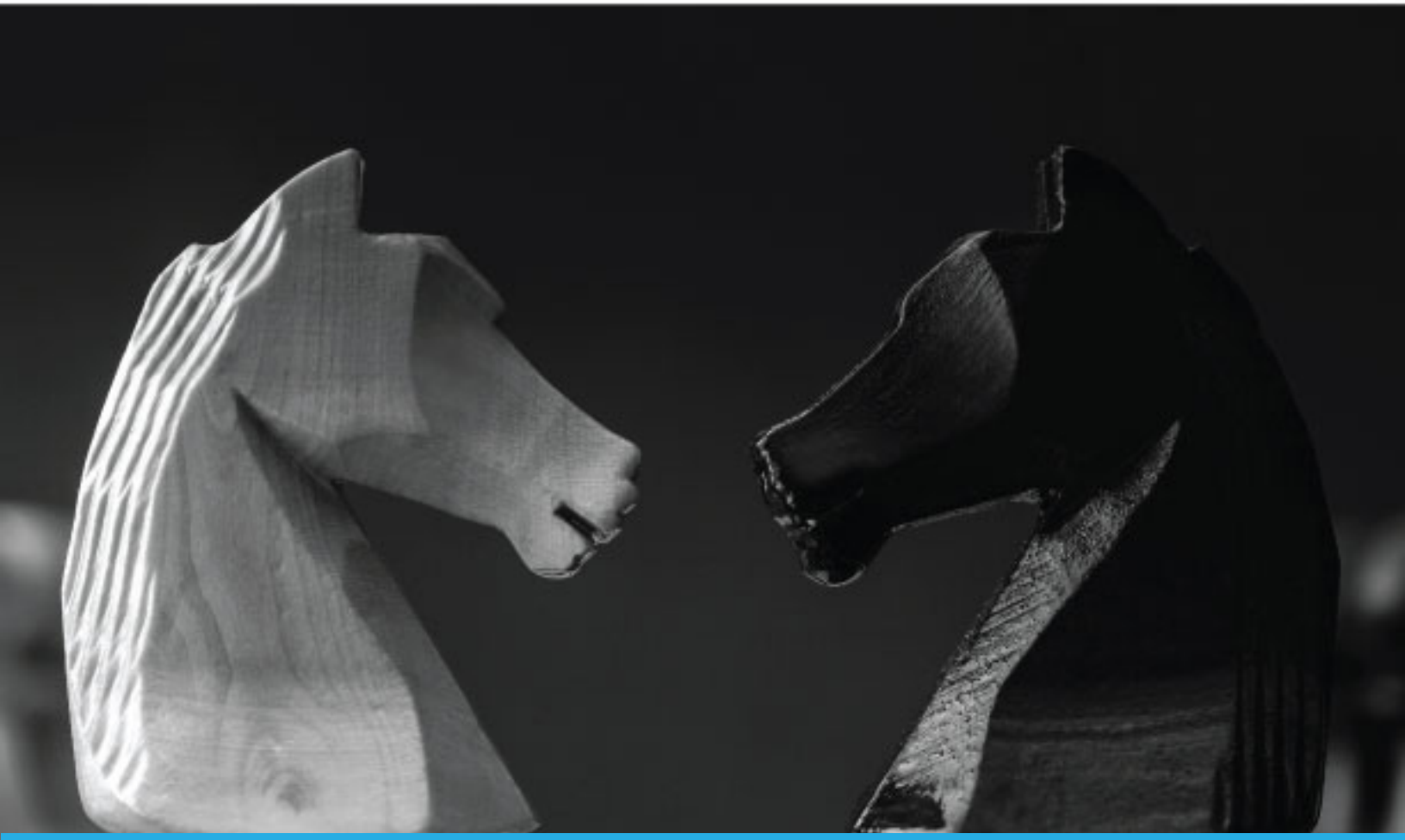
POWER

BUSINESS & TECHNOLOGY FOR THE GLOBAL GENERATION INDUSTRY SINCE 1882

PAS®

ICS Cybersecurity. Safety. Compliance.



The Power of Regulation Versus Well-Oiled Industry Standards

About the Panel

Aaron Larson
(Moderator) Associate Editor at *POWER Magazine*

Aaron is an engineer who has worked at nuclear, biomass, and coal power plants where he gained significant operations, maintenance, safety, financial, and management experience. He has also served in the United States Navy, earned a BS in Nuclear Engineering Technology from Thomas Edison State College, holds an MBA in Financial Management from City University of Seattle, and is credentialed as a Chief "A" Boiler Engineer. Aaron writes news and feature stories on a variety of topics for *POWER Magazine*.

David Batz
Senior Director of Cyber and Infrastructure Security at Edison Electric Institute

As Senior Director of Cyber and Infrastructure Security with the Edison Electric Institute, David helps members understand and apply appropriate security solutions to address emerging threats and issues. In addition to providing in-depth technical knowledge of security and network issues, David leverages over a decade of energy and regulatory compliance knowledge, as well as physical and cybersecurity policy experience and engagement with federal agencies, including the Department of Energy and the Department of Homeland Security.

Jason Haward-Grau
Chief Information Security Officer at PAS Global, LLC

Jason is the Chief Information Security Officer at PAS Global, LLC. He is a veteran technology leader with more than 22 years of cybersecurity and advisory experience within both operational and information technologies. Prior to joining PAS, Jason was the chief information security officer for MOL Group, an integrated oil and gas company with operations in over 30 countries, where he owned and developed the company's cybersecurity strategy. Jason has also held information technology leadership positions at Burberry, Vodafone, KPMG, GlaxoSmithKline, Diagio, Impact Plus and the Royal Bank of Scotland.

About This Transcript

The following is an adapted transcript of the webinar, "The Power of Regulation Versus Well-Oiled Industry Standards," hosted by *POWER Magazine*.

Introduction

The power industry is currently on NERC CIP Version 6 of its regulatory requirements with future regulations expected on supply chain security. Oil and gas has no such regulatory regime, but it does have standards that it uses to reduce cybersecurity risk, such as NIST 800-82 and IEC 62443. For O&G, compliance is an internally generated activity. So, which of these two approaches – regulated or not regulated – is best for industrial control system (ICS) cybersecurity? Does following a government mandated regime better secure an industry, or is self-regulation the answer?

Moderator Aaron Larson, editor of *POWER Magazine,* addresses these questions with two industry experts to illustrate how leaders in the power and O&G industries are addressing compliance and cybersecurity standards.

Panel Discussion

Q: (Aaron Larson, Power Magazine) Does government or self-regulation work better to secure an industry?

A: (David Batz, Edison Electric Institute) To me, it's not so much one or the other. Particularly with respect to the electric factor, I say it's both. For people within the electric sector, generally for those utilities that have assets part of the bulk electric system, they are subject to mandatory and enforceable standards by which they must operate elements of the bulk electric system. Although there are some challenges associated with mandatory and enforceable regulations, it does bring a sense of focus for those entities who are subject to the regulations. In fact, when an entity who is subject to the regulations has a failure, they could incur a very significant monetary penalty that can exceed $1 million per day per violation.

> *"...on a daily, certainly on a weekly basis, the number and types of threats changes and grows; and frankly,* ***regulations cannot move at that rate.***"

Government regulations for electricity system owners and operators fundamentally have functioned to raise the bar for those electric utilities. However, the other important thing to keep in mind is that regulations cannot move as fast as the threats move. For folks who are within the industry, there's a recognition that on a daily, certainly on a weekly basis, the number and types of threats changes and grows; and frankly, regulations cannot move at that rate. So for the electric sector, it's not a question of either/or, but really both.

A: (Jason Haward-Grau, PAS) I agree and I disagree, which is probably a good place to start. Regulation is a fundamentally important component that tends to become the ceiling rather than the floor and is seen as an operational overhead; a cost that leaches away from other areas. Regulation provides a framework, and that's an important facet of what should be done; however, self-regulation allows organizations to be more agile. You can tailor what you're trying to do, and you can be more responsive to it.

If you look at it by industry, each one is a little bit different. When looking at how oil and gas operate in comparison to power generation or transmission, there are differences that need to be considered. The thing you need to be cognizant of is how the regulation gives you a framework, but you need more than that. You've alluded to it, David, that industry cycles of change tend to be much faster than regulations can keep pace. NERC CIP is a fundamentally important capability, but up until now NERC CIP hasn't touched supply chain.

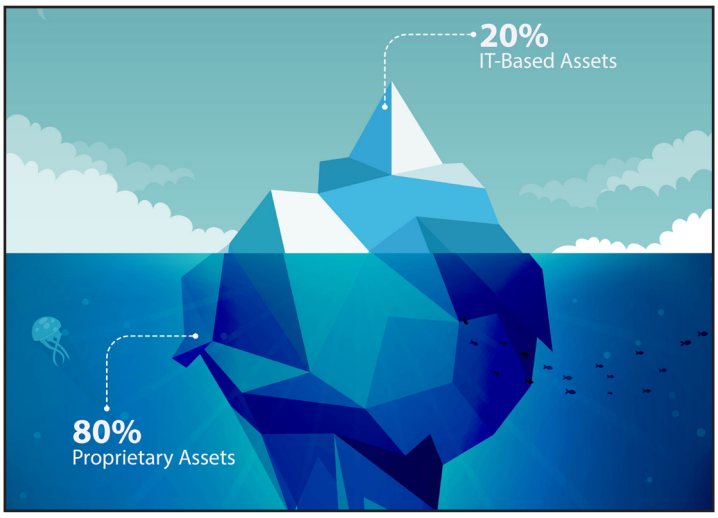
Cross-border situations also make it harder to enforce regulations. How do you deal with NERC CIP when you're compliant in the US, but you have operations in Europe, the Middle East, or wherever else? It becomes a challenge.

Well-constructed regulations provide a framework, and they are fundamental to getting things right. However, it shouldn't preclude us from going above and beyond to ensure our security. The NERC CIP violations are obviously driven by fines, and fines can encourage compliance, but compliance on its own is not the tool to drive more effective cybersecurity in the oil and gas sector or OT in general.

Q: (Aaron Larson, Power Magazine) When it comes to threats, insider threats are, of course, something that everyone needs to worry about. **Which approach works better to respond to insider threats?**

A: (Jason Haward-Grau, PAS) It's an interesting challenge. In both regulated and self-regulated industries, you need to be flexible and responsive to the emergence of threat. The agility of being able to respond to an insider threat is just as pertinent as an external threat. In either case, you need to be able to handle it practically. Knowing what assets you have is the first step to everything.

If you look at the logic of OT, about 80 percent of the OT assets that you have are hidden below IT. If you don't know what you have, you can't secure it effectively, regardless if it's an internal threat or an external threat. You need to also understand where you're vulnerable. You need to be able to track all the way through the lifecycle of your employees, understanding where things work and where they don't work. A precursor to any potential action is that inevitably something changes, so you need to understand what has happened and what



has changed. You need to be able to track that regardless if it's internal or external, legitimate or illegitimate. It's very difficult to track the insider threat from a legitimacy perspective, because they're already trusted and inside the environment.

> *"A determined **insider will still be able to do the things that they want to do.** It's about being able to manage and mitigate risk."*

This also means that you need a collaborative technology strategy. It's not just a case where there's a silver bullet to instantly identify who's doing something out of pattern. Unlike finance where your credit card being used in a different country suddenly triggers an alert, there is no panacea that says technology makes it work. A determined insider will still be able to do the things that they want to do. It's about being able to manage and mitigate risk. The more you see and the more quickly and intelligently you see it, the more likely you are to be able to resolve it with speed.

A: (David Batz, Edison Electric Institute) I agree with the base premise that, at the end of the day, externally asserted standards and regulations fundamentally are not going to be able to solve some of the challenges associated with the insider threat. In fact, we've seen within the U.S. government specific situations where individuals with significant administrative access took steps that were clearly against the rule sets within their organizations to disclose sensitive information.

Organizations must take affirmative steps to protect, but recognize that prevention is only part of the answer and not all of the answer. In the unfortunate event where critical assets are disrupted or possibly damaged, what steps or mechanisms has an organization considered for restoring and recovering their most important assets? Where are they in terms of incident response planning and exercises regarding their most important sets of asset?

Q: (Aaron Larson, Power Magazine) Insider threats aren't the only threats. We also have state-sponsored threats. **Is oil and gas nimbler in responding to state-sponsored threats?**

A: (David Batz, Edison Electric Institute) With respect to state-sponsored threats, it's a little bit of an unfair fight. Perhaps you've heard the expression, "never bring a knife to a gunfight." It's a little bit of a challenge that, no industry on its own, no industry practitioner on its own, is going to be 100 percent successful when interacting with a nation state and state-sponsored actors.

In this situation, it is really important for oil, natural gas, or electricity organizations to have processes in place organizationally to protect their most valuable assets and focus on restoration and recovery mechanisms. Prevent where you can, but take steps to detect and engage with U.S. government entities in this space as well.

A: (Jason Haward-Grau, PAS) There are a number of things that we need to take into account. The reality is that the state-sponsored strikes have expanded. Most of us are aware of the impact in Ukraine. Whether these strikes are official or denied, you can see significantly that the energy industry is being hammered. Some organizations are better positioned to handle this kind of threat. They have better insight and intelligence having operated in a

number of these states over the years.

State sponsorship is not just about shock and awe damage. It can be about getting in, stealing, and getting out. It can also be about getting in, *falsifying*, and getting out, hopefully in a way that's undetected so that organizations start to doubt their own data.

A behavioral shift is really needed across industries. A company can't win against the resources of a nation state. The common acceptance in the IT landscape is that it's not a question of *if* you get attacked or *if* you get breached, it's a question of *when*. It is going to occur in some shape or form. The sheer volume of vectors and complexity in the landscape is such that it will happen in some shape or form. You need a plan to recover.

I'll draw the distinction between IT and OT. In the IT space, breaches happen, and they're tragic, awful, and very difficult to handle. However, if a breach happened in the OT space, you're putting safety at risk because you're dealing with chemicals and complex machinery. You're putting the health and safety of the employees and the communities in which they work and live at risk.

The ability to recover is key, and testing that is fundamental. Regardless if the cause is state-sponsored, organized crime or physical, all these things need to be handled. When you focus on recovery, how quickly can you recover? What can you do? Do you understand your risks?

After Hurricane Sandy, utilities across North America helped restore power to the east coast using conventional mutual system practices. Just imagine if an entire industry is hit. The ability to do that is going to be lessened; but, if we work in the right way collectively, it's going to make a massive difference. If you haven't tested your disaster recovery plan or if you haven't tested your crisis management plan, you don't know if it's going to work. Knowing your critical processes and how you can protect them is one thing, but then testing for what happens when they go wrong is another. How do you ensure that you can have continuity of oil and gas supply? How do you know where are your soft targets? How do you ensure that you harden them, but then test against them being damaged anyway? These are all fundamental to delivering a more secure landscape.

A: (David Batz, Edison Electric Institute) I'd like to pick up on one point that Jason mentioned, and that is a shift in culture. In the old days, folks thought, "nobody would ever attack me. I'm just a little utility company. I'm in the Midwest, or I'm on the east coast, or I'm on the west coast. I'm just a utility, I'm just serving energy, or electricity, or oil, or natural gas. Who would go after me?"

The cultural change that I see happening is that people are now questioning why they are experiencing

> *Alarm and panic is not helpful, but it is helpful for people to* ***be creative as they consider unusual circumstances.***

problems, outages, unusual events, or security events. They're not saying, "oh, I just had a discreet equipment failure," or "this component is broken, so I should just replace it." People are now starting to ask the question, "are the unusual circumstances that I'm observing a discrete failure on technology or is it indicative of something else?" That's useful for people to be more imaginative as to the causes of problems. Alarm and panic is not useful or helpful, but it is helpful for people to be creative as they consider unusual circumstances. It might not be just as simple or innocent as a network connection being down. There might be other forces in play.

A: (Jason Haward-Grau, PAS) There's a denial element that still exists, an anonymity shield. Some organizations think they're too small to be noticed, while other organizations think they're too big to fail.

You're right that assumptions and fear shouldn't be the driver. It needs to be fact, not assumption-based. You need to know where you're vulnerable and what vulnerabilities exist. In the OT space there is a cross-functional challenge of multiple proprietary systems. You need to understand exactly where you can be vulnerable and what that vulnerability looks like from a risk perspective. You need to know what you have, and then you need to be able to overlay that into your processes. Know how you would manage those assets in the event of an incident, whether it's a physical incident like Hurricane Sandy or it's a cyber incident due to malfeasance, a mistake, or a deliberate cyberattack. When you know where you are vulnerable, you can map that against your risks, because it is a question of when, not if.

Q: (Aaron Larson, Power Magazine) What does success look like partnering with the governement in the power industry?

A: (David Batz, Edison Electric Institute) It is important that entities, whether electric or oil and natural gas entities, build and maintain effective relationships with their government partners, even at the local level such as FBI field or local law enforcement offices. Utilities should engage and help them understand what are the more important locations that fall within that law enforcement's purview, such as substations or gas gates. What safety issues do local law enforcement officials need to know? It's important for utilities to engage with their local offices to build and maintain those relationships under "blue skies." It's really challenging to first meet somebody during catastrophic failure. It would be much better to engage with local and regional law enforcement officials under blue skies, when people have time to talk about some of the issues of mutual interest.

It's also important to build and develop relationships at the federal level. Within the electricity sector, there are several engagements with both the Department of Energy and the Department of Homeland Security regarding initiatives like prioritizing research dollars on issues associated with cybersecurity. In addition, within the electricity sector, there is an organization called the Electricity Subsector Coordinating Council that consists of senior executives from across the electricity sector in the United States. They represent all business models including investor owned utilities, public power utilities, and cooperatives. It's at this Council that senior management of the electric sector can engage, share, and coordinate with counterparts like the Deputy Secretary of the Department of Energy and various undersecretaries and assistant secretaries from the Department of Homeland Security.

In the event of a large scale regional or multi-region event, such as storms like Superstorm Sandy or Hurricane Matthew, there is a forum where the owners and operators of the electric system can engage with their government partners to ensure that there's both unity of message and unity of effort for effective restoration. One of the recent initiatives out of the Electricity Subsector Coordinating Council is called Cyber Mutual Assistance, whereby utilities from various business models can help each other in the event that a given utility is having a challenge in delivering electricity to their customers. They can reach out under the protection of a non-disclosure agreement to other representatives from Cyber Mutual Assistance and get assistance as desired. It's a voluntary program under the sponsorship of the electricity subsector coordinating council.

> *"...recent initiative out of the Electricity Subsector Coordinating Council is called* ***Cyber Mutual Assistance, whereby utilities can help each other*** *..."*

Q: (Aaron Larson, Power Magazine) How do both industries fare in light of the growing specter of ransomware?

A: (Jason Haward-Grau, PAS) Some of the challenges include the same question being asked over and over. "How do I know we're going to get attacked? When is it going to happen?" The practical first step is to accept that it's going to happen. The old adage works, "hope for the best, but prepare for the worst." Preparing for an inevitable ransomware attack, in my experience, is much easier than responding to it. You need good, effective backup and to be able to restore on the basis that it's going to happen. Ransomware is a propagating and fast-growing attack vector. It's probably the fastest growing. According to Kapersky Lab, we've seen a 35-fold increase in the last 12 months. It's the weapon of choice because it doesn't need to dial home in the same way as other malware.

The reality for IT is that it's a lot easier to respond because it's a restoration capability. OT is trickier, because you've got to know what you're doing, and you've got to know what is being ransomed and how that's affecting you. The interrelationship and the complexity requires that you have visibility to 80 percent of the critical assets in the process control network.

Good data backup is also critical. If the data is lost and there is no ability to restore rapidly, you can see incremental loss hitting you. I've seen it from a physical damage perspective where you need to be able to recover. The first critical thing is that you don't know whether it's going to happen or not, but let's assume it does.

How would you respond? Where would you be most likely to suffer a ransomware? Where would that hurt you the most? How can you ensure that you can put in place effective continuity processes to cover it?

Asset owners and operators need configuration and OT asset information to do that prioritization. You can't protect all the assets, all the time. It's just impractical and not feasible, so you need to have a prioritization framework or model to protect the most important things first. What drives you? Where do you get your value? How do you ensure that value is applying? You know where your business makes money. When you know what that is, then you should be able to protect it and prioritize accordingly.

And equally, you must understand your vulnerability of attack. Do you have monitoring practices in place? How effective is IT in looking at the OT side of things? What's your business awareness of cybersecurity best practices? Ninety-nine percent of ransomware comes in through the human interactive element. An understanding of those particular tactics is fundamental to preventing as best you can. The ultimate thing is, while you can say no to ransom, you better plan for it happening anyway.

A: (David Batz, Edison Electric Institute) Within the context of electric utilities as well as oil and natural gas, as people prioritize the assets that are most needing protection and the ability to restore quickly, it's very important that people also consider the health and life safety systems that are associated with these assets.

Clearly, one must prioritize life and health safety systems when considering the risk of ransomware. A number of different industries, including hospitals, local police departments, small and not small businesses, and even utilities, have been affected by ransomware. With respect to incident response and incident response practices, it's very important that practitioners really think about how they deal with the potential of ransomware within their organization.

It's also important to involve senior company management representatives as part of incident response training and response practices. Again, under blue skies people have an opportunity to talk through the pros and cons of various approaches in response to ransomware. Sometimes there are no easy answers, but it's better to plan, prepare, and practice against such an eventuality than to be surprised by it. Include other levels in the organization, not just senior management. Include the communications and public affairs folks as well as representatives from the legal and human resources departments. What about your business partners? What is their role with respect to your response, or your organization's response, in dealing with the potential of ransomware?

Q: (Aaron Larson, Power Magazine) In conlusion, what are common best practices that both industries can recommend to secure industrial control systems?

A: (David Batz, Edison Electric Institute) I think Peter Drucker said, "if you can't measure it, you can't manage it." When we talk about industrial control systems, it's critical that asset owners and operators understand each of the discrete components that make up their industrial control systems.

Ransomware not only attacks files, but it can affect baseline configuration of industrial control systems or break certain components. The question is, have entities appropriately characterized and inventoried their industrial control systems?

Another major issue is to maintain visibility and consider continuous monitoring for the most important systems. Again, a lot of security is about prioritization. If a single corporate workstation is affected by ransomware, a single workstation is not a big deal. It's a very easily recoverable asset. However, when thinking about industrial control systems that are connected to large rotating equipment, large transformers, or large pipelines, it's really important to maintain situational awareness and understanding of those assets.

> *"....**maintain visibility and consider continuous monitoring** for the most important systems."*

A: (Jason Haward-Grau, PAS) The approach to industrial security is to work out what you can accept from a business continuity perspective. It starts with the protection of your people and the community in which you operate. There is no other alternative.

You'd liken the same thing to physical security. If you look back at the industrial disasters that have happened as often as they have, they drive learning. They drive education and awareness that make people aware that they have to plan. it's worth reiterating that drills are necessary.

Senior executives need to understand what's happening, and the drills need to be real. There's no point in doing a desktop exercise with stuff that's not likely to happen. Instead do those things that are going to be hard. Show what it looks like. Use published ransomware to ensure that the executives participate and are looking for those opportunities to improve processes. It needs to be top down as well as bottom up. The bottom up guys often do things really well, because they understand at a process level what needs to happen, but it needs to build it all the way up. Leverage NERC CIP to understand and segment for low, medium, and high asset protection.

Mitigation of risk, transition to others, and accepting risk are all options, but do it with your eyes open. There are some risks that you will decide that the likelihood is so remote, you're not going to do much about it. You can do that if your eyes are open, knowing that's what you're doing. You have to review it, though, because risks change.

The challenging thing about this industry is that many of the things that we thought we knew 10 years ago are no longer relevant because the vectors have changed. It's only going to continue and complexity will grow. If you've got the competence to monitor your environment from an IT perspective, then looking at how you

leverage it from an OT perspective is going to be fundamental going forward. If you don't have a program in place, and there are large organizations who still don't have a unified program, get one. Consider what you need to do. Consider planning for the worst and hoping for the best scenario. Then test your program, test your plan.

Additional Resources

For more resources and information on how PAS can help you manage and protect your industrial control systems, visit cyber.pas.com.

About PAS

PAS is the leading provider of software solutions for ICS cybersecurity, process safety, and asset reliability to the energy, process, and power industries worldwide. PAS solutions include industrial control system cybersecurity, automation asset management, IPL assurance, alarm management, high performance HMI™, boundary management, and control loop performance optimization. PAS solutions are installed in over 1,100 facilities worldwide in more than 70 countries. For more information, visit www.pas.com. Connect with PAS on Twitter @PASGlobal or LinkedIn.