

Cyber Security for Control System Environments & NERC – an Interview with Joseph Weiss – Critical Infrastructure Security Expert

Listen to the Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Brian Contos: Joining me today is Joseph Weiss. Joe is an industry expert on control systems and electronic security of control systems, with more than 35 years of experience in the energy industry. He has provided testimony before three congressional subcommittees and spent more than 14 years at Electronic Power Research Institute, or EPRI, where he has led a variety of programs. He has published over 60 papers and has two patents on instrumentation and control.

I've actually known Joe for several years now, sometimes even co-chaired panels on cyber security for control systems. I've never met anyone more passionate about today's topic than Joe.

Thanks so much for joining us today Joe.

Joseph Weiss: Thank you very much for asking.

Brian Contos: Now Joe, a few months ago at CSI we were on a panel together and we were talking a little bit about industry. And as part of this call prep we had a few conversations, and I think it's really fascinating. Could you please share with our listening audience some of the things you're working on?

Joseph Weiss: Yeah. There's actually, I think, two things now that you bring up CSI that are of interest to people. The first one is: I am acting in a support capacity to the Nuclear Regulatory Commission that is developing cyber security guidance for the nuclear power plants, to meet the recently passed security rule that I believe became law at the end of December. That effort is ongoing, and it's essentially there to augment (I don't want to use the word replace, but that's close.) the existing nuclear cyber guidance that's effectively the same thing as the NERC CIPs.

The other thing that I wanted to mention is... And this goes back to our discussions back at National Harbor at CSI. One of the discussions there was the fact that we use very, if you will, old cyber-vulnerable equipment that can't be replaced.

And I was just talking to a friend who had a brand new... Actually two people who have just had brand new cyber security upgrades of their very large power plants. Neither of which, by the way, was a NERC critical asset.

Both of these cases... Both of these control systems were just completed last month in December, and both of them already have had cyber incidents. These are the newest

systems we have. These are the systems that the vendors are saying are as secure as possible.

And it's not to say that the systems are, but it's another reason why we need to have something stronger than the NERC CIPs. Because these are some of the more important power plants in North America.

They're not NERC critical assets, which is mind-boggling. And unless you've got an adequate program, knowing what you're doing, even the newest systems can be compromised.

Brian Contos: Well Joe, let me pause you for just one second there. One of the things we've talked about many times in the past is that (And you sort of alluded to this.) a lot of these systems are built atop antiquated operating systems. They might be running NT 4.0 with no patches, people can't patch them. They can't install firewalls or anti-malware because it breaks the service level agreements, it breaks the warranties.

They had specialized TCP/IP stacks that you couldn't even ping without these devices actually falling over, because they were developed in a vacuum, they weren't meant for that.

But I always kind of put that in the bucket of, "Those were the systems old." Let me ask you this: These new systems that they're deploying, is this just the exact same thing? Are they actually still running on these old OSs, and perhaps older databases and applications that just simply can't stand up?

Or is there a new set of vulnerabilities? And the reason I'm asking is: Have we learned from those mistakes over the last decade? Or is it just the same-old same-old?

Joseph Weiss: Well number one, the answer to your first question is E, all of the above. Not only are we, in a sense, replacing some of the older equipment; but even after the upgrades we will still have, in some cases, Windows 95, Windows 97, and NT 4.0 still there after the upgrades because they cannot be replaced. You're trying to overlay a security perspective on running operational systems, and running the operational system comes before any security requirement.

Brian Contos: Of course.

Joseph Weiss: And it turns out that the only way to replace some of these older systems is either to replace or completely rebuild the equipment they're tied to. And in many instances this is just simply either not possible, or certainly not practical. And so we have the pragmatic problem of having to live with things like this. And by the way, this is one of the things the NERC CIP was never meant to address.

Brian Contos: That really brings up a number of interesting points. The first one that comes to my mind is: When we talk about security, we generally talk about CIA: Confidentiality, integrity, and availability. And I think what a lot of people that don't work in the arena have a hard time getting their hands around is: It's the A, it's availability, it's survivability, it's up-time. These are the most critical tenants of most of these organizations.

Joseph Weiss: And it's the availability of the systems and the messaging. I think this is an important point. There are two aspects you worry about. One is, if you will, data in motion. The other is data at rest. Data at rest is really more your databases and long-term things, and CIA is fine there because it's going to be there for a long time. And so encryption and confidentiality etc., makes sense.

But for data in motion, which is what happens with control systems, your signal has come and gone, generally, within milliseconds to no more than maybe a second or two. And it's gone.

Confidentiality of that is reasonably insignificant. What's so significant is integrity and availability, which by the way, dictates what is it we need to be protecting these for. And we need to look differently, because if confidentiality is not number one on the list, then maybe the technologies that people are looking at are not number one on the list.

Brian Contos: So let me ask you this, this is a nice segue into our main conversation which is NERC. But I think that as we start to go down that path, two questions: Do you feel that the power and energy industry itself is taking cyber security seriously today? And do you feel that the vendors providing the control systems and the cyber assets to these organizations are taking security seriously?

Joseph Weiss: Let me, first of all, split out your first question. Because you used the term power and energy. Energy is generally the oil/gas part of the world. The oil/gas part of the world takes this very seriously, all the way up to very senior management, they really do take this seriously. Power does not take this seriously, and I'm sure this is going to get me a lot of arrows in the back. But the bottom line is that if the power industry were to take this seriously, they would not be following the NERC CIPs, they would be following the NIST standards. And they would care about what cyber does to the reliability and availability of their systems.

And they wouldn't have the built-in exclusions in the NERC CIPs, and they wouldn't have the ambiguity that they've intentionally built into these.

Brian Contos: So then, when we look at the other side of the coin, and we look at the vendors supplying, let's say, energy, for example.

Joseph Weiss: OK. The first general part is, a vendor is only going to sell what a customer is willing to buy. If the customer is not willing to buy or spend extra for a secure system, you're not going to get a secure system. But where I wanted to break this into parts was the major suppliers of control systems not only supply the operator interface, they also supply these field devices.

I believe that most every one of the major control-system suppliers has found religion, with respect to security, for their operator interface. In other words, for their Windows-based control, for the DCS or the SCADA.

What I don't believe is that the other parts of these controls organizations that make the field devices; they haven't found that same religion, which is why some of these field devices have wireless modems - what's even worse, Bluetooth - built into the latest of these field technologies.

They're coming from the same parent company, but they're very much different organizations. So, when you ask, have the vendors "found religion" with respect to security, the answer is, yes and no.

But the other point I wanted to make, too, is the security that we're getting is essentially bolted-on security. The basic control-system platforms that we have are very old platforms that were never designed, originally, with security in mind.

So this isn't where we eventually need to go, where you develop a control system from scratch, looking at how do you optimize security and performance.

Brian Contos: So, very simple question. Well, it's loaded. Are we more secure today than a decade ago, or is it an illusion?

Joseph Weiss: Illusion. And the reason was that a decade ago, I mean, when we first started this, when I first started this at EPRI, in 2000, it was essentially errors by omission. We didn't really understand security. It wasn't anybody's fault. I was in the same boat as everybody else. We were building systems to be interoperable, to be efficient, to be able to communicate with everybody else, et cetera, fleet-asset management, you name it. Security was just simply never a design constraint.

Well, with the NERC CIPs, what you've done is you've created, effectively, errors by commission, now. And believe me, if anybody ever has to go to court, they're going to find out about this, in a very big way, because the NERC CIPs, now explicitly exclude things like telecom, like distribution, like non-routable protocols, market systems.

And then the NERC CIPs then go on to say, "Do a risk assessment to determine what is a critical asset."

Well, you've got utilities who are basically using, if you will, deterministic rules, to come up and justify. Because they already have - this is a technical term - "N - 1". In other words, that they can take a failure of their most critical asset, plus one more, and still be able to operate. Well, they're using that.

And, if you will, the deterministic, or mechanical, world - they're assuming that when something fails, it fails all by itself. And it doesn't propagate throughout the system.

So, people are using this approach to eliminate all kinds of really honestly critical systems. We have entire sections of this country where there isn't a single power plant - not even one - that is considered a NERC critical asset, for the NERC CIPs.

So if you're asking: are we more secure? The answer is no, and in fact, I'll tell you what's even worse.

The NERC CIPs were never written for the actual industrial control system, sitting in sub-stations and power plants. The NERC CIPs were really written for modern IP based control center status systems. And what is going to happen - and is already happening - is that we're starting to negatively impact the reliability of the electric system, because of the NERC CIPs.

And there are several ways this is happening. But we're getting close to where the cure's worse than the disease.

Brian Contos: So when you look into your crystal ball, based on all this information on NERC, where is it going? Does it have to be - is it going to be completely rewritten? Is it going to die? Is FERC going to step in and take away the power from NERC? What do you see? What has to happen?

Joseph Weiss: Well, the way I always respond is, I'm 2,415 united miles from Washington. So I use that as my caveat whenever anybody asks me: what is Washington going to do? But what I can tell you is that NERC, as an organization, has not, in any way,

shape, or form, adequately changed to reflect that they are now the Electric Reliability Organization - which is a quasi-governmental agency.

Independent of anything we're talking about the NERC CIPs, NERC has to start acting like what INPO - the Institute for Nuclear Power Operations - does for nuclear power, and be an industry quasi-regulator. INPO is not an ANSI accredited organization - there is no voting on: gee, what do I want, or don't want?

NERC, now that it's the ERO, no longer has any reason whatsoever, period, to be an ANSI accredited organization - they are a quasi-governmental regulator. The people that you regulate don't get to vote. Unless people are turning stone cold blind, what happened to finance?

What people have to realize is, two things have happened. One, we've had an economic meltdown, because of the complete lack of regulation - or trying to let industry be its own self-regulation.

And the other is, you've got a new party in power all the way up through the executive branch, and they are not going to sit by and allow industry - and by the way, this is not just electric, this is going to also be occurring to other industries.

They are going to demand that real regulation and requirements, are in place to secure system, and not have this be, basically complying paperwork which has nothing to do with securing assets.

And the honest truth is, if NERC doesn't get it's act together, (not the utilities but NERC) I believe that you're not going to see critical infrastructure housed under NERC all that much longer.

Brian Contos: If we look at a lot of the other industries, there's a lot of disclosure, you know: This bank got broken into, this happened, or these retailers lost X million of credit card account numbers. There's a lot of information there. But it seems to me that while we're talking about this industry, there isn't a lot of public disclosure. And a lot of people assume that everything is fine. There hasn't been a major security incident, they don't think anything has occurred, but that's not necessarily the case.

Joseph Weiss: You bring up a good point. When I was still at EPRI, I started and became a technical lead of the Y2K embedded systems program. And it's probably the worst thing to say because senior management views cyber as the second coming of Y2K. But the point being: During Y2K people talked, they wanted to talk. And there was voluntary disclosure throughout the whole thing, in fact sometimes way too much.

When we first started the EPRI program, (The EI, the Enterprise Infrastructure Security, the cyber program at EPRI.) the assumption was that there would be, like Y2K in that people would be... You know, it would be an information sharing program.

Well what happened almost immediately is... What you had was each person would nudge their neighbor and say, "[wink-wink nod-nod] I hope my neighbor gets hit, because if my neighbor gets hit, then I can justify doing something."

Well what has happened is... And by the way, this is part of the reason that the ISACs do not work. But what has happened is: People won't share information with the government or each other in this area. I happen to because the people I know, from all over the world, have essentially created an incident database. It wasn't intending to, but I have.

And I've identified... And every one of these I can validate by going back to the people that it happened to directly. I've got over 100 cases where we've had control system cyber incidents, over 100. Like I say, just literally over the past month, two with brand new DCS retrofits.

The impacts range from trivial, (Which I think is what most people expect.) to moderate, to some very significant environmental discharges, to some very significant equipment damage.

You're talking about having to repair or replace large steam-turbine electric rotors; you're talking about 50 to 75 million dollars, again, directly because of cyber incidents; all the way to at least one that's resulted in three deaths.

And again, one of these things that people say is, "Why do we worry about cyber? It's never killed anybody." Guess what? Yes it has. And this is in the United States; this is not Gazprom or something else. This is actually with our critical infrastructure in the U.S.

But the problem is, senior management is not aware of this. In many instances, people within an organization don't even inform their superiors when there has been an incident.

I guess to me, one of the biggest ones is... I know of one incident, the only one I know of where a SCADA system, an electric SCADA, was targeted. I held an annual workshop, and before we finish I want to say something more about that.

But we had a workshop in Idaho Falls back in 2004, and I had a utility speak. This was not hearsay, this was the utility themselves: Their SCADA system was targeted and hit. We're not sure exactly if it was targeted to start with, but they lost SCADA for two weeks.

They did not inform local law enforcement, they did not inform the FBI, and they did not inform the ES-ISAC. And that's where we are.

Brian Contos: Those are incredible stories. And it's amazing that there is all this information out there, there are these devastating situations that have occurred, and it's just not known. And people I think...

Joseph Weiss: It's just not known.

Brian Contos: People are making decisions based on the fact that they don't think this is going on, and I think that's a real problem. We could probably go on for hours and hours, but I did want to give you a chance to sort of summarize everything. I know you have some final comments.

Joseph Weiss: OK, two things: One is a parting thought, and the other is, if you will, a mention of something I'm doing that I wanted to get out. The parting thought is that cyber, number one, doesn't have to be an intentional targeted attack to do real damage. The cyber incident that killed three people was most likely not an intentional event. It still killed three people, injured eight, caused \$45-million in damage, bankrupted a company, took out a water treatment facility, and took out several refineries for a little bit.

That's pretty significant. And it wasn't even, if you will, an intentionally targeted cyber incident, or cyber attack.

So the issue is: Cyber is very important, it can cause very extreme damage. It also is malevolent and can spread across large swathes. The NERC CIPs are simply not adequate,

as they stand, to address this; or provide any (I shouldn't say, "any.") adequate security of the electric system.

Now I wanted to leave with one other point. I mentioned that I hold an annual conference. One of the things that happens, or a couple of things that happen: One is that we actually have demonstrations of hacking control systems.

Not really the HMI, but the controllers themselves. And I think it's really important for people to understand that this is not just a Windows problem or an Internet problem.

The second thing that we do is: I'm often able to get people who've actually had cyber incidents occur to speak about them in a non-public venue. And the next conference is going to be the week of October 19th in the Washington D.C. area. And if people are interested, if they would contact me, that would be wonderful.

So with that, I wanted to thank you very much for allowing me to speak my mind, and also provide where I think we really do need to be going.

Brian Contos: Well Joe, I've known you for a while now, and you're probably the most passionate person on the subject that I've ever spoken to. So I'm glad you could come by today. I think this is extremely valuable information for not only anybody interested in NERC, but the industry as a whole. I think it was really fascinating stuff, and I think our listeners will really enjoy hearing what you have to say.

Joseph Weiss: Thank you.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200