Mighty Guides®

Strategies for Managing

OT Cybersecurity Risk

Sponsored by PAS®

INTRODUCTION

Kaspersky Lab's discovery of Stuxnet in 2010 turned the industrial world on its head. As the first known instance of malicious code specifically designed to seek out and interfere with industrial operations, Stuxnet was a serious wakeup call for OT operators, especially those in much of the world's critical infrastructure. So how has the OT/ICS community responded to the new reality of OT cyber risk?

With generous support from PAS, we asked 4 OT security professionals the following question:

What are the top three pieces of advice you would give a CISO to make the plant OT/ICS environment more secure from cyber attacks?

For OT and IT security people, this is something of a loaded question, largely because OT cybersecurity is still very much a work in progress. For instance, although many contributors stressed the importance of knowing your environment, that in itself is a big challenge that varies from industry to industry and plant to plant. "Asset knowledge" also means different things to different people.

The essays in this eBook provide a wealth of information and present an inside look at an aspect of cybersecurity that is still not well understood. I am certain that anyone responsible for critical industrial operations will benefit from the advice and experiences of those who have contributed to this eBook.

All the best,
David Rogelberg
Publisher,
Mighty Guides, Inc.

Mighty Guides®

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

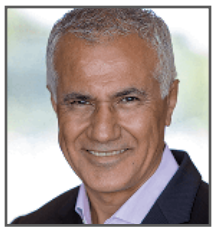
FOREWORD BY EDDIE HABIBI

Digitalization and Industrie 4.0 initiatives require tight integration between the complex, heterogeneous, and highly complex Industrial Control Systems (ICS) and the enterprise IT. However, the very components that enable digitalization—sensors, connectivity and smart applications—also increase risk. Digitalization enhances efficiency, improves safety, and optimizes production, but it also creates more opportunities for bad actors to penetrate operational technology (OT) environments and to wreak havoc.

To secure industrial facilities and ensure safe, reliable production, OT and IT security—traditionally two separate disciplines with different priorities—must come together to share cybersecurity and risk management best practices.

In this eBook, experts on the front lines of OT cybersecurity risk mitigation share their strategies for making control systems more secure. The firsthand experience collected here comes from experts across a diverse range of industries – including oil and gas, chemicals and refining, and power generation. Their essays illustrate the importance of understanding similarities and differences between IT and OT environments. They also share proven experience on adapting IT security controls and best practices to OT environments.

Apply the valuable insights provided in this guide within your own company to protect the endpoints that matter most in your company's industrial facilities—the proprietary industrial control system (ICS) assets responsible for safe and reliable production.



Regards,
Eddie Habibi
Founder & CEO, PAS Global, LLC

Founded in 1993, PAS is a 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 1,380 facilities worldwide in more than 70 countries. PAS was recently named the #1 Global Provider of Safety Lifecycle Management by ARC Advisory Group including #1 rankings within Chemical, Power Generation, Refining, and Oil & Gas. For more information, visit www.pas.com. Connect with PAS on Twitter @PASGlobal or LinkedIn.

STRATEGIES FOR MANAGING OT CYBERSECURITY RISK

In This Section...

OT SECURITY REQUIRES A HOLISTIC VIEW OF PLANT RISK

AGUSTIN VALENCIA

OT Cybersecurity Advisor
Iberdrola

Agustin Valencia is an ICS professional who has held leading engineering, operations, and maintenance roles in the thermal and nuclear generation industry. For the past six years, he has focused on applying cybersecurity controls to both new control systems and legacy systems, from new designs and projects from the operator and maintenance engineer's perspective.

LinkedIn

Cybersecurity has always involved people, processes, and technology, and in a homogeneous IT environment, people often think first about the technological aspects of cybersecurity. But in the OT world that is found inside large industrial plants, "Technology must be chosen for the OT environment and adapted to the plant," says Agustin Valencia. That leaves it up to company processes to fill the cybersecurity gaps. "Technology cannot be enough. In the case of OT systems, procedures and awareness can make the workers our best firewall."

> *Technology must be chosen for the OT environment and adapted to the plant.*

Much of the challenge comes from the criticality of industrial processes, combined with a great diversity of new and old control systems. "Many new components integrate with Ethernet communications and with other things such as firewalls and antivirus software," Valencia says. "They can also connect with the rest of IT software technology. But legacy systems do not provide this capability." To monitor and maintain these systems, it's necessary to extract information directly from the assets, but without affecting communications. Some systems can only do this offline, when a process is stopped. But in many OT environments, processes rarely shut down. »

OT SECURITY REQUIRES A HOLISTIC VIEW OF PLANT RISK

Valencia, whose role at Spanish electricity company Iberdrola covers nuclear power plants and other sources of power generation, approaches OT cybersecurity in this way:

- **Look at risk holistically.** You must first look at all the risks to the entire business, and in the case of large industrial plants and critical infrastructure, this is a much broader risk assessment than is typical in the IT world. “In OT, it’s not a matter of just interrupting the service or losing data,” says Valencia. “You must consider the consequences of a failure that causes damage to workers, to the environment, to the community, the extra cost of stopping production, the cost of waste if production systems are altered, or damage to the plant itself if systems are changed.”
- **Classify assets according to risk.** Of course you must have a complete inventory of assets and configuration status in your OT environment so you know what you must protect. But it’s necessary to take that a step further, to classify those assets according to risk. “Once you know the assets and risk, you can also establish their impact and risk profile,” he notes. In this way, you are able to prioritize vulnerability-management strategies and ICS maintenance. »

“In OT, it’s not a matter of interrupting the service or losing data. You must consider the impact of a failure that causes damage to workers, or to the environment, or to the community, the extra cost of stopping production, or the cost of waste if production systems are altered, or damage to the plant itself if systems are changed.”

- **Develop OT-specific policies, procedures, roles, and responsibilities.** It's important to recognize that OT cybersecurity is not just an IT problem. There is too much in the OT world that is unique and different from IT. This means everyone in the plant needs to understand their contribution to OT cybersecurity. "People must know their responsibilities," says Valencia. "When a problem arises in a specific environment, everyone has a duty for detection, information, analysis, isolation, erradication, or restoration. In OT, the cyber part is complementary to the process part, so the organization must train everyone on their role."

In the OT world, many cybersecurity practices are unique to the industry and the plant. For instance, one can't rush into a plant and install the latest patches if there is an incident or a threat. This can trigger failovers that stop a system or process, which cannot be allowed to happen in an OT environment. "Everything must be tested," Valencia stresses. "And you need that holistic approach. If a threat is coming from somebody who can touch my legacy system, perhaps I have to deploy physical security. But if my problem comes from the network, I can implement controls over that piece of hardware to cover that vulnerability in the legacy system." ■

KEY POINTS

Download the full e-book: Reducing Industrial Risk: 20 Experts Share Strategies for Managing OT Cybersecurity

1 **Classify assets according to risk, so you know what you need to protect and can prioritize vulnerability-management strategies and ICS maintenance.**

2 **OT cybersecurity is not just an IT problem. Everyone in the plant needs to understand their roles and responsibilities for OT cybersecurity.**

JASON HAWARD-GRAU

Chief Information Security Officer
PAS Global, LLC

Twitter

Website

LinkedIn

ICS cybersecurity is a risk we should manage and not fear. We must not abandon progress in the face of cyber threats. The threat of cybersecurity will not stand in the way of digitalization and Industrie 4.0. It is just another hurdle to overcome. Just like any other risk, we must understand it, take decisive measures to protect against it, and make security awareness a part of our culture as we have done so effectively with safety. CISOs, plant managers, and IT and OT/ICS security teams must find a balance between digitalization and cybersecurity, two business tactics that have the appearance of being in conflict.

DON'T MEASURE OT CYBERSECURITY RISK IN TERMS OF FINANCIAL IMPACT

OMAR SHERIN

Director
Ernst & Young

Omar Sherin holds a BSc in Computer Engineering and has 15 years of experience in critical infrastructure protection. Sherin is an elected voting member in the ISA99/IEC62443 standard for industrial control systems security. He is also an international member of the Industrial Control Systems Joint Working Group (ICSJWG) created by the US Department of Homeland Security.

Twitter I LinkedIn

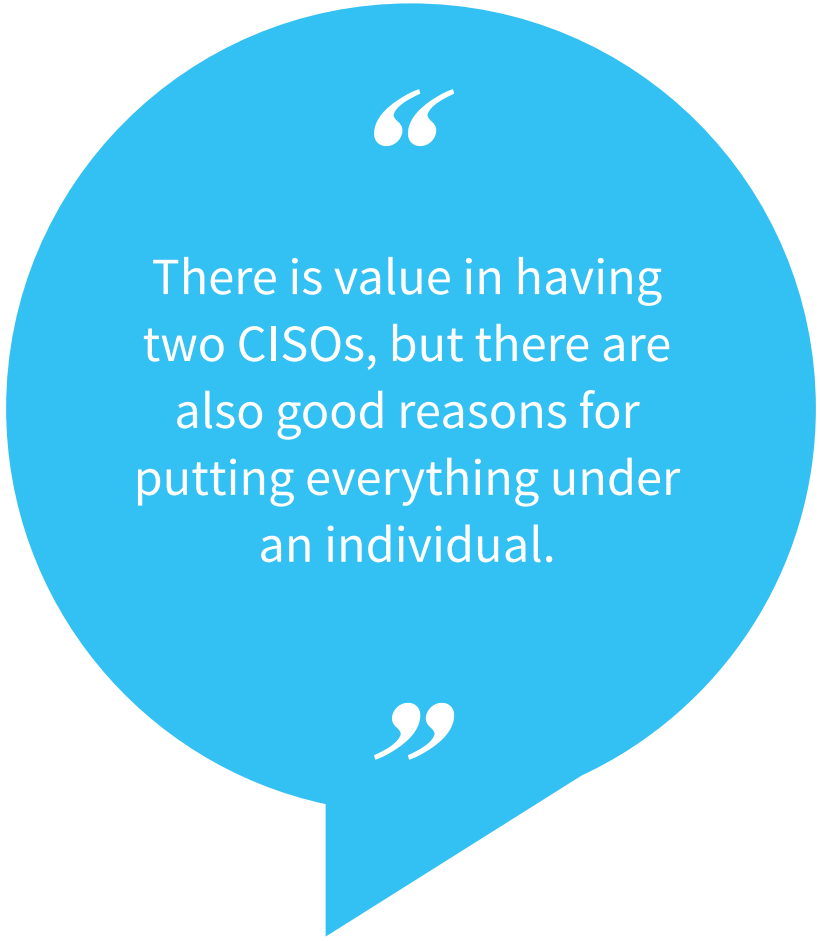
Omar Sherin, cybersecurity director (OT) for Ernst & Young covering the Middle East, India, and Africa, has a broad perspective on OT security. "I've been a provider of security services as a consultant, I've been an asset owner, and I've been a national regulator," he says. "Having different backgrounds has helped me see things from these different perspectives." In his view, the three most important things every OT security practitioner needs to do are:

- **Know the assets you have in your plant.** "Before discussing how to protect what you have, you need to know what you have," Sherin says. He advises considering new technologies to help with this task. "More OT vendors offer automated asset inventory tools designed for OT environments. It is not perfect, but they are a step towards gaining visibility we didn't have before." He also suggests a plant-segmentation strategy that makes different teams responsible for different areas, zones or process areas. "Everyone is responsible for his own area and to monitor, index, and catalog properly. This makes it an achievable task, especially for big plants that are spread over hundreds of kilometers," he notes.

> *Before discussing how to protect what you have, you need to know what you have.*

DON'T MEASURE OT CYBERSECURITY RISK IN TERMS OF FINANCIAL IMPACT

- **Calculate cybersecurity risk in terms of plant safety first, not just financial impact.** In the IT world, risk is often measured in terms of financial impact on the business, but this has little meaning in many industrial environments. "In many OT incidents we have seen, it's not about money. The impact is far greater than financial, and it's even harder to calculate impact for an asset that is critical infrastructure." One way to get plant operators and equipment vendors to focus on cybersecurity and increase accountability is to make it a question of plant safety. "One problem asset owners always have, especially for the old systems, is that the service-level agreements, contracts, and warranties say nothing about cyber breaches," Sherin explains. "The cyber risk was not there 10 years ago. But what they have always had in those contracts is plant safety. By linking cyber impact to safety, you bring the OT guys onboard. Now contractually, all the vendors have to help you. When you link security to safety, it suddenly makes sense to people. That's a language they understand." Sherin says that Ernst & Young has extended the standard hazard and operability study (HAZOP) to include cybersecurity, which it refers to as S-HAZOP.



DON'T MEASURE OT CYBERSECURITY RISK IN TERMS OF FINANCIAL IMPACT

- **Clearly define who is responsible for cybersecurity in the plant.** "Many companies struggle with this," says Sherin. "The governance model is not yet there and so there's often conflict." Some companies choose to create a single chief information security officer (CISO) who is responsible for OT and IT security across the board. Other very large companies choose to have two separate CISOs, one for OT, and one for IT. "In this type of structure, OT and IT are completely separate and treat each other as third parties. Each focuses on securing his area. Their relationship is governed by SLAs and agreed protocols," he adds. For the two-CISO model to work, they must collaborate closely. "It makes a certain amount of sense because IT and OT have different priorities and do things differently," Sherin says. IT might be focused on confidentiality while OT is focused on reliability. For OT, safety is important, but that is not an IT concern. If IT has an incident, you can just stop or restart the asset, but you cannot just do that with a plant. "There is value in having two CISOs, but there are also good reasons for putting everything under one individual. I think there's no right or wrong way. The important thing is that it be clearly defined," Sherin says.

All these things are evolving as changing technology causes OT and IT to converge. "Over the next 10 years or so, you will see more wireless plants. You will see more digital oil fields where entire rigs are free of humans, completely run and maintained by robots," Sherin concludes. ■

Download the full e-book: Reducing Industrial Risk: 20 Experts Share Strategies for Managing OT Cybersecurity

KEY POINTS

1 **Plant segmentation, in which different teams are responsible for different areas, makes cataloging assets possible, especially in very large infrastructures.**

2 **One way to get plant operators and equipment vendors to focus on cybersecurity is to make it a question of plant safety.**

RISK MANAGEMENT REQUIRES EFFECTIVE COLLABORATION

CRAIG MORRIS

Head of Information Security
North Oil Company Qatar

Craig Morris is the head of information security for North Oil Company. He previously managed industrial cybersecurity for Maersk Oil Qatar. With more than 25 years of experience in IT and cybersecurity, he has been involved in complex enterprise and industrial environments while on global assignments in Asia, Europe, the Middle East, and North America. During that time, he has covered most aspects of IT and cybersecurity including operations, strategy, architecture, and incident management.

Twitter I LinkedIn

As information security manager at North Oil Company in Qatar, Craig Morris is currently focused on leading the company's information security strategy and governance for enterprise and IT/OT systems. When considering high-level ICS security priorities, Morris recommends that security professionals keep these three tips in mind:

- **Develop a common understanding with the stakeholders about what is in the OT environment.** Stakeholders are not always clear in an OT environment, and the people you need to talk to may not be at the top of the organization's chart. That's why it's important to make a concerted effort to locate the people who work directly with the systems in question. "Get these guys together, feed them doughnuts, build the relationship, and map everything on the whiteboard," Morris suggests. "Once you bring it all together it starts to make sense, but usually no one brings it together. It's often the security guys who start trying to bring this stuff together and run into problems, and the reason they run into problems is because they don't understand the culture." »

> *"You need to understand how your assets are architected because that becomes important when you do risk and vulnerability assessments."*

- **Understand how the ICS environment is architected.** Once you have developed a common understanding about what field instruments, control systems, and workstations, and more are in your OT environment, you need to have a holistic picture of how everything works to truly understand the full range of vulnerabilities that may exist. “As a chief information security officer (CISO), you need to understand how those assets are set up,” he says. “You need to understand how your assets are architected because that becomes important when you do risk and vulnerability assessments. You have this system over here, it’s connected in this way, and that connection method is a vulnerability. Or maybe it’s not a vulnerability, maybe it’s the way it’s designed.” An engineer will always be able to provide you with a logical explanation as to why an asset was configured in a particular way, but at the end of the day you will still need to make a calculation as to the risk it poses.
- **Develop a risk-management program that includes a vulnerability assessment and a remediation plan.** This must also be done in conjunction with stakeholders. “Start assessing the risks and vulnerabilities in your assets so you can determine what controls are actually necessary in the environment,” Morris advises. »

“Start assessing the risks and vulnerabilities in your assets so you can determine what controls are actually necessary in the environment.”

He prefers to conduct penetration testing later in the process, however. “If you use normal penetration testing techniques, there’s a very good chance you may damage a functioning process. So when we do penetration tests, we do them offline in the test environment.” After that point, Morris advises CISOs to develop remediation plans and appropriate standards in conjunction with stakeholders to make sure their recommendations can actually be implemented in the OT environment.

This is essentially a three-step process: develop a clear and shared understanding about what assets currently exist in your environment, determine how they operate and what vulnerabilities may arise as a result, and then develop a risk-management program that assesses those vulnerabilities and devises a remediation plan to alleviate them. As Morris emphasizes, it’s important to pursue these initiatives in partnership with stakeholders in order to be certain that the resulting risk-management program can actually be implemented in the OT environment, as it is the stakeholders who will be able to advise you on the practical realities involved in doing so. With this kind of collaborative approach, you can create an effective risk-management strategy for your company. ■

Download the full e-book: Reducing Industrial Risk: 20 Experts Share Strategies for Managing OT Cybersecurity

KEY POINTS

1 **You need to have a holistic picture of how everything in the OT environment works to truly understand the full range of vulnerabilities that may exist.**

2 **An engineer will always be able to provide a logical explanation as to why an asset was configured in a particular way, but at the end of the day you still need to make a calculation as to the risk it poses.**

ICS CYBERSECURITY RISK MANAGEMENT REQUIRES A CUSTOMIZED APPROACH

CLINT BODUNGEN

Vice President,
ICS Cyber Security
LEO Cyber Security

Clint Bodungen is an industry-recognized ICS cybersecurity expert with more than 20 years of professional experience. He specializes in ICS security R&D, penetration testing, and risk analysis, with many of the world's largest energy organizations in the oil and gas and electric utility sectors as his clients. In his capacity as a volunteer cybersecurity mentor, Bodungen hopes to help usher in the next generation of young ICS cybersecurity professionals. He is the lead author of *Hacking Exposed, Industrial Control Systems.*

Linkedin I Twitter I Website I Blog

As vice president of ICS cybersecurity for LEO Cyber Security, Clint Bodungen is responsible for overseeing general cybersecurity services as well as ICS-specific services. Leveraging his deep experience in and operational knowledge of both fields, he develops creative solutions for customers to build and manage innovative operational security programs. When considering high-level ICS security priorities, Clint recommends that plants develop a comprehensive yet tailored cybersecurity risk-management strategy with these three strategies in mind:

> *Business executives, plant managers, and asset owners are concerned about the reliability, efficiency, integrity, and safety of their production and their data.*

- **Pursue a customized approach to risk management.** Bodungen believes there isn't really a single silver bullet that each and every plant can use to manage its vulnerabilities most effectively because every plant environment is different. "If I'm talking to you as an asset owner or a plant owner or operator, my top priorities may not apply to you. Your top need may be timely patching or network segmentation, whereas another organization, depending on the industrial vertical or the plant, may find it lower on their list because their business has different needs and priorities," he says. Accordingly, your approach should be tailored to your business, its industry, and its unique requirements. »

ICS CYBERSECURITY RISK MANAGEMENT REQUIRES A CUSTOMIZED APPROACH

- **Prioritize risk reduction and elimination.** At the end of the day, you're not implementing cybersecurity for the sake of cybersecurity—you are enabling the business to achieve its goals. "Business executives, plant managers, and asset owners are concerned about the reliability, efficiency, integrity, and safety of their production and their data. They want reliable, efficient, and integrated data so that they can have reliable, efficient, and safe operations," he explains. Accordingly, anything that threatens those top-level business goals is the risk that you are trying to avoid.
- **Incorporate threat modeling into your risk-management strategy.** It's not enough to know what your assets are, where they are, what vulnerabilities are associated with them, and what data communication paths or physical paths feed into those assets. "When you assess the assets, their vulnerabilities, and their communication paths, you're starting to identify attack vectors, which can be used in threat modeling," Bodungen says. "Now you need to know who might be interested in attacking those vectors, what mechanisms or what means they are using to attack, and which industries they are attacking." This builds a larger picture of the threats your business faces as well as a much more accurate prediction of the likelihood of an attack. »

"When you assess the assets, their vulnerabilities, and their communication paths, you're starting to identify attack vectors, which can be used as a part of threat modeling."

ICS CYBERSECURITY RISK MANAGEMENT REQUIRES A CUSTOMIZED APPROACH

Bodungen also strongly believes that any risk-management strategy must be nimble enough to adapt to changes in the threat environment. Threat modeling can be especially valuable for this purpose. It's also important to conduct your risk assessments more frequently than once a year—otherwise you might be missing important changes that arise. In addition, he recommends conducting a consequence analysis to help management gain an understanding of the risk involved in not pursuing certain cybersecurity strategies. These are some thoughtful steps that plants can take to strengthen their cybersecurity posture, guarding their ICS environment against the specific threats that apply to them, and continually updating their approach to factor in new threats as they emerge.

Download the full e-book: Reducing Industrial Risk: 20 Experts Share Strategies for Managing OT Cybersecurity

KEY POINTS

1 **ICS cybersecurity is not a one-size-fits-all endeavor. Businesses must tailor their strategies to match their unique environments.**

2 **It's important that top-level business concerns surrounding reliability, efficiency, integrity, and safety guide your plant's risk-management strategy.**

GARY WILLIAMS

Sr. Director, Cybersecurity
Service Offer Leader
Schneider Electric

LinkedIn

It all comes down to this: Cybersecurity has to be part of your operations lifecycle. And in order to do that, you have to make everyone, everywhere, responsible for cybersecurity. We say this again and again, but it's true: Cybersecurity isn't a destination; it's a journey. Security can never be viewed as a one-off project. Attacks on industrial control systems in the era of the IIoT are escalating, and they extend across industries, geographies and broader society. The risk for catastrophe is too great to ignore. New threats, attack techniques, and technologies are continually advancing. That means your people and your security protocols must always be advancing too.