Convergence: Integrating Physical and IT Security
Transcript

Part 1: What Is Convergence and Why Is It Important?

Julia Allen: 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 Julia Allen. I'm a senior researcher at CERT, working on security governance and executive outreach. Today I'm pleased to introduce Brian Contos, Chief Security Officer at ArcSight, and Bill Crowell, former Deputy Director for the National Security Agency. We'll be discussing the political, business, and technical issues in bringing together traditional physical and IT security solutions, commonly referred to as convergence. So, first of all, Brian and Bill, thank you. I really appreciate your making the time to speak with us today.

Bill Crowell: Our pleasure.

Brian Contos: Yes, thank you, Julia. It's really a pleasure to be here.

Julia Allen: So why don't we get started? Let me just throw out the first question to help bring our listeners along with us. So what is convergence and why do you believe it's so critical, given today's changing security landscape?

Bill Crowell: Well, convergence is the bringing together of multiple security disciplines into a common platform. And the real driver of convergence today is the network, the ability to connect many different processes — security processes — and to build those into various layers of security in a way that makes things better. Convergence all along has been something that has been making things smaller, faster, cheaper, and now connected. And the importance then in terms of what it does for us is it allows us to expand the context of security to include video surveillance, physical security of almost every type, logical security, for example network and applications security, and even supply chain security, as we'll discuss I'm sure later – where you can track the elements of business and make sure that they are secure, not just in the physical sense, but also in the environmental sense, from their origin to the place where they will be used.

Julia Allen: Well, I'm kind of curious. Obviously, traditionally these have been very separate disciplines with separate competencies and skills and backgrounds. Is there kind of a seminal event or something that really has caused this acceleration in bringing physical and logical or digital security together?

Brian Contos: Well, I certainly think that the advent of the Internet, at least the late phase adoption, sort of post-1996, has really helped. And we're seeing a lot more in terms of IP (Internet Protocol)-centric solutions. So take the process control industry, or SCADA (Supervisory Control and Data Acquisition) specifically as a branch of that. You're seeing now that these devices that existed for several decades, 40 years in some cases, that were very closed off and isolated. They didn't have network communication, they were very proprietary; but today now they're not. They're running common hardware and software, they're very IP-centric, they're networked with each other, and in some cases, for operational efficiencies and management and maintenance and whatnot, they're actually connected to a corporate network, with maybe a firewall in between,

which of course is then connected to the Internet; and there's threats of course inherent to that. But the whole idea of bringing IP into these solutions I think has been a really big jumping-off point for conversions.

Julia Allen: So you're saying here, just the fact that we've all become so much more connected, so much more ready access to information and to the assets that hold that information, tends to kind of blur or fuzz up some of the historical or traditional distinctions.

Bill Crowell: That's absolutely right. And in fact one of the things that we address in our book is the notion that the skill sets and the organizational structures that support security will be changing very dramatically in the future. We will be seeing security officers who will reach the CxO level or the corporate level, probably combining the functions of the CIO (Chief Information Officer), the Chief Security Officer, the Chief Information Security Officer, into one organization.

Julia Allen: We're seeing that too where some of the traditional CISO – Chief Information Security Officer — roles and CSO, which is traditionally responsible for physical [security], are actually starting to merge, and sometimes we've even seen those show up underneath something like a Chief Risk Officer.

Brian Contos: Yes, I'm actually seeing convergence even stepping away from security, just happening all across our industry. I mean, look at telephony NIT (network information table). I remember when I first started, you had these telephony guys that had their punchdown blocks and they were very concerned about 5 order of 9's [a measure of network availability] and uptime, and then you had these IT guys that were always rebooting stuff and changing stuff around, and there was just a different perspective. Well, now, because of Voice over IP and other technologies, they've come together.

We're also seeing that with security operations centers and network operations centers. So I think it's a fundamental shift for our entire industry now that convergence, not just in security but in general, is making a lot of sense.

Julia Allen: Well, you started down this path, Brian and Bill. Let's go a little bit further with this one. What are you seeing? You've mentioned some, but what are some of the implications of this merging or converging, both for employees and for business leaders who need to staff to these new skills and competencies?

Bill Crowell: Well, I think that we have touched on it already. So let's expand a bit on that. The notion that security can be put into silos for networks and for physical security and for HR (human resources) kinds of activities and so on, in our mind, will eventually disappear. We should have only one set of records, if you will — identities for people — whether it's for their entering a building and being badged or entering the network and using applications. That will streamline things, but it will also make security better.

Today, sometimes as many as four or five different organizations have to be involved in order to — if I can use this expression — shut the door on an employee that has left the company, or open the doors for an employee coming into a company. And that will all be done just one time, in the future, using identity management as the central core for allocating authorizations and access. We'll see other changes as well.

One is that at the present rate of expansion for video surveillance, we certainly could not afford all of the eyeballs that would be necessary to watch all of the screens that those cameras can generate. So smart video or video analytics will be used to try and streamline and make more

effective video surveillance so that you are looking at cameras only when something is happening, and so that you are able to do forensics. And also, as Brian I'm sure can discuss a great deal, we can begin to collect events, physical security events, from video surveillance cameras, that can then be correlated with events in other parts of the security system, including logical systems. So a person entering a building in France cannot be logging on to a system in the United States from a U.S. terminal.

Julia Allen: Now, Brian, I think you were going to say something here, but I'm particularly interested in — clearly there are all kinds of technological and data correlation, data analysis monitoring implications. What about competencies and skills? Is convergence changing both what people need to know how to do and how business leaders need to learn how to staff these new converged functions?

Brian Contos: They are, but it's not being done holistically. And again I'll go back to that telephony and IT example for Voice over IP. In that case we actually saw the IT staff develop a very strong competency and telephony solutions to the point where in some organizations there is no longer a telephony team.

Now, I don't think that's going to happen with physical and logical security convergence. I don't see the guys that are responsible for managing risk and compliance, operating firewalls, defining policy, being the folks that are going to roam around the building and looking for intruders and dealing with law enforcement.

So I think, as Bill alluded to earlier, I think ultimately these groups will report to a centralized CxO-level person that's responsible for risk in general, especially as people are becoming more risk-aware and less sort of fear-aware; all the FUD (fear, uncertainty, doubt) that's been thrown at them over the last decade about "be concerned about this type of attack" or "be concerned about that," regardless of what industry you're in. I think we're going to see a centralized person that's responsible for everything from risk and compliance and physical security and logical security, and under them we'll have these varied groups. I think we're still going to have the person that's very specific to IT and the person who is very specific to physical security, but they're going to have much better communication. We're going to see synergies between the technologies. We're going to see policies and procedures that integrate them both.

And Bill made a great statement. He talked about having a single card — and a lot of people are using what's called CAC, common access cards — to physically enter a building, to log on to the network, to encrypt email, and so on. It's great for provisioning new employees. It's great for revocation, if somebody leaves the organization. It's great for monitoring a specific individual's physical and logical whereabouts and what they've done in generating a trail. I think technologies like this are going to become more common, and they're going to rely on these groups being able to communicate better and make sure their technologies interoperate better.

Part 2: Getting Started

Julia Allen: Thanks very much. I'm kind of curious, since we're kind of on a roll here with some excellent examples, how have you seen organizations and leaders get started in terms of both recognizing that they need to be bringing some of these skills and competencies and solutions together? How have you seen organizations kind of get rolling on their own convergence activities?

Bill Crowell: Well, there's an interesting situation here in that this is one of the cases where the federal government in the aftermath of 9-11 has actually led the way in establishing a standard for

federal use, called the Homeland Security Presidential Directive Number 12 — HSPD12 — which essentially develops a standard for the combining of physical access, logical access, and identity cards in a single credential. And while it certainly is not proscriptive that it would be used by industry, it is a very complete standard that does allow various agencies of the federal government to have a common and interoperable set of credentials.

To me, that's a tremendous step forward, because the federal government had literally thousands of different kinds of credentials in the past. Even within single agencies there were sometimes multiple kinds of credentials. I think we'll see the same kind of thing develop in some of the kinds of businesses that have risk profiles that demand early adoption. Financial industry, I think, is probably the one that we'll see lead the way in the commercial business sector.

Julia Allen: What do you think some of the catalysts have been to get convergence efforts started?

Brian Contos: Well, I think people definitely have a better understanding of risk, and they realize that a threat from somebody trying to hack in from the outside, or the threat from an insider planting malicious code on the network, or somebody from the cleaning crew walking out with a server that contains your customer database, are all pretty legitimate risks, and they have to be approached in a way that's more general, more holistic.

And, like we mentioned very early on, the idea of having IP-centric solutions — that's going to allow them to take advantage of these overarching policies that say, "Yes, it's a good idea to look at physical security, it's a good idea to look at logical security category." I think that's helping to drive that. And solutions like RFID (radio frequency identification); Bill mentioned video analytics. There's a number of technologies out there now that are very focused on this specific problem that are helping these organizations say, "Let's take your risk posture, let's move it from the idea that convergence is a good idea to a practical one." And they're finding that this is just a very natural, logical progression of their organizational environments.

Julia Allen: Yeah, that makes a lot of sense. Let me move on, if I may, to ask both of you: what do you think some of the - based on your observations and working with organizations who are going through this, what do you think some of the biggest challenges have been to date, both political and technical?

Bill Crowell: Well, one of the biggest challenges is standards. We've seen that in virtually every one of the logical security technologies, whether it was encryption, authentication, identity management, and so on. So standards are a big potential driver and also a big impediment if we can't actually achieve uniform standards across this industry.

A second potential impediment — in fact, it's an impediment that we do see in the industry right now — is this skill set change. The people who've been involved in physical security for the most part have been law enforcement professionals who went into the security business. And the people involved in logical security have been primarily IT specialists who developed special security skills. We're going to have those kinds of people still, as Brian mentioned, but we're going to have to find a way to bring them together under common management with people who do understand both or all of the areas of the new security regime.

Julia Allen: Brian?

Brian Contos: Yes, I agree with Bill wholeheartedly on that one. One of the biggest issues is as low tech as you could possibly imagine — it's lack of communication. And it's not just that these groups don't communicate well. In many cases, they don't even really know who each other are. I

was working with a very large telecommunications company and they were in the process of bringing on one of these CACs, these CAC (common access card) solutions that I had mentioned earlier. And one of their biggest issues was, well, who is in physical security, who runs that? Is that facilities, is that HR, is it a different group? Do we outsource it? They weren't even sure who the group was. So the simple act of just getting together and talking through the solutions as a team I think is a huge step.

And then, of course, there's the overriding politics. At a lot of organizations it's sometimes hard to get past that barrier of, "This is the role of a physical security person, this is the role of a logical security person. They're completely in a silo, they should never communicate, there's no reason for them to communicate" — getting past that barrier. Now that barrier has been disappearing, especially over the last couple of years. But general communication is certainly the big driver behind getting these two groups to work together.

Julia Allen: So given some of those challenges and opportunities, what do you both think are some steps that business leaders can take to get their convergence efforts started?

Bill Crowell: Well, the first step is to recognize that convergence is taking place and to begin looking at their own organization in terms of the opportunities that that would provide them — organizational opportunities, opportunities to save money in terms of the expense, the cost center of security.

And then one other we haven't really touched on yet, but I think it's going to be important in the future, and that is the opportunity to make security actually a part of aiding the business function. For example, video surveillance cameras don't just have — can look for marketing information as well as for security information. And there are opportunities like that that are extremely important for the business leader, the CEO, or the head of an agency to examine and to then build into their planning for the future.

Julia Allen: Brian, any thoughts on steps for getting started?

Brian Contos: Yes. Well, we've been talking a little bit at a high level, so I'll jump back down, right into the technology side. I would say when you're evaluating various technologies or looking at what you currently have made an investment in, look across the board at incident prevention, incident detection, and incident response, both on the physical and the logical side, and see how you can tie these two things together. More chances than not, you're going to find with newer solutions that there are going to be synergies, there are going to be ways to integrate. Of course there are the cases — and I'll share one with you.

We were working with a large financial on the East Coast. They actually had a badge reader system, and they wanted to pull it into their centralized monitoring solutions, with other firewall and database logs and things of that nature. Well, the problem was we found out that the device actually could generate logs, but when you looked at the logs they were LPR (line printer remote) output, which is printer output. So you got a bunch of hash marks and page numbers and generally things you don't expect to see in a log. Well, you can clean that stuff up. But then when you got to the actual data you found out that what it was producing was simple maintenance data - "I've been up and running for five years straight, I've had two falls, I've had this many problems." It didn't even track who entered or who exited the building.

So when you're evaluating new technologies — and the physical technologies are much slower upgrade time; you'll find a lot of solutions that have been deployed for 10 years or more — look for ones that are IP-centric, look for ones that you can integrate with, like a centralized LDAP

(lightweight directory access protocol) solution that creates ODBC (open database connectivity) database logs, that you can communicate with and correlate with all your other devices. So I think from a technology perspective, it's just another area to keep in mind when organizations are doing product analysis and looking to make procurement decisions.

Part 3: Trends and Future Directions

Julia Allen: Excellent advice. That helps make some of the concepts really tangible. As we start to get towards our close, I'm interested — we've talked a lot about where the two of you see this whole arena moving into the future and in trends that you see on the horizon and actually happening today. I'm also curious to explore a bit if you see any differences by market sector or type of organization or public versus private. Are you finding particular trends or issues tend to aggregate within a particular market sector, or does that not really matter that much?

Bill Crowell: Well, I personally believe that while there will be differences between public/private, financial and retail, and so on, that over time those differences will become more differences in functions and functional approaches rather than in technology. Essentially we will see the combining of video surveillance, RFID tagging, identity management, information security, and physical security systems by, in every case, being able to generate security event data that then can be analyzed and correlated to provide information about what's happening in terms of risk. That will be the common thread across all of those, and the differences will probably be in various degrees rather than in kind.

Julia Allen: Brian, any thoughts on that?

Brian Contos: Yes, I'll just say this. When I first started looking at this issue and working with organizations, intuitively I thought it would be critical infrastructure. I thought it would be large federal, government organizations, military intelligence, the things that you would think are just very, very concerned about security, that they would get this right away. And in some cases they did, and in some cases they didn't. And then further I found that retail and health care and financials, again in some cases they did or they didn't get it.

So I actually find it to not even be a question of what vertical and whether or not they're in the public sector or the private sector, as much as the vision of some of the key decision makers in the organization, their capability of saying, "We either have the people under us that are explaining this and communicating the risk effectively," or, "We intuitively ourselves understand the value." And, again, that seems to be without borders.

Julia Allen: So how do you think you would raise the awareness of someone in a key decision-making position to address this in a holistic, enterprise-wide way? Any thoughts about that?

Bill Crowell: Well, the way that Brian and myself and our colleagues have been addressing it is to actually write a book which addresses all of these issues, including the technology, the organizational issues, and even the how-to, on the technical side, build converged systems. We believe that there has been a shortage of information about not only the advantages and the ability to change the entire complexity of risk assessment and risk management, but also that there's been a dearth of information on the how to do it technically and how to make it work.

Brian Contos: Yes, one of the approaches we took, and I'll just mention the book again, was the fact that—.

Julia Allen: And the name of your book?

Brian Contos: Physical and Logical Security Convergence Powered by Enterprise Security Management. But one of the things that we did in the book was we looked at the idea that risk is risk; it's not discrete just because it's physical or logical and there's business drivers. And I think as security practitioners — of course I came from the logical security side — we've always had to try to develop this skill set of communicating risk in business terms to executive management, to explain that a buffer overflow on this database equates to possible fraud or identity theft and any number of things that they can understand so executive management can make a key decision. We try to get across the fact that this is now applying to both physical and logical. So when you're trying to communicate these risk levels to executive management, consider these variables.

And as Bill mentioned, there wasn't a lot out there, and that's one of the reasons that we did decide to write the book. There are some white papers and varied pieces of information on the Internet, et cetera. But really bring this general thought process together when you're talking to executive management and when you're trying to explain risk, and that will really get businesses thinking about this in the right way.

Julia Allen: Well, I'm so very appreciative of your time and experience and perspective today, both Brian and Bill. Thank you so much. And of course we'll include information about the book and any other related references that you would like to include in our show notes. Just in closing, is there any key points you'd like to summarize or touch on that we haven't mentioned? Or have we pretty much covered it for this conversation?

Bill Crowell: Well, one concept that I think is an important one to just kind of lay in at this final moment is the fact that for years now we've been talking about security and layered defenses. The truth of the matter is layering defenses, whether it was in the IT world or in the physical world, was very, very difficult to achieve before this notion of convergence came along. And now, because we can connect all of these over the IP network, we really can have many layers of security that are aware of each other, and in doing so we make it much more difficult for people to defeat the system, if you will, by attacking one of those layers, because they still can't get through all of the others.

The other notion that Brian mentioned and I'd like to just reiterate is that the CEOs, the boards and the senior executives of large organizations and businesses, don't really think about security; they think about risk. And if you try to talk to them about security, they kind of yawn. But if you want to find out what keeps them up at night, it's the risk associated with business over the Internet or the risk associated with terrorism threats, if they're a critical infrastructure, and they focus on that. And we've tried to make that the central theme in the book, when we address this convergence notion.

Julia Allen: That sounds very well advised and works particularly well for the audience that we're hoping will find this information useful, putting it into terms that they can really identify with. Brian, any final thoughts or closing points?

Brian Contos: No, I think Bill really summarized it well.

Julia Allen: Well, again, thank you both very much. I appreciated this opportunity, and I look forward to talking with you again in the future.

Brian Contos: Thanks, Julia.

Bill Crowell: Thanks very much, Julia.