**RedZone Podcast Episode #74: Critical Infrastructure Protection – with Jim Linn, Managing IT Director of American Gas Association**

Bill: Well Jim, I want to welcome you to the show today.

Jim: Thank you, Bill.

Bill:

[00:00:30] Let's dive in a little. You and I had a sidebar before we got started, and I think it's an interesting one to have a conversation about. I don't think I've talked about this before. So being as you and I are in the IT space, you as the managing director information technology with American Gas Association. Would that be the equivalent to the CIO in a commercial setting?

Jim: Yeah, I'd be a CIO equivalent. I'm the highest ranking IT person here.

Bill: Excellent, excellent. One of the things we talked about was you and I both have kids that are growing up and helping, at least, doing best we can to guide their careers, and I was sharing with you a story that I heard about Mike Rowe who is the guy that ran many seasons with ... What was it? Jobs-

Jim: Dirty Jobs.

[00:01:00]
Bill:

[00:01:30]
Dirty Jobs, yeah, and now I guess he's running a foundation. I think it's called the Mike Rowe Foundation, but it's a very ... I think all of the major players like Caterpillar and Ford, and they run a lot of jobs through him, because hundreds of thousands of jobs are available to kids these days that they're actually computer ... They're basically computer technician jobs in many respects. Do you think we value that type of career path these days?

Jim: I think our study's gone beyond. I think we value white collar jobs. I think that there's a perception that, in many cases, there's a need for a lot of education, and a job in an office, and traditional hands-on jobs [inaudible 00:01:47] trades are just not as value as they used to be.

Bill: Yeah.

Jim:
[00:02:00]

[00:02:30] It's unfortunate. There are tremendous opportunities. There's even a lot of opportunities within the industry that I work in for hands-on trade jobs and even crossover jobs between trades with some technical knowledge. So if you take someone who would be well-skilled with running gas pipes, gas pipe controls, pumps, valves, it takes a real expert in that to then transition to someone who can protect that. Because all of it is electronically controlled now, it's not like -- if you go back to the car analogy -- a simple engine.

Today, if you have your car hood, it's not just a simple engine, it's a simple engine and all sorts of computer components and sensors. The same thing's true for all the critical infrastructure. The guts are still there, but it's all computer controlled.

Bill: Do you find that is there, not necessarily a crisis, but is there a challenge in upleveling these skills of some of the older workers and attracting new talent?

[00:03:00]
Jim:
Attracting new talent's been interesting. The last few years, energy has become more popular, so that's been helpful. But getting enough folks that are able to do cyber that have some knowledge of infrastructure itself is not easy.

[00:03:30] We have been grateful in many respects to see folks transition in from military backgrounds. There's many folks in those positions that tend to know the tangible and security on top of that.

Bill:

[00:04:00] Oh, interesting. Yeah, I think it's really quite interesting because the ... I might have shared the story with my audience prior, but for those that are listening for the first time, it was interesting. My son was on a soccer team and I was friendly with one of the kids that is just in community college and he come up and he said he just dropped out of community college.

He's Hispanic, and I said -- not that that's a big deal, but I had also known most of the kids on his team were like, their parents had immigrated or jumped the river or their kids were their way out -- "Why are you leaving community college?" Good kid, and he had been recruited for soccer and he'd gotten hurt and nobody really cared.

[00:04:30] He wasn't really on the academic path and he goes, "Well, I'm just gonna work at Walmart and make some cash, make some money, and go to school part-time." I said, "That's interesting. You're gonna work 50 hours on your feet at Walmart and then you're gonna go to school part-time." And I said, "Manuel, you're never gonna do that." I said, "What do you like to do?" And he said, "Well, I like working with my hands."

[00:05:00] I said, "Okay." I said, "That's a starting point." I said, "What about apprenticing?" And I pulled out my phone -- literally on the sideline -- pulled up my phone, we started looking at plumbers, electricians, and I said, "Manuel, do you see here it says that you can make 50 grand, 70 grand with a certain certification. 100 grand with an advance certification, and 120 -- and that doesn't even count if you end up running a business."

Jim: Right.

Bill: And I said, "You know what kids are making out of college these days?" I said, "They're starting out at 50. Or 60." I said, "And you go out ..."

And he goes, "Man, that's a really interesting idea." He goes, "My mom is an electrician."

[00:05:30]
Jim:
Oh, my.

Bill: I said, "Well, go talk to her boss. Or go talk to your mom." Sure enough, he's apprenticing. I said, "Now you're apprenticing at $15 an hour. You're learning a trade and you're gonna come out making 50, 60, 70."

[00:06:00] So it's just interesting. It's a different pathway, but I find that very interesting to know some of these that are options that kids come out debt free, they have a huge skill, and if they pivoted later on in their life, so? They have a huge skill and they can go pivot and go back to school.

Jim: Right. That's a tangible skill you can always use.

Bill: Yeah.

Jim: Even if it's just in your own house.

Bill: So in the gas industry, what are some of the big challenges that you guys are facing right now as a critical infrastructure industry?

Jim:
[00:06:30] Well, the area that my team has been brought together on is cyber security. There are five of us but I provide most of the information technology subject matter expertise of the team. We also have a legislative person. Someone that ... Also a threat analyst for ISAC. We have two folks that handle more of the operations end of it. One would be the primary US government and liaison person and policy person.

[00:07:00] We have cobbled this team together over the last five years to really help our industry embrace the reality that we're being attacked on a minute by minute, second by second basis from all over the world. That's a real challenge, and it's true not just for our industry. It'd be true for any critical infrastructure sector. I just happen to be in the natural gas distribution industry.

[00:07:30] But we're eagerly trying to do everything we can to provide information sharing and whatever knowledge and safeguards to serve our members. We've also found as we've been pursuing the sharing of cybersecurity information that, given the attention in recent months and years on pipelines and concerns about locations of pipelines, there've been ample physical disturbances to report on, too.

[00:08:00] So if it would be a protest in a certain area, we become aware of those events as well and share that with our membership and it's been an interesting mix of sharing both cyber information and physical information to try to keep everything safe, secure, and the gas flowing.

Bill:
[00:08:30] What does it mean, the word "sharing"? Just to dispel the ... Because I think part of the people listening are, "What does an ISAC do and what does it mean to share information?"

Jim:

[00:09:00] That's a very good question. Many folks would be unfamiliar with the concept of ISAC -- Information Sharing and Analysis Center. Most of the critical infrastructure sectors have one. What we do is obtain information from a variety of sources -- many of them US government sources -- and they would be from familiar agencies. In our case, Department of Energy, Department of Homeland Security, FBI, others.

We not only receive that information, but in the name when it says analysis, we're looking for connection points and trying to not just pass information from one point to another point -- although we do some of that -- but we're also providing context.

[00:09:30] I'll flesh it out a little bit more. On a daily basis, we may get dozens of alerts from those US government agencies, typically by e-mail. We will reformat them and post them to a secure portal where participants in the ISAC have access. And they're alerted by e-mail when there's a new posting in the portal.

[00:10:00]

[00:10:30] That's one type of sharing that we do. It's from outside sources with or without some analysis to our participants. The other thing that happens within the context of the portal is participants share with each other. That's not always an easy thing to achieve. Our ISAC is roughly three years old and in the three years' time, we are at a point today where roughly 15% of our information shared is from participant to participant. Which does not sound like a lot, but for our level of maturity, it's huge. It's really huge.

Bill: And they are doing that via e-mail between each other?

Jim: They're doing that with secure postings with portal.

Bill: Okay.

Jim:

[00:11:00] And then an e-mail alert when something's been posted. They're sharing with each other indicators of threat activity. So if they're seeing their networks being probed from certain sources, they're sharing with their colleagues what the probes are, where they're coming from, what they look like so that their colleagues, if they may not be seeing them today, they are tomorrow or later today and they can be prepared for them.

Bill: So how are you ... When you say probe, would this be of the top 300 tools that are basically you're looking for compromise different sets of tools in the protocols that they will reside on? Is that essentially ... Are you looking for inbound activity?

[00:11:30]
Jim:
We are. We'll often see inbound internet activity towards our networks.

Bill: Okay.

Jim: Just looking for where a foothold might be able to be developed.

Bill:
[00:12:00] What about the controller systems? The more legacy-oriented systems that have been built by seamens and other large industrial-controlled companies through the years and that are embedded in ... I'm assuming they're embedded into the gas industry?

Jim: Sure.

Bill: How do you handle those type of challenges?

Jim:
[00:12:30] Many of the older systems are built to connect through older computers, and many have been running for long periods of time. It's difficult to do upgrades. When you think of this business, the first two tenants of the business are to keep everyone safe and to keep the gas flowing.

[00:13:00] When you think of doing upgrades to industrial controls -- and industrial controls could change valve positions or pumps or other items that would adjust the flow of gas -- by nature you're looking at potentially taking some piece of your system offline. You need to do it safely. That's a significant process. You don't just do that all the time, every day. You have to schedule it well in advance, plus it's gotta be well-planned.

[00:13:30] So, it takes a long time to do those upgrades. Because of that, there are components that are known to have vulnerabilities in them that still exist. What we've done as an industry is build a number of security layers around them so that if there are known vulnerabilities, there are other tools -- firewalls, et cetera -- that cover them to prevent people from dealing with the vulnerabilities. They can't get to those vulnerabilities if there's a good firewall in place.

Bill:
[00:14:00] So you're going to basically create intro walls. Basically internal ... You're gonna internally firewall and cordon off those systems in to their own little playground so you can really examine them closely.

Jim: Right. And we subdivide just about as much as we possibly can for that purpose.

Bill: Okay. Based on risk that this compromised system would have in the event of a take down?

Jim: Right.

Bill: Okay.

Jim:
[00:14:30] That's really how everything's been managed. It's just a big risk equation, and every component, every part of every component, has a risk factor associated with it. The items with the highest risk have the most attention and investment spent on them. Items with the least risk would have the least attention and investment spent.

Bill: Is there a framework that you're finding that a lot of your members find very useful as far as a lens that they try to map to from their infrastructure?

[00:15:00]
Jim:
Sure. I think that the few tools that people tend to use the most -- and this would go beyond the framework, but -- they're a set of TSA pipeline security guidelines that we use that's both cyber and physical. There's also the NIST framework that has been developed. We use that extensively. And there's a cybersecurity capability and maturity model developed by Department of Energy that we use.

[00:15:30] We use all three of those. Different companies may spend more time focusing on one over another perhaps, but all three of those are heavily used. And other things. There's numerous different things that people can use. Those would be maybe the top three I would think of.

Bill:
[00:16:00] If the ISAC ... So when you're pulling information, is mostly right now the ISAC will receive information from essentially the bigger agencies. The FBI, Department of Homeland Defense and others.

Jim: Yeah.

Bill: Is the sharing ... You're taking the inbound e-mails, you're scrubbing those e-mails and then posting them to your portal. That's how that's working right now?

Jim: Right. On a daily basis there are numerous of those e-mails.

Bill: Okay.

[00:16:30]
Jim:
We also take feeds from US-CERT -- Computer Emergency Response Team -- ICS-CERT, others. Not everything that we receive do we feel is directly pertinent to our members. One ...

Bill: The context you're referring to is context for the appropriateness for your members?

Jim: Exactly, yeah. The one thing that is somewhat of a benefit, most of the larger companies that are members of ours are getting those feeds directly themselves because they've already got those relationships with the government entities.

[00:17:00] Some of the medium to smaller-size companies may not, and if they don't, if they're part of the ISAC -- which all of them are at this point -- they're getting from us the alerts that are probably the most pertinent to them, and we're filtering out ones that may not be as pertinent to them.

[00:17:30] Not every industrial control system alert is specifically [inaudible 00:17:25] the gas industry. There's countless industrial controls. Some are used more in other industries. Maybe electric, it may be healthcare, it could be manufacturing. We're looking for the ones that are specifically geared towards the natural gas industry.

Bill:

[00:18:00] Okay. Now, as far as where you think ... If we're having this conversation three years from now in the future, what would you say the ... Where would you see the maturity being from the ISAC that you run? Where -- in the ISAC as an industry as well -- where do you think things are gonna morph to as far as how your members will be able to take action from the information that's provided by you?

Jim:

[00:18:30] Right. I think there's a few things that we'll see in three years. The 15% of member to member sharing has grown exponentially over the last three years. I see that continuing to grow. So I see more members sharing information with members. The information they're sharing amongst themselves is far more valuable than the information that they'd be getting through the government -- not that there isn't value there, there clearly is -- but the things they're actually seeing on their networks are gonna be able to help each other on a moment by moment basis.

[00:19:00]

[00:19:30] So I see that significantly increasing. The other thing that I see that there would be a transition, just in the recent last few weeks we've arranged a much closer relationship with the electric ISAC where our threat analyst spends two days a week on their watch floor. They're a much more mature ISAC than we are. They've been in existence for many years, so our analyst has much to learn from them but they also get the benefit of seeing his first-hand knowledge of natural gas and how that feeds in to the electric power industry. Which is a significant fuel for electric generation.

[00:20:00] We're sharing information almost immediately between gas and electric. I think in ... I'm not sure that I'd put a time frame on it. Maybe three years, maybe more than that. I think we'll see a melding of parts of the energy sector so that it's not portioned off to different players, but they're all working together in perhaps one energy ISAC.

But there's still a number of things to put in place before that happens.

Bill: Is it mostly political or technological?

Jim: I'd say it'd be mostly ... I don't want to use the word political. You could use that word. I think it's administrative.

Bill: Administrative? Okay.

Jim: Yeah. I think it's administrative.

[00:20:30]
Bill:
So if you had the ability to take these feeds and adjust them in to the equipment and the hardware and the software itself, would that be something that you would say is a part of the roadmap, is being able to take actionable information from the government and adjust it in to your equipment without a human being involved?

Jim: Yeah. Just last year the Department of Homeland Security initiated an Automated Indicator Sharing program. There's also ...

Bill: What's it called?

[00:21:00]
Jim:
Automated Indicator Sharing. AIS.

Bill: Okay.

Jim:

[00:21:30] There's been a somewhat legacy similar program in the electric-utility space called CRISP, that's a Department of Energy initiative. I do see more and more Automated Indicator Sharing. The indicators ... If you participate in the AIS program, they come through the Department of Homeland Security. They're shared by ... I don't recall the last statistic of the number of participants.

I believe hundreds of companies participate. Companies and agencies participate. I think there's gonna be more and more of that. We need to make sure that there's really solid vetting of who's participating, because you don't want to take indicators from a source that would be questionable.

[00:22:00] There's still some work to be done on that, but the regular sharing of machine to machine information, that's what's gonna keep things really safe. Because if, for instance, one firewall sees bad things coming their way and it can automatically report that in machine time to hundreds of thousands of other firewalls, that's security.

Bill:
[00:22:30] Yeah. I wanted to ask that because I really do see security evolving into really a biological model where our body doesn't have to think about the infection, it just deploys. And it's nine times out of 10 successful, and when it's not, you get sick or you die.

Jim: Right.

Bill: But it's very automated.

Jim: Yes, yeah.

Bill:

[00:23:00] And I'm thinking that even in the natural ecosystems around us, if there's a threat to a pond, there's natural algaes and bacteria and such that get deployed. Some animals die, but then the ecosystem takes over. It's an interesting model that I'm thinking that that information sharing would probably have to transform.

Jim: Right, and I think that there's always gonna be a place for both. Both automated and also analyst-based because it's difficult in the automated to have that same context, and I think that there's an analyst role where a human can see trends.

[00:23:30] Computers see trends, too. I don't believe that we're at the same place that we are with humans being able to see trends, if they've had the right level of experience in whatever it is. I think that's the one thing with our industry, and it's true of other industries, too.

[00:24:00] When people operate large systems, whether it's a gas control system or manufacturing system or electric power grid, the people that have done this for decades have enough years of observing the system. They just know when it's right and they know when it's wrong, and when you bolt that on to indicators, then you have good information.

Bill: Sure. Yeah, that's ... As humans, we have that pattern recognition built in pre-wired in to our brains from being able to hear the rustling bushes before the tiger jumps.

Jim: Exactly.

Bill:
[00:24:30] You've got somebody that's been 20 years in the gas industry, they're certainly gonna have that pattern recognition. I almost think that the machine learning algorithms are gonna be ... I look at them as software robots assisting a human analyst.

Jim: Yes, yes.

Bill: Because who's better qualified to find the needle in the haystack of zeros and ones and bits and bites than just an automated robot?

Jim: Yeah.

Bill: So it's interesting you may see the industry evolving to that capability.

[00:25:00]
Jim:
Mm-hmm (affirmative). Yeah, that's definitely ... That's where things are headed. There's been more and more emphasis on automated sharing.

Bill:

[00:25:30] Where do you ... I had this conversation with the [inaudible 00:25:10] to Chief Information Security Officer who participates a lot with the product development and there's a couple Silicon Valley-based firewall companies that are -- this is a year ago when I interviewed him, but I'm sure it's even more, now -- where the CEOs have agreed to put their swords down and actually share information amongst themselves because there's a common understanding that your value proposition is not in the information. It's the value that your particular firewall adds to the marketplace.

Jim: Yes.

Bill: And not in the flow of information. In fact, you could make all the firewalls ... You could take that card off the table for everybody if you just shared it organically. Now you add value on top of your firewall.

Jim: Yes.

Bill: And how you grab the information and present it and make it easy and reducing complexity for people managing it. Blah, blah, blah.

Jim: Right.

[00:26:00]
Bill:
But I'm wondering from an ISAC perspective where you think your unique value proposition's gonna be for your members over the next three years?

Jim:

[00:26:30] Right. Well, that's a good question. Most of the general public would not be aware that just last year there was a new initiative to create ISAOs -- so it would be Information Sharing Analysis Organization -- that would not be linked directly to an infrastructure sector. It could be a group of individuals, companies, that come around any topic to share information.

[00:27:00] So if that exists, then there are other organizations that could quote unquote "compete" for what we're doing. We've gotta be in a position where we are bringing the right people together and sharing the right information, and doing it in a timely way. We're committed to doing all three of those things.

The other thing is ...

Bill: What's that organization called? ISAO?

Jim: ISAO. That'd be a broad terminology like ISAC.

Bill: How do you spell that?

Jim: I-S-A-O.

Bill: I-S-A-O. Okay.

Jim:
[00:27:30] There's some cities that are launching ISAOs which, obviously, span multiple industries just to get information shared. There's other groups.

Bill: Interesting. So you essentially -- for your competitive point of view, not that it's competing, but -- your context around your members is the key piece that the Department of Homeland Security's not necessarily able to lean a lot of their weight in to. Is that what I'm understanding?

Jim: Yeah.

Bill: Okay.

Jim:
[00:28:00] I think the other thing that we've done perhaps as a differentiator or as a way just to broaden our scope is, in addition to the original 200 gas-utility companies that we serve, in the last four months or five months, we have partnered with INGAA -- which is Interstate Natural Gas Association of America -- that would be the organization that serves the gas pipeline industry.

[00:28:30] So there's a few dozen gas pipelines in the United States. They're now partners within the ISAC, so they're sharing information along with gas-utilities. So we have not only distribution, which is what we call utilities, we also have transmission, which is pipelines.

[00:29:00] Most recently, we have begun partnering with the Canadian Gas Association. They cover both distribution and transmission -- so, utilities and pipelines -- for the Canadian provinces. At this point, and we're still onboarding some of these companies. They're not all fully onboarded to the ISAC yet, but when they are, the ISAC's reach will be US and Canada distribution and transmission.

We're gaining the breadth that we had hoped we would get and the right partners as we continue to do the good job that we've been doing of sharing information that makes it valuable to everyone that's participating.

[00:29:30]
Bill:
Now, are you saying that some of the 200, some of the smaller folks are having a little bit more staff challenged? So they're able to take your information and it's much more useful, or they can use it with their teams a little bit more deeply?

Jim: Sure.

Bill: Because they're ... Is that common just for the small, or is it ... Do you see the bigs even though they have a big team, not necessarily strong?

[00:30:00]
Jim:
That's a good question. I would be honest and say the information we're seeing shared by participants, more of the sharing is done from the medium to larger-sized companies, and perhaps more of the consumption by the smaller companies. I don't think it's a surprise and every person I've spoken with that's in a larger company is very happy that they're able to serve the small companies. Very much so.

[00:30:30] You mentioned the partnership between multiple firewall companies. One thing that's a real benefit to natural gas utilities, there really isn't competition. There is a spirit of sharing in general.

Bill: Okay.

Jim: I've worked with other disciplines within the industry over the years I've worked with AGA and seeing folks share information just to help each other has been phenomenal. This is another example of that.

[00:31:00] I think because it's security information, it's a little bit more slower in coming, but it's coming.

Bill:

[00:31:30] Where do you see the innovation needed right now? From the vendor side, where from your view of the world do you see that where we could really use a boost or innovation, or even what vendors do you see are coming up with some really innovative products that could benefit your industry or the CIOs should be paying attention to?

Jim:

[00:32:00] Right. That's a good question. Because of the nature of our organization, we tend to not speak a lot about vendors. However, in concept, the one area that we have been looking at recently is quantum computing. Our partners, the Canadian Gas Association, provided a webinar for Canadian and domestic gas companies on that topic and it's readily apparent that, in the near future, quantum computing will so drastically speed computer operations that what we know currently for security algorithms will essentially be meaningless.

[00:32:30] So there are some partners out there that are working on solutions to that today and there's a degree to which it's a little ways off yet, but I think it'll come around faster than folks think that it will. I'm glad we're starting to look at that. That's something that's been front of mind for us recently.

Bill:

[00:33:00] What about the machine learning? What about some of these advanced techniques, these math techniques for building some capabilities in to analyzing data and pulling context out of data more rapidly? Have you looked in to that much?

Jim: I haven't spent as much time with that.

Bill: Okay.

Jim: We've spent more time with some threat analysis products that would enable the people to piece together things that they're seeing.

Bill: Okay.

Jim: We've spent more time than we have with machine systems we could train to do that.

[00:33:30]
Bill:
Okay. So your role as a CIO has morphed through the years, I'm imagining, from someone who has now not only responsibility for keeping the lights on for general day to day operations for IT, but then this also new capability. What was the shift? How did that shift happen?

Jim:
[00:34:00] How that shift happened. That's interesting. It's been a 20 year shift. I've been here for just about 20 years. Initially, my responsibilities were exclusively internally IT.

[00:34:30] As time changed, there became a need for someone else to cover some other industry areas, and I think what the AGA as an association does that's somewhat unique, many other associations have different staff that cover industry things versus internal administrative things.

We've done with our accounting group, our IT group, our legal group, others, our staff who cover those internal disciplines are also the ones that are caring for our members and providing staff executive services through the committees and running the programs. So that's been exciting.

[00:35:00] My start was with customer service, so we had an individual running customer service programs over 15 years ago who left the organization and because we felt as an organization customer service was so technology heavy, it would make sense for me to serve that group. Which I did, and still do. Customer service is part of my portfolio along with security for CIOs in the industry and, more recently, cybersecurity.

[00:35:30] The customer service and CIO programs I've done for so long, they're fairly constant on an internal basis.

Bill: Okay.

Jim: The internal IT responsibilities that I still oversee, I've got a phenomenal team that cares for those so-

Bill: It helps having a great team, actually.

Jim:
[00:36:00] Yes. It always helps having a great team. So they do what they need to do. I just provide leadership. There's a defining moment back in 2012 when the Shamoon virus impacted Saudi Aramco and [Iran's 00:36:09] gas and compromised tens of thousands of computers immediately.

[00:36:30] When that happened, it became apparent not just to our industry but a number of others that cyber was really sadly what everyone thought it was. And we began, then, to really put significant effort towards this. That's when for the last five years it's been a daily sprint to keep up with cyber.

Bill:

[00:37:00] What's really interesting is that it's the role of the CIO -- and I don't know if you did this consciously or unconsciously, but -- as that shift happened, it's not like the 'maintain the infrastructure' responsibility went away, but you immediately now are offering ... You came up with a way to offer value to members that I would consider offense.

[00:37:30] You almost, you're providing not only offense to members, providing them almost a new product service line, but you're also ... So it's completely what with NIS would probably be in the realm of sales and marketing function. "What can we market to our members?" But what's really interesting is, it's a completely necessary service that you reverse engineered and figured out how to launch that in to your membership.

Jim:

[00:38:00] Right. That's one of the things that I've liked the most about this job, and historically, my father worked for a gas-electric utility for his entire career and coming to AGA initially even without these cybersecurity responsibilities, I feel like I'm in an industry that people really need. It's not like you really have to sell it. It's just, it's there.

[00:38:30] People need gas to keep their homes warm and to cook and to serve a variety of purposes. The last five years, not just being able to be with an organization that helps to support companies who provide that, but to protect it and realizing that the security climate that we're in, has been very fulfilling. I'm thrilled to be doing what I'm doing, and I feel like there's a very small way I'm able to make sure that gas is flowing in our country. It's really exciting.

Bill: You're leaning in to your native talents and to amplify that beyond the four walls.

Jim: Yeah.

Bill:

[00:39:00] And in a big way. Did you ask for permission to do it or was it handed to you? Was it serendipity? Or did you seize the opportunity? What was your mental framework for ... Clearly you've been here quite a while, but still, you were 15 years in to it. Did you just have a ton of equity built up within a bank account built up within the organization to step in to that role, or did you have to go to people and say, "I can do this. Just give it to me. I can bring this on"?

Jim:

[00:39:30] That's a good question, too. One of my colleagues has actually spent more time with our industry on security than I have, and it would be traditionally as much physical security as it is cybersecurity. In the years leading up to the 2012 defining moment, there were a number of times where she would contact me and have me work with her on cyber-related things because it just wasn't as much her area of expertise.

[00:40:00] So the more that we started to shift that way, it just became obvious that there was a need for more hands and it just seemed to be the right thing to do. I think that there was less prescription and more, "This is just right. Let's just do it."

Bill: Okay.

Jim: Yeah.

Bill: That's great.

Jim: When it comes to jobs, it seems like there's more bad things fall in to place than planning things out.

Bill: Sure.

Jim: Whenever you try to plan things out, it tends to not work the way you think it's gonna.

Bill:
[00:40:30] No, that's really great. That's really great. A lot of the themes we've been talking about recently is innovation and how the CIO can make a big impact in the organization. Sometimes it's prescriptive, sometimes it's serendipity, sometimes it's just you're flung with the river and it's going left, you go left.

I don't think there's an absolute formula, but clearly you had a team that enabled you to be able to take on another opportunity without crushing you in the process, which is nice.

Jim: Right. Yeah, it wouldn't have happened without the team that supports me.

[00:41:00]
Bill:
So from some of the take aways that might be an interesting ... That's probably one of the mission-necessary pieces for, I would say, just observing yourself and others that the team, having a solid team in place gives a Archimedes lever for the CIO to then have some space to tackle some other pieces that the business may need.

Jim: Right, for sure.

[00:41:30]
Bill:
If you had to start your career over again 20 years from now, 20 years ago, with all the wisdom that you have to this point in time, what would you say to yourself looking back if you could have that voice of wisdom which is clearly not necessarily achievable, but what could you say to the younger CIOs if you could be that little voice in their head as they're launching in to their paths?

[00:42:00]
Jim:

[00:42:30]
That's a good question. Thinking deeply about that, one of the most important things is building relationships with other people in your organization. The information technology role is one of support and leadership. Knowing your organization's mission, knowing what the other leaders are trying to accomplish, and working with them to accomplish it, that's important. Your relationship skills and communication skills are probably the most important things for a CIO role.

[00:43:00] Most of the individuals that I have known that have come in to those roles have come in as prior analysts, programmers, and to be good at those jobs, it's not so much about relationships and communication. If someone is really desiring to move in that direction, ensuring that they have those skills is important. If there's a necessity, get there through technical skills as well. That's a lot of skills.

[00:43:30]
Bill:
Where would people start to develop leadership skills? Because that's a ... That's actually the second time in two days that I've heard that and I'm curious where someone could start. Is it a class? Is it a book? Is it experience? Is it hard knocks? What do you think?

Jim: There's two thoughts that come to my mind, and I'll talk about both communication and leadership. I had a boss ... Oh, goodness, it must have been 25 years ago.

Bill: Mentors.

[00:44:00]
Jim:
Yeah. He recognized that I needed to grow in communication skills. He pointed me in the direction of Toastmasters.

Bill: Oh, interesting. Yeah, yeah.

Jim:

[00:44:30] When I got to the very first meeting, I was so scared. I still remember being scared. Even the idea of talking in front of a group of maybe 20 people was daunting. At this point in my career, I've spoken to groups of a few hundred at times. I wouldn't say that I'm not nervous at all, but I certainly can do that much better than I could 25 years ago.

That's a very specific thing.

Bill: Right, exactly. Yeah, that's perfect.

Jim:
[00:45:00] The one thing about leadership I think that is helpful, in many parts of life there's opportunities to serve in volunteer capacities that are types of leadership.

Whether that's leading your kid's sports team or other extracurricular activity team or group, to civic leadership. There's countless opportunities for people to volunteer to serve. I think serving in some sort of a leadership capacity just develops your leadership skills and it also benefits the community.

[00:45:30] For me, I don't think there's anything better than that. I've had an opportunity to serve on my kid's private school school board for a number of years. I've had other leadership opportunities in the church that I've attended. That's what I would say in terms of leadership development.

Bill:
[00:46:00] Right. So you're breaking it down in to two pieces. The communications piece with Toastmasters, for example, and the civic piece. It's interesting, too, is that you can take a class on communications, or you can read a book about it, you can read about leadership, too, actually put it in to practice. What a better way to do it than through the service that you mentioned?

Jim: Right. There's no better leadership preparation opportunity than trying to lead a committee meeting on any topic.

Bill: Yeah.

Jim:
[00:46:30] Once you've got the scars from a few of those that builds leadership capabilities right then and there.

Bill: I would agree with you. I just stopped coaching soccer for the first time in 10 years this past fall, and I would say that some of the challenges experienced through volunteer travel soccer coaching was stunningly on the back of some of those things and learning there. It's pretty amazing.

Jim: Yeah.

Bill: I agree with you. Any type of volunteer capacity is a big deal.

Jim: Right.

[00:47:00]
Bill:
Well, I really appreciate you for your service and being willing to share about your career and things you're doing now to further the industry, the natural gas industry, and the profession of the CIO.

Is there any parting words as we wrap up or any words of wisdom that you wanted to share with the audience that you think would be useful take aways for people that as we wrap up this episode?

[00:47:30]
Jim:
Yeah, thank you. I think there's two different things that are on my mind. Just in the last few minutes, talking about participating in the community.

[00:48:00] Much of what I do as a CIO just is just caring for people. That's really what it boils down to. I think there's not enough you could say about having a mindset of being not only willing to, but eager to care for people whether it's their computer or whatever it is about them. That's very important.

[00:48:30] I think the other take away that I would want to give people is, in he last few years, I have seen the security threat that we're all under currently and it is real. I would just want to encourage everyone to be as cautious as they can be and also let people know that I've worked first-hand with numerous men and women that are securing the energy delivery for our country and I'm proud of the work that they're doing.

[00:49:00] I am confident that they are giving 100% to make sure that you have electric power and natural gas flowing on a regular basis.

Bill: You mentioned that before, that you felt like that was a completely committed group of, like the volunteer fire departments. Just passionate about delivering the securest infrastructure possible.

Jim:
[00:49:30] Absolutely. The men and women that are caring for those are just a remarkable group of people. I've seen them all over the country working very hard. I'll end e-mails at night, they're responding in the middle of the night to me.

Just a great group of people working hard to make sure that everyone in this country ha the power that they need.

Bill:

[00:50:00] That's a great ... I'm glad you wrapped up with that. And also the caring for people I think is a ... It's really interesting, because I feel like the power of the CIO is increasing as is ... I forget who quoted this, but, as software is eating the world, it's putting the CIO in to very much a leadership role. And the older the CIO, the more wisdom they can actually bring to bear.

At the end of the day, it's the appreciation for people are the end consumers and making sure that we have the human being in mind at all times. That's a good reminder for everybody.

Jim: Yeah. For sure.

[00:50:30]
Bill:
Well, I want to thank you, Jim, and until next time, we'll look forward to doing this again.

Jim: Thanks, Bill.