Public-Private Partnerships: Essential for National Cyber Security Transcript

Part 1: Communication, Trust, and Information Sharing

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 operational resilience and software assurance. Today I'm very pleased to welcome back

John Haller and Sam Merrell, two of my colleagues who are members of CERT's Resilience Enterprise Management Team. I'd also like to welcome to the podcast series Philip Huff. Phil is the Manager of Security and Compliance with the Arkansas Electric Cooperative Corporation.

For today's podcast, John, Sam, Phil, and I will be discussing the actions necessary to create public and private partnerships between government and industry to strengthen national cyber security efforts. So with no further ado, I'll welcome back John.

John Haller: Hi, it's nice to be here.

Julia Allen: And Sam, really glad to have you with us today.

Sam Merrell: Thank you very much, Julia.

Julia Allen: And Philip, thanks for joining us.

Philip Huff: Thank you, Julia. Good to be here.

Julia Allen: Just one more thing, for our listeners' information John, Jeff Carpenter, and I have posted a podcast on establishing a national computer security incident response team, which is the first in this series on best practices for national cyber security, and today's podcast in the second in the series. So if you like the topic, make sure to tune back in the future.

So Sam, why don't you get us started, just to lay some of the foundational definitions? What exactly is a public-private partnership? What do we mean when we say that? And particularly when it comes to national cyber security, why are public-private partnerships so important?

Sam Merrell: Sure. So I guess it's best to establish a context and say that public-private partnership is best characterized as being a means to an end. It's a tool to enable other things to get accomplished. So particularly when we think about critical infrastructure protection in the United States and any other market economies, the infrastructure or the elements of an economy that are the most important and most significant are often owned and operated by the private sector.

What's curious is that in most nations the government or the public sector holds responsibility for protecting the infrastructure. But in the case of critical infrastructure, the government doesn't actually own that in a lot of situations. So the public-private partnership is a mechanism to facilitate this shared risk management.

The idea that the government has a lot of information that it learns through various means and methods, and these owners and operators of critical infrastructure have the hands-on access to the, in this case, information systems and can actually take the acts necessary to protect that. So the public-private partnership is necessary because of the fact that we have these various components that are responsible for overall national cyber security management.

Julia Allen: It's kind of a tough role for the government to have both the oversight responsibility, maybe the national mission and information coming from all these sources but yet not have the feet on the ground, right? Because the real operational responsibility is in the private sector, correct?

Sam Merrell: Exactly. There's a lot of challenges. And some of those challenges are organically developed over time, trying there are challenges such as legislative barriers. There are just normal communication barriers, running to challenges of just information sharing from, that involve a global economy.

For example, as an individual organization, it may be owned by foreign national but it's still part of another nation's critical infrastructure. How do they work through those barriers of sharing information yet not sharing too much information? So there's a lot of very interesting challenges to making this successful.

Julia Allen: Great. Well first Sam, as you know, we're going to talk a little bit about the work that CERT has done on best practices, and then Philip has kindly joined us to talk about an actual case in point of a public-private partnership that he's involved in.

So again, to continue with our foundation, in yours and John's report, *Best Practices for National Cybersecurity: Public-Private Partnership*, there are two top-level strategic goals with sub goals. So if you could just introduce the two top-level goals and then we'll dig into those a little bit more.

Sam Merrell: Absolutely. So, and if you think about public and private partnerships as a method of communication, these goals shouldn't be, aren't very surprising. So first and foremost, we say that the primary goal for these types of relationships is to facilitate communication between the two entities, the government that has certain information it needs to share and the private industry or the private sector that needs to implement or take action.

And then second of all, these relationships exist for a very deliberate reason, that is to support the overall national cyber security strategy. So they can't be understood in a vacuum. They have to be wrapped around the context of why are you having that communication, what do you hope to get out of the communication, and what national capability do these communications need to enhance or enable?

Julia Allen: Great. So John, your turn at bat. So with respect to the first goal, the one about facilitating communication what have you found are some of the key actions that help participating government and industry organizations get a better understanding of each other's point of view? How do you break that down at the practice level?

John Haller: Well, one of the primary things is that the governments and industry really need to establish trust between the two of them. And one of the main things there is in many cases and this is very contextual. In other words, it may differ by economy or country or history. There may be structural and legal barriers that prevent private entities like firms, like profit-seeking firms, from exchanging information with the government and vice versa.

Again, that can relate to historical factors, like maybe they have no tradition of that kind of communication, or political factors, or legal factors. And I'll just give a quick example from the U.S. case.

Several years ago, in fact in the aftermath of September 11, 2001, the U.S. government wanted to encourage industry and critical infrastructure providers to share more information about critical systems vulnerabilities and certain vulnerabilities.

Well, one of the issues that industry had was that the United States and many other western countries have freedom of information laws, laws where citizens can go through certain procedures and obtain information held by the government, information that's in the so- called public sphere.

Now, in the U.S. of course, there have always been certain limitations to freedom of information laws, for instance, surrounding national security and so forth. But the concern for industry was that if they provided information to the government that goes into the public sphere, that anyone would be able to obtain that information, criminals wishing to misuse their system or even competitors, or the information could just be misused in a variety of ways.

So before there was really a better exchange of information, the government had to come along and modify that law, change the legislation in ways essentially to expand the definition of national security information and to categorize information that private firms provided with regard to critical systems vulnerabilities as protected or not necessarily subject to the freedom of information laws.

So I mean again, that's just one example from the U.S. case. Depending on the country or who's looking to do this, the reasons or the obstacles to public-private communication might vary. But the main idea is to really take a look at the laws and really communicate about what some of the barriers are to an exchange of information.

And I mean, a big part of that, and it's not necessarily covered in the paper, but a big implicit part of that is really trust at the personal level. I mean the ability of leaders in the government to really put energy into this and cultivate relationships in industry I think can't be underestimated.

And the second part of that is more specific to what we say communications methods, channels, and rules. So for instance, government needs to communicate with industry and decide within industry what kind of rules they'll put in place to protect and exchange information. So who's going to store information? What's it going to be used for?

But more specifically, for instance if government provides sensitive information to, let's say, an industrial firm, how can that information be used within the firm, and with whom can it be shared so that all sides have a good idea of really where their information's going and what it might be used for?

Julia Allen: I think the information and the sharing of information and the classifying or categorizing of the information and how it's to be handled is so key to making these types of relationships go.

So in the general practices or guidelines that you've developed, do you find that it varies at all by critical infrastructure sector? Or do you think there are commonalities pretty much across all sectors in terms of information sharing?

John Haller: I think that some of the commonalities may have to do with the sensitive government information. For instance, information about threats and so forth. Some of those rule sets seem to be pretty similar.

However, with regard to information that industry would share and give to government, I think that really tends to vary pretty widely based on the sector, and what kinds of information they might share with the government, for instance about assets and vulnerabilities. I don't know if Phil has any comment on that, being out and working with NERC and so forth. But my sense is that as far as information coming from industry to government, it might be very specific to the sector or even the firms.

Philip Huff: Yes, and from a private sector perspective, especially from the electric industry, we aren't as aware of the way information is handled coming out of the sector as much as coming in. I think you captured it correctly, the various levels at which information is classified. That filters down to us in the private industry as well.

Part 2: Private Sector Benefits and Pain Points; Partnership Models

Julia Allen: Okay Phil, since you've got the air space now, excuse me, Philip. When it comes to supporting a national cyber security strategy, which Sam identified as the second goal -- taking this communication and trust relationship and applying it to an actual issue or area of concern in terms of cyber security strategy.

You're obviously on, more on the private side. So what do you see as some of the benefits of the partnership for an industrial organization? But on the flip side there are benefits but also perhaps you could touch on some of the concerns that you see.

Philip Huff: Yes sure. And I'll try to discuss the benefits first. You had mentioned previously that it's a pain point for the government to have information but not have boots on the ground. And I think likewise from our perspective in the private industry, we have the boots on the ground, but a lot of times we don't have the information.

And so that one of the chief benefits for us is to have involvement in the solution. If there are new threats or if there's concern about how the private sector is handling cyber security protections, then it's very beneficial for us to be involved in crafting solutions, crafting mitigations that make sense and are effective within the industry.

I think especially with cyber security, if a threat's cyber related, it's typically very complex. And a lot of times the government doesn't necessarily understand the full ramification that industry is trying to keep up and trying to understand what the ramifications of the threat are.

And so a lot of times the initial reaction, at least from a regulatory perspective is, "Well, we don't really understand it, so just protect everything." and that can be very damaging in that public-private partnership, obviously.

If the private sector has a legitimate role in crafting the mitigation, not just where we have input but where the input is heard and responded to, then I think the industry can take the threat information and better determine how to actually mitigate the threats and vulnerabilities. It also allows us to have buy-in on the solution, which is very important as well.

I think secondly, another benefit is for as we mentioned, the government has a very good understanding, they clearly have the upper hand in understanding the threat. Traditionally in

our risk models in the industry, we look at historical data and look at probability for threat information. And so we really don't have good models to be able to determine emerging threats. And the government can really help out with that where if there are these low-frequency events, we really need that real-time threat information to be able to make determination. Because our traditional models of internal information, internal threat information, just don't really help out with those high-impact, low- frequency events.

And regarding the pain points, I think in a similar vein, it's difficult for us to receive relevant threat information from the government, particularly if they don't have, as was mentioned before, that trust relationship built where there is information flow between the government and the private sector. And typically at some briefings, we may be given just a broad brush of threat information and very little of that is actually relevant to us.

Also, it can be equally frustrating to hear briefings where they provide just enough threat information to where there's really no feasible solution to it. So it's this bad thing that's so bad you can't possibly do anything reasonable to prevent it. And I think that type of sensationalism destroys the dialogue between the two parties.

I don't want to sound fatalistic here. I think we've been able to manage as an industry. I think the electric sector in general, we've been at this for a long time and we have people that can play in both the government and private sector that can speak both languages. And we're starting to get more relevant threat information.

Sam Merrell: I think what's becoming clear is there's an overall balance that needs to be struck between the tensions of not sharing too much information but sharing enough to help out and be useful.

Philip Huff: Right.

Sam Merrell: And it's been a long road to take to get to that point to understand where that balance can be struck and I think in a lot of aspects, it's still been a growth opportunity, where the government's still trying to figure out how to effectively communicate without revealing too much things that they didn't want to reveal but still be contributing to a solution.

Philip Huff: Right. And it's important for an industry that's so technical -- those type of people, myself included, we pretty much demand the level of detail that's necessary for us to create mitigation strategies because that's really effective. This broad threat information isn't as useful.

Julia Allen: Great. Well thank you both, Sam and Phil. And Phil, we're going to get you back on the call in just a minute to talk specifically about the North American Electric Reliability Corporation. But I'd like to interject one question for John, again, just to put this basic structure in place.

So John, in the report that we've been talking about, one of the other aspects of it is that you define, based on your observations and experiences, you define three models for structuring a public-private partnership that you've seen work effectively. So could you briefly talk about each of these and maybe some of the pros and cons?

John Haller: Sure. I mean, first what I'll mention is, and I guess this is a common saying around our organization, “all models are wrong, some models are useful.” So I'll just say as I'll talk about these with the understanding that they're not necessarily mutually exclusive. In other

words, the actual public-private partnerships that exist today and are in operation may share characteristics of all of these. But basically, what we tried to do was, we looked at how governments and private industry are structuring partnerships now and what some general clusters of examples are, or models of examples that can help countries that want to do this understand how they might structure it.

So the first one we identified was a hierarchical model. And this is very similar to what, in many ways, DHS has, where they identified 18 different critical infrastructure sectors. They more or less set a schedule of meetings and designed certain bodies and forums for industry and government leaders to meet. In the United Kingdom, there are information exchanges that are generally similar to this, where they identify different infrastructure sectors and there's a set schedule of meetings that goes on and so forth and where information is exchanged.

As far as pros and cons, like any hierarchy, they tend to be rule based. So the one advantage of this type of arrangement is probably that there are usually good rules around sharing information and that can be a benefit. And as far as disadvantage, I would say also like hierarchies in general, they may not always be inclusive of the right parties, or they may not always the information you capture in the activity that goes on is dependent on the structure of the hierarchy. So I mean there are pros and cons there.

We identified what we call a community model, which I think in some ways the North American Electric Reliability Corporation that Phil's going to talk about is a little bit like this. But this is really a model where shared, different firms or different groups with shared interests come together to share information with each other and also with the government.

So a big example of this is the U.K. WARP system, the Warning, Analysis and Reporting Point, where what the government did was they essentially said, “Look, cyber security is a challenge and there are lots of vulnerabilities and threats out there. And what we want to do is create an environment where different groups in the community can exchange information with each other and with the government as they need to. And we don't necessarily want to dictate in this particular arrangement who does that.” So they created rules and regulations surrounding sharing information.

And they also did very simple things, like creating common reporting formats, for example, like common XML spreadsheets and XML reporting formats, to allow organizations to exchange information with the government. And they put those out there for different communities to use really as they saw fit. So if you look at the WARP if you look at the U.K. WARP website there are a number of different communities that have taken advantage of this arrangement. So particular parts of the national health system or healthcare system in the U.K., different geographical communities, and different industrial communities of basically similar firms.

I think a real advantage of it is it's great for outreach and awareness to different, to communities in the nation. Perhaps the disadvantage might be you have less it might not be the best format for sharing sensitive information because it's not really the whole idea is to include different parties, not really to exclude based on security guidelines and regulations. But it's a really interesting way to look at it, and I think that a big advantage is the outreach idea there.

Finally, the last one we thought about was a third, what I'm calling a third party facilitated model. And this is really where there is a separate legal entity that sits between private industry and the government. For instance, I used to work as part of a nonprofit corporation that sat between U.S. federal law enforcement and the banking industry. And the banking industry

shared information with us that they might not have necessarily been willing to share directly with U.S. federal law enforcement.

One of the advantages here can be that it's an extra layer of protection for the information and a neutral venue -- since it's actually a separate legal entity where private industry may feel more comfortable sharing information and having anonymized and distributed by that third party, rather than giving it directly to the government.

The third party may have their own rules and so forth surrounding, again, protecting the information. And frankly, the third party, depending on how well capitalized they are, in other words how much money they have, they may also have some financial responsibility where they can independently take care of any data breaches or deal with any problems that might come from, might come from use of the information. So that can be a real advantage.

The other thing about a third-party model is that the third party may bring some additional added value to the enterprise or to the public-private partnership. So actually, if you think about our own organization, the CERT program and the Software Engineering Institute, we take a lot of information in from private industry that we use in different ways and then we share information with the government.

And we provide a lot of research and analytical ability that might not really be available otherwise to either party. And of course, we also have one of North America's best technical universities right across the street where we can reach out to them. So in many cases, that third party adds value and provides things that neither the government nor industry would really be able to access on their own.

Julia Allen: The thing that I find particularly helpful in your description and the paper and the fact that you've identified organizations that represent each of these models is for someone, for a country or for a consortium or whatever special interest group there is that wants to try and build one of these, they've got real examples to go take a look at, and they can pick and choose the parts of it that work best for them, correct

John Haller: Yes, that's the yes, exactly, that's the idea.

Part 3: NERC - A Successful Public-Private Partnership

Julia Allen: Great. Well Philip, let's get you back on the call here and talk about something perhaps as an actual case in point of many of the foundational principles and practices that we've all been discussing.

So with the Arkansas Electric Cooperative Corporation being part of NERC -- we've mentioned NERC, the North American Electric Reliability Corporation that's clearly, NERC is one example of a very effective public-private partnership. So could you fill our listeners in a little bit about NERC and how it relates to the goals and models we've been talking about?

Philip Huff: Yes, absolutely. And I'll describe how it fits into the community model that John was mentioning. First of all, just some quick background on the North American Electric Reliability Corporation. It has existed since the late 1960s as an industry standard-setting organization. Only recently has it received the statutory responsibility to provide mandatory and enforceable standards across the industry.

So it does participate as a very collaborative community-based organization with the industry. But also, there's that enforceable side, where with a million dollars a day penalty. So it does -- it's a unique tension that exists in that organization.

I serve as vice chair for the standards drafting team for cyber security standards, so I spend a good deal of my time with NERC and have seen how it can effectively participate as and facilitate that public-private partnership.

It's in a good position in terms of its mission being reliability. I think that's a shared goal for both the government and industry to have reliable electric power. So it puts NERC in a good position where reliability is a key factor in both the cyber security threats and vulnerabilities as well as a factor in applying mitigation.

So on one hand, NERC membership is not it's mandatory. It's not voluntary. But on the other hand, participation in that open dialogue is voluntary and open. So there are two sides to NERC from that regard. With regard to how it is able to facilitate that public- private communication, NERC has several information disbursal programs. It participates in several assessments of the industry and it holds calls with those in the industry that are really heavily involved with critical infrastructure protection.

One of the biggest advantages in such a broad industry with over 1900 organizations, it has contacts for each of those organizations with regard to CIP (critical infrastructure protection). And so and the organizations are very interested in participating because they do have those mandatory standards.

And so they're able to reach out and disburse information fairly quickly. And we're also able to provide input through the Information Sharing and Analysis Center which NERC also operates. So there's a lot of ways that NERC contributes to that communication between the government and private sector.

Also, NERC has knowledge of the industry, both with the assessments, with the compliance aspect of seeing how the industry operates, and working with the industry collaboratively on the standards and mitigation. But it also reports to FERC and is very involved with DHS and other programs. So we have a lot of people at NERC that have their feet in both the government and private sectors.

So with regard to how it is able to support that national security strategy, NERC is able to take information from the government and understand that and translate that to mitigation strategies that the industry can participate in and understand and be a part of the solution.

Julia Allen: When there is a major threat or emerging incident that involves the grid and the area of concern that NERC is responsible for, does NERC have a role to play in those kinds of situations?

Philip Huff: Yes, absolutely. First of all, they have alerts that they send and literally within a day, the entire industry can be informed. And we have contacts within the organization that we get that information.

So if there is an emerging threat, we get that information fairly quickly. And there's a back-end regulatory aspect. There's nothing necessarily mandatory. Regulation works a lot slower and for good reason. But that initial mitigation strategy -- we have the tools in place to be able to get that threat quickly to those in the organization that need it.

Julia Allen: Excellent. Well Sam, why don't you do the wrap up for us? Are there some places that you recommend where our listeners can learn more information, either broadly on the topic or specific to the work that we're doing at CERT or the work that Philip is doing at his organization?

Sam Merrell: Sure. I think NERC as an example is a terrific place to start. As Phil said, they are very active in not only taking the strategic direction of the government but operationalizing it for their specific industry. Over and above that, the Department of Homeland Security has a lot of information about information ISACs, Information Sharing Analysis Centers.

And they also have information about their brand new NCCIC, the National Cybersecurity and Communications Integration Center, which is another really positive example of how cyber security public-private partnerships are working. And then over and above that, the CERT website of course has some great information.

Julia Allen: Great. Well Sam, I thank you very much for your time and comments today and for leading this great effort. Thank you.

Sam Merrell: Thank you all very much.

Julia Allen: And John, a pleasure to have you back on the podcast series. And really enjoy learning about all of your outreach internationally. Thank you.

John Haller: Yes. Yes, it was a lot of fun.

Julia Allen: And Philip, great to have you on the call and keeping our work on track with an actual case in point with your work at NERC. Thank you so much.

Philip Huff: Yes thank you, Julia. I appreciate the opportunity.