Saving Money and Effort Automating Compliance Podcast Transcript

June 5, 2023

With Andrew Ginter from Waterfall and Kathryn Wagner from AssurX

Andrew Ginter: Hello Kathryn, and welcome to the podcast. Before we get started, can I ask you to say a few words about yourself and about the good work that you're doing at AssurX?

Kathryn Wagner: Yeah, good morning, Andrew I'm very happy to be here. I am Kathryn Wagner, Vice President of Industry Solutions for Energy and Utilities at AssurX. I have a background in engineering and also software development and management.

I have nearly thirty years of experience with systems integration and compliance in a bunch of industries including manufacturing, and now it's mostly energy. For the last eleven years, I've been with AssurX helping our customers implement solutions for NERC and other quality and compliance related requirements. While being a product manager for our NERC compliance and related systems that focus on reliability and resilience, I also help guide the strategic vision and seek expansion opportunities into other regulated industries within the energy sector or even other critical infrastructure sectors. And no doubt, AssurX has been a leader in quality and compliance management systems for over twenty years. We operate in highly regulated industries such as energy and utilities, which is my part of it. So, pharma and biotech medical devices, manufacturing and food and beverage. And those are things I don't really deal with all the time, but our company does.

Andrew Ginter: So, thanks for that. We're going to be talking about compliance management in just a minute, but I understand that you folks got started years ago in the space of quality management. Are the two fields related?

Kathryn Wagner: Yeah, Andrew. They're a natural evolution from one to the other so quality management involves things like managing documents, processes, procedures, issues, non-conformances, CAPA, which are corrective and preventive actions, audits, suppliers, customers, changes, risk, workflows, approvals. So, all those things to meet regulatory obligations and optimize quality. So, compliance management has similar elements but with a different language. That's the way I like to think about it. For example, in the quality space, manufacturers must manage their suppliers. They have supplier risk assessments, contracts, contacts, what parts they supply, communications with those suppliers. And in the utility world, we must manage vendors so that requirements defined in CIP13 (supply chain risk management), but it includes things like vendor risk assessments, vendor contacts, vendor contracts, so the hardware, software, and service that that vendor supplies and vendor communications. So, it's a different terminology but very much the same.

Andrew Ginter: So that makes sense, and this brings us to our topic which is compliance management. I mean I was introduced to the idea of compliance and

compliance management with NERC CIP back in the day and of course you're in the electric sector you know much more about this than I do, can you talk a bit about NERC CIP. You mean you read NERC CIP and it on the surface. It looks like any other security standard. What is compliance in the NERC CIP context? How does this work?

Kathryn Wagner: Okay, Andrew so NERC CIP is all about cybersecurity. It's cybersecurity as it relates to, energy folks. So that is making sure that you have controls so that your power facility or your substations and your control centers so that they're all secure so they're not going to get hacked so that the grid stays up ultimately. And it really involves protecting the people, processes, assets, and data that keep the grid running and the NERC CIP is really about the cybersecurity but compliance with the NERC CIP is what happens when the auditors show up.

You've got to be able to produce all the data and evidence that those auditors want as it relates to those CIP standards. So that involves this thing called the ERT. So, it's evidence request tool the auditors over recent years they've produce the spreadsheet so that everybody reports in the same way. So, it makes it easier both on the regulators and on the entities that are being in compliance. So that evidence request tool people spend hours and hours filling it out. It comes in two parts. So, the first part is a bunch of lists of data. So, they list out their sites. They list out the cyber assets at those sites, they list out all the people interacting with that, who has access to those things, and then a couple other parameters. Physical security parameters, electronic security parameters, data storage locations, vendors and other things. But all that data is supplied in lists in the first part of the audit, and then the next thing that they do is the auditors pick sample sets from those lists, and then they request more data.

So, they have at least 75 different reports that they ask for which is very detailed data on every single requirement that's in the NERC CIP standards. So, some examples of those: Like, was this location commissioned or decommissioned during the audit period? They might want to know all the access authorization records for a set of individuals; all security patches that were released, evaluated, applied for set of assets; evidence that the full configuration change process was followed for any kind of installation; evidence that incidents, cybersecurity incidents, that the response plan was followed for each incident that they asked you about. So all this data is very challenging to organize. It's not trivial at all to pick out this data. I've heard some horror stories from our customers – it takes weeks and weeks of pulling data from different systems. You know, the learning management system, the HR system, the asset management system. Pulling all this data and then they have to manually cross-reference it and reformat it so that it fits in the ERT so that the auditors are happy.

Nathaniel Nelson: Andrew I got not only bored but a little bit vexed just like listening to that answer and all the steps involved all the files all the – you know it's a lot is everything that Kathryn just described really like all the bureaucracy, the documentation necessary. And it kind of makes sense that we're now talking about this in the context of maybe automating some of these processes.

Andrew Ginter: As far as I know it is necessary, I've heard countless complaints about the amount of paperwork involved in NERC CIP and I mean I struggled just when I heard or describe the spreadsheet much less the other 75 documents that have to go along with it. I have a little personal experience very recently with spreadsheets we were doing the annual Waterfall threat report. I needed to put a spreadsheet together, my colleagues and I, of really only like 100 incidents, security incidents, with a dozen columns and it took just forever to get that one rotten little spreadsheet organized and here in the NERC CIP spreadsheet, we're not talking a hundred rows. We're talking more than like several thousand if you have 700 substations and you know how many computers and network devices have you got in each substation. That's a lot of data to be to be dealing with in a spreadsheet much less the other stuff. So yeah, it's – you know – I'm feeling the pain here.

Andrew Ginter: Okay, so there's a lot of data and it makes sense. When you're dealing with large amounts of data makes sense to automate that process. But can I ask you sort of a subtlety here. The people who are looking at automation for compliance, is the main motivation here saving money, reducing the cost of gathering all the data or is there something else that work? Does the machine – would a machine gathering of the data sort of do a more thorough job and, and I don't know, reduce your compliance risk somehow? The risk of an auditor saying you have missing data?

Kathryn Wagner: Absolutely companies want to save money and that is a huge motivator but there's a bunch of different aspects to that. The first aspect is kind of obvious they want to avoid regulatory penalties, and I think everybody knows that NERC CIP noncompliance can cause fines of up to $1,000,000 per day, per violation. So that's a lot of money and there has been some examples in the past. There was one entity that got charged something like $10,000,0000 for cyber security noncompliance. The second motivation is really, what is the cost of poor cybersecurity and that really says if you're not secure, then the hackers can get in. And those hackers cost money whether it's ransomware or they start controlling your equipment like they did over in the Ukraine a couple years ago, they can cause damages which of course costs money to go and fix that up. But not just the fixing the problem that those hackers caused but also it damages the utilities' reputation and that's a really subtle cost. It's hard to put a finger on a number but it's out there. The last thing that affects the cost and why we want to do some of these better management of compliance is a desire to reduce workload and improve efficiency. Without a good program, people spent hours and hours preparing for audits and then doing compliance tasks.

I've heard over and over again, over the years, how their users hate doing compliance. They don't want to do it. They save it to the last minute. For the compliance teams, it's hard to force them to do that work. If you get a system in place, then you make it minimal impact as a means, and then the compliance team has everything in a central location. I've heard that there's been incredible savings preparing for audits because of having a good program. So there's the three different ways that I feel that utilities are saving money with a program avoiding regulatory penalties, having good cyber security, and then reducing the workload of their employees.

Andrew Ginter: Okay, so automation makes sense. You know…saves money makes the job more thorough, makes us more secure, actually, but it's one thing to wave a magic wand and say let's automate the whole thing. It's another thing to actually do it. What does this automation actually look like? How does it feel to use it?

Kathryn Wagner: Well Andrew the real goal is to make sure that you stay in compliance year-round. Not just waiting until the audit to go find out if you were in compliance or not. You need to be able to prove it at any point in time on short notice and that's why people use compliance management software. Now any good compliance management software is going to include features for managing the compliance data and protecting it so that the right people get access to it and the wrong people stay out. Tracking responsibility, knowing who's responsible for what tasks, for what regulations, and then documenting that. Managing documentation and evidence managing risk, issue tracking, incident tracking, and then the mitigation plans or corrective action plans to resolve those issues, task management, and especially important is the notifications, reminders, and escalations. So, if those tasks, those compliance tasks are not getting done or not getting logged into the system that people are reminded and people are aware and there's visibility to those tasks so that they do get done on time. Audit reporting is the output of the compliance management system when you're dealing with NERC you know there's two pieces of it. There's the CIP evidence request tool that I talked about earlier for all that CIP data. But then there's also the management of the RSAWs, which is the older. So, the other NERC standards have to do these RSAWs. They're reliability standard audit worksheets and they're really filling in a narrative and listing out the evidence that they've collected to meet that requirement and those are time consuming so software will help pull that data together. And help you report on it when it's necessary.

Andrew Ginter: Okay, so there's a lot of stuff that needs automation. But how do you actually do the automation I mean these records...do you pull them from I don't know the brains of the PLCs or do you know? What does automation actually do in terms of gathering and organizing the data for you?

Kathryn Wagner: Ah, well there's a lot of different ways that automation can help you and there's a lot of different forms that that can take, so let's look at an example. Okay, so for one of the requirements says that you have to verify at least once every calendar quarter that the individuals with active electronic access or unescorted physical access have authorization records. So you're comparing what they have access to, based on access lists, to you know what they've been authorized to do. So that might really involve two different systems while many different systems because they have access it to many different networks or OT devices or IT devices and so on and the access card system to get in the different areas of the plant. So can set up the automation to help with that in a couple different ways. So, one of those is a very manual way if you set up some sort of a scheduled task that once a quarter somebody is going to be required to remember to go out and pull the asset list manually from the devices. And then pull the authorization information from that system and then manually compare those two lists

together and look for any anomalies. So that's awfully manual, but it is automated because they're automating that task every quarter. You could also set up something that you have a quarterly task initiated, but it uses integration to automatically pull that data from the various networks and other software out there or the devices themselves to get those asset lists and automatically pull the data from, whatever is tracking the authorization records. And then either you could have a person do the comparison between the two now that they've automatically got the information or maybe you're clever enough to put together some sort of computer program to do the comparison and perform that validation automatically as well.

The last good example I have setting up automation to help you out is setting up a daily feed or daily pulling of information from those other sources, pulling it into the compliance management software so that you always have the ability to report on or see the two different things and make that validation. And you could even go further than that and set up controls so that the system can detect some discrepancy between the two and it can alert on it, send out emails, or show it up on a dashboard or even initiate other tasks and workflows to get that accomplished. So that's a good example of a couple different ways that you can do automation within the NERC CIP environment, and I have a list of examples here things like polling the network for asset list and open ports, querying assets for baseline information, connecting to an HR system to get your up-to-date employee information, on the learning management system to get your training information, patch discovery services to obtain patch information, and then things like scheduling document review when evidence collection and tasks, so a number of different ways to leverage automation.

Nathaniel Nelson: So, Andrew it sounds like luckily a lot of this long and arduous process can be automated but is there anything outside of the scope here like what do you still really need to do by hand?

Andrew Ginter: That's a good question. There's a couple of answers to it in terms of what's possible today and what could be possible in the future. Let's take, just a simple rule. There's a requirement to change passwords every I don't know twelve months or eighteen months or something like this. And if a PLC even has a password, but network switches have passwords, firewalls have passwords, a lot of gear nowadays has passwords. May not be per user, maybe be shared, but still a password is a password and if it exists in the CIP world, it has to be changed periodically. It's one thing to ask the question of the device. Do you have a password? Who's got accounts? The accounts list on the device, that that's sort of a more common feature of devices that you're able to figure that out, but trying to figure out when did the password change? I mean does the device even keep track of when the password changed the last time? Is that even something you can ask the device? So, some of the data can, is some of the data is there, some of the data you just have to keep track of manually, you got to make a note in your, you know, compliance tool or something saying, I change the password because the device can't tell you when things happened, when was the last patch applied. You might be able to ask the device which patches are applied but can you ask it *when* they were applied? So, that's a long way of saying you know some of it you can

automate, some of it you have to keep track of yourself in your system. You can either keep track of it on a sticky note or you can keep track of it in a software system. But down the road it seems to me that all of this stuff can be automated in the long run. Now you might need the cooperation of the device vendors. You might need to upgrade the versions in the device vendors. It seems to me there's sort of nearly infinite opportunity to like innovate and create new software to simplify this process here and it strikes me that over time you're going to see more and more of that happen. Because there's just so much money being spent by the electric utilities on this compliance task. And if they're spending the money doing it manually, they are open to spending less money getting it automated and spending more money on automation. On newer versions of devices that keep track of some of this stuff automatically, newer versions of automation tools that can pull the data from devices. So it sounds to me like it's an area that's sort of ripe for innovation.

Andrew Ginter: So That's a lot of stuff that that a compliance manager could do and you folks produce these products. You produce and sell a compliance manager for NERC CIP among others. Can you talk about sort of not just what does your stuff do? But in a sense how does it do it? I mean if I say yes I'll take three of the assurance things. What am I buying are seats in the Cloud or agents that snuggle up to the PLCs to gather data. What does your system look like?

Kathryn Wagner: Yeah, so AssurX software, we do have cloud options and on-premise options. I will say that most of the NERC entities that use our software have it on-premise due to the sensitive nature of the data that they're trying to manage and it is probably a little bit easier to secure the integration with those third party devices and so on and other software if you're all on-premise. So, what does it look like? So, we have a user interface which is browser-based and behind there, there's a database and a server. You can configure those in all different architectures so that you have load balancing and failover and all sorts of things. We typically have things like a development environment, a testing environment, and a production environment and our software. Yeah, we have the AssurX platform which has all the features to create solutions, any solutions whether they're energy solutions or life sciences manufacturing solutions that platform gives you the ability to create unlimited dashboards and forms but has the security, it has the database layer, and it does all the code, or has all the code in it. Everything that you do with the AssurX is point and click, drag and drop, easily configurable, etc., and then we use those features on our platform to create the whole suite of these NERC compliance management solutions. So, we call that ECOS, an AssurX Energy Compliance System.

And that is a full suite of solutions that does both the OP NERC compliance management and the CIP compliance management and then it can be extended to do a bunch of other things as well. So what our customers do is they install, they get the platform installed, then they load up our solutions. Some of them focus in one area, some of them focus in a different area. We provide all of them, and then the customers configure our system. AssureX is highly configurable, and they adapt the forms and the workflows to meet their needs. Okay, so and that's where you can do all of it without

integration – a human is interacting with things tasks are assigned to humans to go and do things, or you can start plugging in that integration to pull the data and interact with all the third party software. So that ECOS solution is focused on NERC compliance and other compliance management aspects, and I do want to say that we're expanding our offerings. So not only to do with NERC CIP but things like the TSA pipeline security directives. A lot of our customers are energy customers, but they also do gas and that makes the gas pipeline very applicable. And those TSA regulations are similar enough to the NERC CIP regulations that our existing solutions can be easily adapted to meet those needs.

Nathaniel Nelson: In this episode we're talking about Kathryn's specialties in energy. We talk about NERC CIP but what about other industries, Andrew?

Andrew Ginter: Yeah, you might imagine that NERC CIP is what 12 or 15 documents by now with a lot of detail in them. You might imagine that if you have sort of a compliance system set up for NERC CIP, you could use the same system for other industries because if you've already got 15 standards in the NERC package is that not everything you might need for everyone and the answer is no.

I mean the TSA, you know like six weeks after the Colonial incident came out with a new security directive for pipelines, and it was only, I don't know it was as long as one or two of the 15 NERC standards put together. So it was like only a fraction of NERC CIP, but still it covered different stuff. Concrete example -- it talked about dependencies. It said if your OT system depends on your IT system, then you have to get rid of those dependencies and if you can't get rid of them, you have to document them, you have to report them to the TSA. Because every one of those dependencies means that if you cripple the IT network and you cripple the systems that OT depends upon, then you've crippled the OT system because the OT system needs the crippled IT systems to work. None of those words exist in NERC CIP, this is sort of a new concept. In the TSA, yeah in spite of the NERC CIP documents being much bigger than the TSA document.

Nathaniel Nelson: That might beg the question. if we have these characteristically different regulatory needs and standards and what not. Are they equally or more or less automatable? You know like for talking about power versus water treatment or whatever, would Kathryn's kind of approach work in the equivalent way elsewhere.

Andrew Ginter: And that's a good question and in fact I asked Kathryn that question so let's so let's go back to her and see what she says.

Andrew Ginter: And you did mention the TSA directive and I mean I've been looking at the TSA directives over the last several weeks. They seem very different from NERC CIP. I mean they're structured differently. You know the TSA directive has for instance, a section in the requirements that says "your goal as a pipeline operator is to keep the pipeline running at necessary capacity even if the IT network is crippled" and they don't define necessary. I assume it means necessary to the business or necessary to the

society. A lot of these pipelines are critical infrastructure. you don't have to keep it running at full capacity have necessary capacity I'm going, how can you audit against that? But I look at the thing and it has that's sort of a high-level requirement and then it's got a bunch of much more specific requirements that seem sort of much more auditable. Can you talk about? This seems like a fairly different animal from NERC CIP. Can you talk about what can you track in that space.

Kathryn Wagner: Well Andrew I want to say that we're not trying to control the OT nor the IT network or any of the devices that operate on it. We're really focused on pulling in and gathering that data that we're going to need for compliance purposes, and we also are able to coordinate activities that may result from. The interruption to the network or even just some changes to the network like firmware updates and security patches and access changes so on among other things. The TSA security directive mandates that you must have a cybersecurity incident response plan. Okay? This is very similar to CIP 8 which is the cybersecurity incident reporting and response planning. So same idea…you have to have a plan for dealing with things. Both of them require an update up to date documented plan for responding to cybersecurity incidents that includes the procedures for what needs to happen. But it also includes the roles and responsibilities of all the people that are going to be dealing with those incidents and then of course notifications to whoever needs to be notified after the incident.

And then it says within ninety days you must document the lessons learned from the instant and then update the plan accordingly making sure that each person who has a role in the plan is notified of those updates.

Andrew Ginter: Well, thank you Kathryn this is this has been great before we let you go can you sum up for us, I mean what's the most important thing to remember about the yeah the world of compliance automation.

Kathryn Wagner: Well compliance automation especially with cybersecurity things like NERC CIP. It's challenging. There's a ton of data to coordinate. There's a ton of people to coordinate and it makes sense to automate those tasks and gathering up that data anytime you can take the human element out of it you're improving things. So we do, of course, have the software to help you with that if you'd like we also have experienced people. You know we've worked in a lot of different industries to help with quality and compliance. So please reach out to us our website, of course is www.assurx.com and then you can always reach out to me on LinkedIn if you want, I'd love to hear from people, and talk about how we can help solve your problems. So, thank you Andrew for having me here today on your podcast I really enjoyed it. It's been a lot of fun.