Enterprise Architects Increasingly Join in Common Defense Against Cyber Security Threats

Transcript of a sponsored podcast on how private enterprises and government agencies can combat the growing threat of cyber crime and the looming threat of cyber terrorism.

Listen to the podcast. Find it on iTunes/iPod and Podcast.com. Download the transcript. Sponsor: The Open Group

Dana Gardner: Hi. This is Dana Gardner, Principal Analyst at Interarbor Solutions, and you're listening to BriefingsDirect. Today, we present a sponsored podcast discussion, coming to you from The Open Group's Security Practitioners Conference in Boston, the week of July 19, 2010.

We've assembled a panel to examine the need for improved common defenses, including advancing cooperation between enterprise architects and chief security officers to jointly defend against burgeoning cyber security threats. The risks are coming from inside enterprises, as well as myriad external sources.

We'll learn more about the nature of these borderless, external, cyber security threats, as they emerge from criminal enterprises, globally competitive business sources, even state-based threats, and sometimes a combination of these. We'll also hear recommendations on developing smarter processes for cyber security based on proven methods and pervasive policies.

To help broaden the scope of enterprise architecture, and to develop a leverage point for mission architecture, levels of security and defenses, please join me in welcoming a security executive from The Open Group, as well as two cyber security experts who are presenting here at the conference. Allow me to introduce you to General Harry Raduege, chairman of the Deloitte Center for Cyber Innovation. Welcome.

Gen. Harry Raduege: Thank you very much, Dana. It's good to be here with you.

Gardner: We're also here with Usman Sindhu. He is a researcher at Forrester Research.

Usman Sindhu: Thank you, Dana. Good to be here.

Gardner: And Jim Hietala, Vice President of Security at the Open Group.

Jim Hietala: Hi, Dana.

Gardner: Let's start with you, Harry. Tell us about the nature of the threat. Perhaps there's a level of the intensity about these external threats that the enterprise practitioners, the architects, don't perhaps quite appreciate yet.

Raduege: Thank you very much. Today, at this conference, we put a few of these areas that you've mentioned into perspective. As far as the world of cyberspace, it's a tremendous opportunity for us to gain the benefits of being able to communicate, not only nationally, but also internationally, and across all borders in the area of cyber.

But, with that openness, come these new threats. The vulnerabilities that we have of operating in cyberspace are magnified by the threats that are out there today. These threats are in the areas of identity theft, information manipulation, information theft, cyber crime, insider threats that are prevalent in many of our organizations and companies today, the threat of espionage, of losing lots of intellectual property from our businesses, the cyber attacks that are taking place, the denial-of-service (DOS), and also the threat that we see on the horizon -- cyber terrorism.

Gardner: If you're a business or a government agency, perhaps a multinational corporation, is there a commonality or is everyone getting hit the same by these sorts of things? Who's vulnerable, who isn't?

International problem

Raduege: The Internet and all of our connections in cyberspace are across all nations of the world. In fact, this is an international problem and opportunity for us to take advantage of it. Basically, Dana, we're all in this together.

THE Open GROUP
Making standards work®

This is the significance of this type of a gathering, to talk about the real benefits of cyberspace, but also to talk about the issues of cyber security that are facing us all. The importance of the underlying foundational aspects of having a great enterprise architecture is pointing more toward a mission architecture for business success.

Gardner: Are there commonalities, more need for standards, practical ways that cut across the different types of organizations that perhaps are in the works, but that other people aren't aware of? That is to say, how important is education towards moving against some of these common threats?

Raduege: A number of organizations like The Open Group are working on the common standards that are so important for the international community to comply with and to have as guiding factors. Education is very important, developing a cyber mindset across all people of the world, not only in the government organizations, but for industry, and also the individual users at home.

The aspects of education and training and awareness of what's going on there in cyber is paramount for proper operation, but also for the protection of your critical information.

Gardner: Harry, are there things that are going on within governments, and not just in the US, that are buttressing the protections and reducing the risk for enterprises and that maybe

enterprises aren't aware of? How could that cooperation between public and private perhaps improve?

Raduege: Since everyone is member of this international community in cyberspace, everyone's trying to address the issues that are so common to each one of us. Many people are bringing best practices to the table. We're learning from each other's experiences. As I mentioned earlier, we're all in this together.

The international cooperation, the international collaboration, and the opportunity to meet and discuss these areas are very valuable to all of us individually, and to our companies and to our nations.

Gardner: Usman, you had an interesting presentation. Tell us about this notion of smarter. How is it that organizations, particularly enterprises, need to adjust their thinking in order to better protect themselves?

Sindhu: We're living in a very exciting time in terms of the innovation, as well as the adoption of technology. Inventor Ray Kurzweil talks about the law of accelerating returns. He says that we're experiencing 20,000 years of adoption and technology growth. In the 21st Century we'll have lot of innovations and more so technology adoption in a much more accelerated fashion.

The smart concept

That's where the smart concept comes in. This entails smartening our physical infrastructure, our critical infrastructures like utility, healthcare, financial services, transportation, public safety, and also city administrations, down to the IT system itself.

It will use of lot of IT enablement from either the cloud or communication infrastructure, things like RFID technologies, 4G technologies, and solar technologies, to embed lot of situational awareness, analytics, and locationing into the systems.

The need for this is present, if you look across the board at some of the incidents or some of the events. The BP incident shows us that the inefficiency, the number of physical infrastructures that are siloed, present a huge opportunity for technology growth.

This is a smart kind of a concept that embeds itself into smart city infrastructure where all the different components embed all the IT technologies together. There are other initiatives like smarter grid or smart healthcare that are embedding these IT technologies as well.

That's a great way to start the 21st Century with this innovation, but the need for security arises at the same time. As Gen. Raduege mentioned, cyberspace is a new frontier, or information security in the cyber world is a new frontier.

That's where we have to address lot of different issues and problems around policy, architecture, and best practices. It's only going to get more serious, as we connect a lot of different systems that were not connected in the past.

Gardner: So, from Forrester Research's perspective, this smartness isn't just a technical smartness, but it's also the policies, the methods, and best practices. Tell me why best practices fit into this notion of smartness, and then maybe revisit how the threat increases with that interconnectivity.

Sindhu: Traditionally, security has been a point technology. Even in the government space, there has been a lot of focus around just technologies. Earlier today, in other sessions, we saw how the importance of point technologies has been overemphasized, rather than risk analysis and the process.

Today, many organizations, including the public and private sector, are waking up to the fact that technology alone is not the answer. It's the process and people as well. That's where deriving these best practices would be a key in collaborating with the private and public sector and bringing in an architecture that supports all three silos.

As far as this interconnectivity is concerned, you'll see lot of different business-to-business (B2B) and business-to-consumer (B2C) interactions. It happens today. Today, business partners and distributors do business on the go, on social media, either Twitter feeds or Facebook, or something I call ad-hoc communication through their mobile devices. This is the nature of today's interaction. This is the nature of B2C and B2B interactions.

Perimeter notion

With that, threats increase manifold, because we tend to look at more of a perimeter notion of security. If you look out there, we're actually in a stock market situation, where information is flowing all over the place and we have no perimeters, so to speak. We need to understand this re-perimeterization, rather than de-perimeterization. How do we put security control at proper threat levels?

Gardner: One area where increased connectivity is not a threat is in connecting more of the enterprise stakeholders who perhaps have a role or a piece of the security puzzle, for them to be a bit more cooperative and coordinated. Tell me how smartness fits into collaboration between architects, chief security officers, and other stakeholders?

Sindhu: It's a great question. One of the key aspects of smartness is cross-industry and cross-team collaboration. Today, when we start to look at some of the smart deployments, either in the vertical sectors like utilities, healthcare, or even other private-sector industries, we see more and more that security is getting attention from the board-level and C-level executive.

Similarly, enterprise architecture is getting its attention as well. Going forward, we see a great emphasis on combining these two initiatives, even though it's still a very nascent stage at the

board-level talks and C-level talks. We're not seeing a huge focus on cyber security in some instances, but of course it's changing. It's increasing.

It's fair to say that the security and enterprise architecture will play a key role, as both concepts mingle together to bring about best practices in architecture in the early phases into planning, deployment, and delivery of the smart services.

Gardner: How about that, Jim Hietala at The Open Group? You're all working with framework certification, defining and professionalizing the role of the enterprise architect. How well are we doing with imbuing security into that larger picture of enterprise architecture, as well as technology and process?

Hietala: I'd echo what Usman said. It's early for really bringing enhanced security into the professional enterprise architecture. So, in The Open Group Architecture Framework (TOGAF), three of the nine iterations of it, we've added significant security information and content that enterprise architecture need to bear in mind in developing architectures.

But, that work is ongoing. We have a couple of projects both to enhance the security of TOGAF, and also to work to collaborate with the Sherwood Applied Business Security Architecture (SABSA) folks, another security architecture development methodology, to harmonize those two approaches.

There's a lot of work ongoing there, and there's a lot of work needed in developing reference architectures outside of purely IT. We have a document that we are updating called Enterprise Security Architecture. It will be published this fall, and updates some work that was done five or six years ago, sort of an IT reference architecture.

We see a need, as you start to look at cyber security and the different kinds of architectures, to develop new reference architectures to address some of these new applications of IT technology to everyday life. If you think about networks in cars or networks of smart devices comprising the power grid, what does security look like for those things? Our membership is starting to look at some of those and trying to determine where we can add some value for the industry.

Gardner: Let's think a little bit more now about this notion of mission architecture, The Open Group and many organizations are involved with enterprise architecture, but, Harry, what do we mean by mission architecture? What does that mean and how does it relate to the concept of enterprise architecture?

Changing world

Raduege: The Internet has changed our world and the way we operate. For years, we've had enterprise architects who have been working down the hall or in the basements of organizations, and who have been trying to figure out the best way of technically aligning the Internet and all of the interconnected networks to make it work as best it could.

Now that this world of cyber has really come upon us, it has really elevated the importance of the enterprise architect into the higher levels of an organization, just because of the threats that are constantly coming upon us in our business operations and our mission success.

The enterprise architect has now gotten the attention of the C-suite executives and organization leadership. But, they don't like to think as much about enterprise architecture, because it really has that technical connotation as my colleagues here have mentioned, we're really talking and focusing more now on the people and the process aspects of running the business properly.

The front-office people, the C-suite executives and leaders of organizations, instead of thinking about enterprise architecture from a technical aspect, are becoming much more interested in a mission architecture.

In other words, what's the architecture needed to complete my mission so that I can have success -- whatever your mission is, if it's government activity or whether it's industry. Mission architecture has taken on new meaning that takes into account the technical architecture, but also adds the workforce domain and the process elements of the organization.

So, mission architecture is really pointing toward business success, whatever your business is, whether it's government operations or industry.

Gardner: Usman, how do you relate mission architecture to your discussion about being smart?

Sindhu: A couple of things that come from a mission architecture perspective and a smart aspect in general, is what we're seeing in the industry as the IT risk baseline. There has been a lot of work done, and it gets even more important. How do you derive an IT risk baseline?

Architecture is important, but there is no silver bullet to it. Since the smart concept is industry-wide and is global, there could be many references to architectures that could go in. Some things have started to happen. For example, the Department of Homeland Security came over to IT risk baseline about a year-and-a-half ago. It collaborated with the IT vendors and IT sector in general and started to create this risk baseline, which comes about in the earlier phases of architecture.

As you develop a framework, you take feeds from the various industry standards and regulatory compliance mandates and you start to create a risk baseline, a risk profile that touches every single silo of people, process, and technology. Over the time, you do the collaboration, internally, but externally as well.

Also, you market the risk baseline component so that you are complying with it, but you're also educating this to your peers and your other adjacent industries. The smart concept, at its heart, would require a lot of collaboration among the public and private sectors. I see a lot of this is being driven by the government. The Department of Homeland Security is actually working on coming with the next iteration of this baseline, maybe next year.

I see a more cohesive approach, even though a lot of work needs to be done here, and in distinct industries like smart grid. There has been a lot of focus around standards. The National Institute of Standards and Technology (NIST) is working on creating a cyber security baseline and framework that touches interoperability as well as the security standards. A lot of work needs to be done. We're still at a very early stage.

Gardner: As we elevate from IT concerns to architecture and enterprise concerns -- and now we're talking at the mission architecture level -- do we run the risk of this becoming a hot potato? That is to say, no one really owns it, but it gets handed around. How do we organize an approach to a mission architecture in such a way that it's got the right level of command and control and yet is inclusive? Any thoughts around the organizational imperative, Harry?

Organizational concepts

Raduege: Maybe we can take a page from what the United States government has just recently gone through with organizational concepts, because we knew that many different activities across the federal government had a big part to play in securing cyberspace. The Department of Homeland Security, Department of Defense, the Intelligence Community, Department of Interior, Department of Commerce, Department of State, every one of those federal government activities had a specific role to play in securing cyberspace.

However, we found out that there was no one totally in-charge of orchestrating the elements and activities of our federal government. So with the President's Cyberspace Policy Review, he decided to appoint the first ever White House Cybersecurity Coordinator, Howard Schmidt. Howard is the overarching orchestrator for all of our federal government activities, all the state and local and interfaces with industry, and also the international community.

If we're going to think about an organizational construct, our nation is led with that kind of an example of an individual at the top who provides the oversight, is also responsible and accountable for the proper operation of cyberspace and the cyber security elements.

Gardner: Jim Hietala at The Open Group, any thoughts about this organizational angle in terms of the personnel, their roles, and a rethinking of how these categories have so far been structured?

Hietala: From an enterprise perspective, looking at mission success and thinking about cyber security really is the CISO role inside a given enterprise. That probably is most relevant to address the issues. The interesting thing is that many of the new developments that we're looking at -- whether it's smarter hospitals, smarter medical devices, smarter electrical grid -- are industry specific and they require a lot of cooperation between organizations in an industry.

There's a role for standards and industry organizations to pull together and come up with some common standards to facilitate better security, maybe better frameworks or things like that, that can be leveraged across an entire industry.

Gardner: Any thoughts about getting started? Where do you get traction on a problem like this? Again, we've got a lot of different stakeholders and many different siloed types of activities and technologies. Where do you begin to actually get ahold of this and make some impact?

Hietala: It depends on the industry, but you get started just getting smart people in a room and trying to find consensus around the problems and potential solution. We do a lot of that here at The Open Group in different areas. We have a lot of defense work that we're doing with the suppliers to the military and those sorts of things. We get them in a room, drive consensus, and develop standards and best practices that all of them can leverage and that help their business be more secure.

Gardner: As Harry mentioned, there are some examples in the US government. There are governments, I imagine, as well where they've attacked this problem. They've made some strides, developed some approaches and methods. Is there an opportunity for increased public-to-private cooperation and standardization and can you think of any examples of how that's working?

Hietala: Definitely there is a need for increased public-sector and private-industry cooperation. We have an initiative here at The Open Group called the Acquisition Cybersecurity Effort. It was brought to us by the Department of Defense as a consulting effort. They wanted an organization to pull together private industry and try to drive some standards looking at the supply chains to the major IT suppliers. That work is ongoing and that would be a good reference of an initiative like that.

Gardner: Harry, how about from your perspective on getting started? Where do you get a handle on this beast?

Specific areas of expertise

Raduege: As my colleagues here have mentioned, a lot of times in private industry, there is a number of individuals who, just like in the federal government, have specific areas of expertise and responsibilities in the organization. From the boardroom perspective, this could be a little confusing. You'll have a Chief Information Officer, a Chief Information Security Officer, a Chief Privacy Officer, a Chief Management Officer, a Chief Financial Officer, and a Chief Operations Officer.

Doesn't this sound kind of familiar to what our federal government looked like -- everybody has a specific role that is very, very important, but then, who is the one person then who talks to the CEO or the board? I know a lot of organizations wrestle with that concept.

In 1996, there was actually legislation, the Clinger–Cohen Act, which was officially called the Information Technology Management Reform Act. It said that across the entire federal government, there would be CIOs appointed, and they would report directly to agency heads. That has guided our federal government for quite some time, but these aspects of all the different

areas need to be brought together and focused within organizations. We really have our work cut out for us.

Gardner: To you, Usman, perhaps some thoughts about getting started on the process of getting smarter?

Sindhu: One thing I'd like to echo from the previous question as well is that it's interesting to see how long it took security to get the attention it needed. Finally, it's getting the attention at the C-level. Then, from a budget perspective as well, they're getting a much better share of the IT budgets that they had before. So, there is a good momentum around understanding security early in the development phase of a project, a product, or any other deployment.

Now, when cyber security is talked about, this is another new beast for many organizations to deal with. In fact, I was speaking to one of our utility clients, and the cyber security lead mentioned that he has no approach or visibility into the earlier phases of when the vendors are selected or when the RFPs are made. He only comes in a second tier, when he has to accredit all the different vendors.

So, there is still a kind of ramp to cross at getting attention at the earlier phase from a security professional's perspective. Cyber has to be on that agenda as a top priority.

As far as smart initiatives, you need to get security involved and architecture involved earlier in the phase. I normally use a three-level or a three-phased approach, when we talk about the planning.

Many of the smart initiators today -- smart city, smart grid, or smart healthcare -- are mostly in the planning phase. In a year or two, we'll see a lot more deployments. Deployments are happening today as well, but we'll see a lot more deployments in a year or two. Then, the delivery phase will come when the smart services will be delivered to the consumers and businesses.

The role of the architecture and security has to be involved right from the planning phase, where you manifest the value of security being built in, either to the products or in general to the architecture? That has to be the first step -- that we acknowledge the need to embed that into the overall process.

Gardner: Thanks so much. We've been discussing the need for improved common defenses including advancing cooperation between enterprise architects and security officers, and to jointly defend against burgeoning cyber security threats.

This sponsored podcast discussion is coming to you from The Open Group's Security Practitioners Conference in Boston the week of July 19, 2010. I'd like to thank our guests. We've been here with General Harry Raduege, chairman of the Deloitte Center for Cyber Innovation. Thank you.

Raduege: Thank you very much.

Gardner: Usman Sindhu, researcher at Forrester Research. Thanks for the input.

Sindhu: Thank you. It's been a pleasure.

Gardner: And, Jim Hietala, Vice President of Security for The Open Group. Thank you, Jim.

Hietala: Thank you, Dana.

Gardner: This is Dana Gardner, Principal Analyst at Interarbor Solutions. You've been listening to BriefingsDirect. Thanks for joining and come back next time.

Listen to the podcast. Find it on iTunes/iPod and Podcast.com. Download the transcript. Sponsor: The Open Group

You may also be interested in:

- The Open Group's Cloud Work Group Advances Understanding of Cloud-Use Benefits for Enterprises
- The Open Group's Allen Brown on Advancing the Value of Enterprise IT Through Architecture
- Mutual Embrace of SOA and Cloud Computing Builds Into Productivity Waltz Across the IT Landscape