series, a whole range of issues.

Julia Allen: And is that strictly because of the subtlety or the more covert nature, or because the targets have also become much broader, the targets of the threat?

Tom Longstaff: Well the targets of the threat are somewhat broader because after all, there are more things that are accessible from remotely, from the Internet, from electronic devices. But really, it has to do with the changing nature of the threat and the way most business leaders were trained to think about Internet and electronic threat. We were all going through school and as we started to learn about how to operate in business, we really came in with the mindset of, "Put some protections in place and monitor your network, and when you see an attack, respond to it." And that's really been a primary mindset of business for the past, oh, 20 years or so, since we've really begun to take advantage of information technology.

Julia Allen: So you're saying this notion of kind of the fortress mentality or protect the perimeter or—in other words, that there's actually a boundary around you or something that you could actually secure. You're saying that's how we kind of came into the business.

Tom Longstaff: That entire mindset—the entire fortress mindset—is how many of us were trained to think as especially security professionals or as business leaders. Unfortunately, the truth of the situation today is that's not the model in which we operate. It just isn't the model in which commerce takes place. So what you have to think about doesn't fall neatly into inside and outside, or in my castle and in my keep and beyond the moat.

So the real effective mental model today is to really think about the network as also the place where you do business. As the Internet and everything networked with all of your customers, your suppliers, everybody that you do business with is a node in your network. They're all an interconnected part of this big sort of circle of business, to paraphrase a statement, where your security is not only dependent upon what you do within the assets that you own, but also the limits that you impose on business with others—what you want your clients to do, what you want your providers to do, how they interact with your data.

Julia Allen: Well, and what they expect of you in terms of protecting their data and information and process flows.

Tom Longstaff: Exactly, because the exact thing works in reverse. You are not an island unto yourself either. You are connected to other people's networks. You are essential to other businesses. The interconnectedness and interdependency among these business processes is what has to drive the mental model for security today.

It's just, you're not protecting a machine anymore. You're not protecting your database. What you're protecting is your business process. You're protecting the integrity. You're protecting the viability of the processes.

Julia Allen: But the fact that you could still execute the process, right, and all of its component parts.

Tom Longstaff: Right, and that the process does exactly what you think it's going to do. That means that you're interacting with the right people inside your network, that you have a level of trust that's verifiable, that you have expectations that are very clearly spelled out. Each one of these things doesn't sound very much like traditional security, but they all contribute to the mindset where you have to start thinking about, "Well, what do I need to do to ensure that my business processes are not interfered with by some kind of party?"

Julia Allen: Right. It gets back to this fundamental dilemma of what is critical—what is my critical asset? Recognizing that we can't protect everything, how do I identify what are the objects or artifacts or concepts that I need to include in my security strategy? If business process is a pivotal one of those, then that really is a different way of thinking than most people tend to think about security controls.

Tom Longstaff: Right. I would say business process *is* the fundamental thing that you're trying to protect these days. The information associated with the business process, the different kinds of access controls and things of who participates and how do you know who's participating in those business processes...

Julia Allen: So does threat then become a notion of what would threaten or interrupt the execution of the business process? Is that kind of what you're saying?

Tom Longstaff: Kind of, and now you can see the context where I say threat's getting a little more subtle and underground. Because instead of threat banging on the front door of a fortress, you

instead have the threat manipulating these business processes in ways to extract information or change the value of information or change the value of the goods and services.

Julia Allen: Or take money—

Tom Longstaff: Or take money.

Julia Allen: —Out of the process.

Tom Longstaff: Or somehow interfere with the trust relationships that you have. So what is the biggest danger of phishing, for example? Phishing attacks are these e-mails that you get that purport to come from a financial institution that says, "We think your password may have been compromised. Please log into this web site and enter your user name and password so that we can update your information and protect you." And in fact, you go to a rogue website, very cleverly disguised as the official website.

Julia Allen: It looks like the real one, right?

Tom Longstaff: It looks very much like the real one, and they're attempting to get the information from customers. The real insidious part of phishing is not the money that they lose. It's not the money the customers lose, and it's not the money that the financial institutions lose. Those are very bounded, and they tend to be fairly easily recouped. What really gets damaged most in a phishing attack is the relationship between the client and the financial institution.

Because now, clients can't really trust that they're interacting correctly with their institution, and institutions can't trust that clients are always going to do the right thing because they can be easily led down this garden path.

Julia Allen: So you're saying even if the financial institution has said, "We will never send you e-mail of this type. We will never solicit that kind of information"—you're saying even then, people are still trusting when it looks like it's official.

Tom Longstaff: Right. So that's the business process that phishing is interrupting. So it's a clear example of what I mean. The banks themselves can't solve this issue because it's partly an issue of people controlling information that's essential to the bank, which is their own access control information.

Part 2: Technologies To Watch Out For

Julia Allen: Okay. So we've talked about the changing threat, going from more overt to more covert. We've talked about business process really being the essential representation of the business relationships. Obviously technology plays a very significant role in this. So let's turn our attention to technology, both technology solutions and technology that provides a whole lot more challenges for us to deal with. How would you advise business leaders to get smart about and consider how they can effectively deploy technology solutions?

Tom Longstaff: Well, given the mindset that I just talked about with the business processes, the most important technologies to watch are anything supporting communication and business process. So anything supporting the relationship that you have outside of your business—or inside of your business, when we talk about insider threat—those technologies are the ones to be most suspicious of.

Julia Allen: So give me a few examples.

Tom Longstaff: So for example, as we move from e-mail to web-based services, from web-based services to things like Ajax where you're going to data models that are being pushed more and more outside of your corporation. These are technologies that are changing the entire nature of who has what information at what given time and who controls it. And it's not just because I have a new JavaScript application. It's because I'm actually changing who is in charge of the essential pieces of this trusted relationship.

So the technology that has linked this whole web of business processes together has also distributed the business information all throughout this entire web that we have. It's not in any one given place anymore.

Julia Allen: So you're saying some of the underlying infrastructure, the paths that the information transits and the way in which the information and the handshakes and the various things happen to actually allow information to move from one place to another. You're saying that's where some of the protection and controls need to be.

Tom Longstaff: Right. Everything from the low-level protocols and the encryption that goes into the various lowest level of the information to the high-level protection standards and even things like DRM, digital rights management, that we have to protect our content.

So all of these are standards of one kind or another. They're different ways that we have agreed upon to protect information at various levels of abstraction, all the way down from the raw network wires all the way up to the very abstract kind of business information that we rely on. And it's those kind of agreements that we have between all of the partners in our network that are really what we're relying upon to protect our business processes.

Julia Allen: So how do these agreements manifest? In other words, how do these trust relationships evolve, from your point of view, and how do you get to a common understanding that addresses both some of the threat and some of the technology issues you've raised?

Tom Longstaff: There are three primary ways. The first way is there's a very traditional, more formal way of doing things on the Internet, usually controlled by the Internet Engineering Task Force, the IETF. They have a number of security groups and they handle most of the low-level protocols, most of the way information moves around on the network itself.

The second way is when we have de facto industry standards; so when you get a big vendor that essentially creates an industry standard for some kind of information representation,

Julia Allen: Just by virtue of their market presence—

Tom Longstaff: —By virtue of their market presence and sometimes, by virtue of just having been early in the field and defining the standard. So for example, PowerPoint is an example of how everybody moves presentations and things around. PDF is a standard for information. Excel spreadsheets. These are all very well-known standard forms of information. They all have some built-in protections. They all have various kinds of passwords that can be build in, some various kinds of encryption, some access control—rudimentary in some cases, but again...

Julia Allen: But they're nonetheless—

Tom Longstaff: But they're standard.

Julia Allen: And perhaps serving as sources for future levels of protection should that be called for by the marketplace.

Tom Longstaff: The third way, which I think is one of the most interesting ways that we do it, is through emergence, and this is when we have things like social networks and small applications that hit, that happen to become the very thing that we latch on to. So this whole push that we have right now toward things like Ajax and Web 2.0 and all of these technologies for moving the data model to the client is kind of an emergent technology that caught on in a number of different areas.

Julia Allen: Okay, and how do you see these emerging technologies providing part of the solution set or at least a place in which solutions can live?

Tom Longstaff: Because the security also emerges with the solution in those cases. They're not defined by any one vendor, and they're not defined by an IEEE or an IETF standard. They're instead defined by a rapid evolution of people using the tools and dealing with the threats as they emerge as well, because as we get these emergent technologies, the first people to use them are the ones very familiar with technology and also how to break technology. So we get a very rapid evolution of threat, response, threat, response, threat, response. Then business latches hold. Once business latches a hold of these emerging technologies, it ratchets up the threat.

Julia Allen: In other words, you've solved a certain class of threat. It's like the reason we're dealing so much with various forms of cancer today is because we've solved all of the diseases that killed people off earlier.

Tom Longstaff: Right. It's sort of comparable to that, except much more quickly. We've got things that go from very rudimentary attacks to very sophisticated attacks in a period of 18 months. There's a very, very rapid response and threat, response and threat. Then when businesses latch on and they start putting value into these technologies, the more value it is, the more we get a concerted effort to quietly attack the technology. The first attacks are almost always loud. They're easily spotted. They're talked about.

Julia Allen: They're visible, right.

Tom Longstaff: They're visible. By the time they hit business, they're no longer that way. They start to sink beneath the top veneer, and they start to really begin to get at the underlying data models in a way that the criminals—and we'll call them criminals—hope they won't get caught in order to take whatever it is they're taking, and disrupt the process.

Part 3: Actions Leaders Can Take

Julia Allen: Well, clearly, being the Deputy Director for Technology for CERT, you live in this space. It's something that you explore, that is a big part of your day-to-day existence and your conversations with colleagues and with clients and customers. That's not the case for most of our listeners. So if you could step back a bit and say if you were a small, medium, even a large enterprise today and trying to grapple with this shifting threat and technology landscape, what would you advise to effectively, maybe not get in front of the problem, but perhaps keep up with it at some level?

Tom Longstaff: Well, if you're the kind of business that really wants to take advantage of emerging technology—I mean if you're the kind of business that wants to say, "Let's take this Ajax thing, this

Web 2.0, and let's run with it as a business model"—if you're that kind of business, then you've really got to think outside the fortress model.

I mean, the first thing you have to consider is, "Where's my data and how is it being protected? How are my business products being protected, and how can I really clearly state who I trust and what I trust them to do?"

When you think about the problem in that way, that is an excellent place to start, because that automatically prioritizes where to begin to put your defenses.

Julia Allen: Okay. So what is most critical for me to continue to stay in business? What do I absolutely need to have no matter what?

Tom Longstaff: Right. And of course, what do you have to have? You have to have trust. You've got to have trust with your clients, with your partners. If that trust breaks down, it's very difficult to stay in business. So you start there and start by understanding, "What does that mean in terms of a protection model? Does that mean that I have to worry about protecting the data I keep and hold onto?" Well maybe, if I process credit information and that's my business, that becomes an important part of the trust relationship with others is that I protect that information. But maybe if I'm on the other side of that equation, an important thing for me to do is to assure that I can specify the right things for my partner so that they can protect the information.

Julia Allen: Right, so that you're clear with them what your requirements are to maintain—again, getting back to this notion of trust—to maintain that trust relationship.

Tom Longstaff: That's right. So that's where you start. And even if you're not a company that's embracing the latest technology, you still have to think about how you're migrating over time. Because many companies are migrating from a model where they're keeping all of their information close and keeping it protected inside of boundaries that they own to more and more distributing those business processes. Now for some companies, that's going to be a slower process, and they'll have more time to think it through, more time to watch the people on the edge.

Julia Allen: Right, to not be on the bleeding edge.

Tom Longstaff: Not be on the bleeding edge. But it is important to watch them because that technology is coming to everybody. Even if you're a very conservative organization that's keeping everything behind a firewall and you have your IDS systems and you're watching everything. Even then, you're going to move and you're going to shift.

Julia Allen: You're saying you really can't be competitive in this worldwide marketplace if you continue to operate with that type of conservative approach. You've really got to open things up and then figure out how to operate.

Tom Longstaff: Right, and even businesses that traditionally have not played much in the Internet world are beginning more and more to have to play in that world. For example, I look at the entire power infrastructure where for years, the power, the electric power infrastructure, has been very isolated from other kinds of networks and information. They lived in a world amongst themselves with their own power engineers, their own systems, their own sort of isolated business practices.

Julia Allen: Their own means for distribution.

Tom Longstaff: Their own means for distribution. Everything controlled within a group, but a small, controlled, trusted group; a group that pretty much knew how to trust each other.

Julia Allen: Is that no longer the case?

Tom Longstaff: It's absolutely no longer the case after deregulation, after the power industry has become more and more into the marketplace, the open marketplace.

Julia Allen: So is it kind of similar to what happened with the old Bell, the Bell telephone where it went from being very centralized to very distributed—lots of providers, lots of interaction, lots of competition?

Tom Longstaff: Except with Bell, when you break up a company like Bell, you actually end up with a lot of entities that compete against each other. With the power industry, you have this strange thing where they have to cooperate too. They compete, but they also cooperate. Because of this, they're still tightly interconnected, but now the trust model changed, and nobody really reacted to that change. They didn't think about the implications of what it meant to suddenly have to operate in an open marketplace.

So for example, we had industries where the marketing department that bought and sold energies suddenly had to be directly connected to the operational parts of the network that controlled power, so they could get up-to-the-minute information of what was happening.

But as soon as you open up that door of who's connected, then suddenly you have people from the outside that could potentially come into the operational networks.

The reason I bring them up as an example is they're an industry that didn't think it through, and they took a long time to realize that the threat model had changed. So as a result, we have things like the New York blackout. Once the New York blackout happened, we started looking at the infrastructure that were actually controlling the interaction of all these different companies.

Julia Allen: Right, saying, "How could we avoid having this happen? First of all, how did this happen, and then how could we avoid having it happen again?"

Tom Longstaff: Right. So a lot of things were uncovered during that particular investigation about the way the cyber part of that environment was interconnected. I think it opened a lot of folks' eyes. In the business world outside of power, of electric power, we now have the opportunity to learn those lessons as well.

The more we virtualize, the more people effectively become insiders to your business. Thinking about them that way is another way that you can begin to approach technology and approach the idea of "What technologies are good for me?"

Julia Allen: Well, this has really given a great deal of food for thought in terms of shifting the way that we even think about the problem landscape. To close for today, can you say a little bit about the fundamental issues that you're tackling or that you would like to see the program tackle over the next, say, three to five years?

Tom Longstaff: Part of the answer comes into, how do we promote dealing with the threat as it becomes more and more distributed, and more and more quiet, more and more covert? Because that means that our ordinary vulnerability reports and the ordinary idea about "watch out for this kind of port"—it's just not as effective anymore.

So understanding, how do we communicate the changing threat? How do we communicate what to watch for? How do we help people understand how change is happening on the network and what they need to happen? This is a fundamental question throughout CERT. We have to begin to adapt ourselves to this sort of changing landscape and this changing nature of the threat going more and more underground.

Julia Allen: Well, it sounds like plenty of interesting challenges and issues for your office in the future going forward.

Tom Longstaff: Thanks very much, Julia. Always a pleasure.

Julia Allen: Thank you.