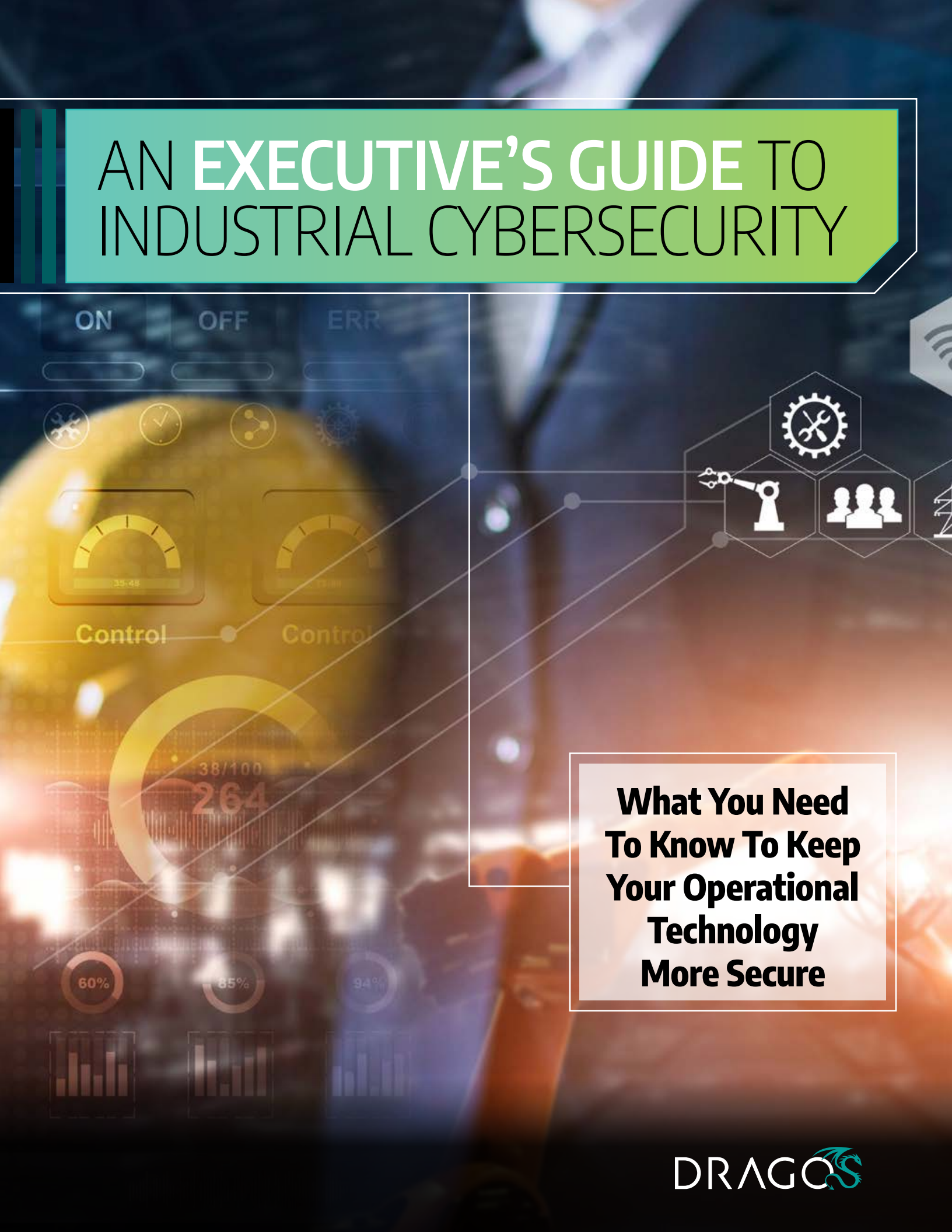
AN **EXECUTIVE'S GUIDE** TO INDUSTRIAL CYBERSECURITY



What You Need To Know To Keep Your Operational Technology More Secure

DRAGOS

The Importance of Industrial Cybersecurity

As enterprises invest heavily in digital transformation, industrial cybersecurity will increasingly serve as a critical enabler for safely and securely advancing business goals through technological innovation.

Advancing connectivity and digitalization of operational technology (OT) provides significant benefits to the business, including:

- increased automation,
- improved process efficiency,
- better asset utilization, and
- enhanced telemetry of machinery for business forecasting and equipment maintainability.

But when the cyber risks of this connectivity aren't addressed in tandem with innovation, the benefits can be diminished by heightened impact from security incidents.

The previous year offered up dramatic examples of the types of critical infrastructure risks that are exacerbated by the absence of effective OT cybersecurity preparation. The industrial world has seen electric power plants at risk from vulnerable information technology (IT) remote administration tools, and disruptive cyber attacks against water treatment facilities and natural gas pipelines.

This is a pivotal time for boards of directors and their executive teams—led by guidance from CISOs and risk executives—to start aligning appropriate risk management with operational innovation.

What you'll learn...

Included in this primer are the key concepts executives need to know to get up to speed on OT systems and how to better secure them.

- How ICS/OT systems are key to running the business
- How digital transformation and hyperconnectivity increase risk and exposure to these systems
- Why OT cybersecurity is different than IT cybersecurity
- How the OT threat landscape is growing rapidly and increasing in sophistication
- How many threats typically associated with IT still impact OT
- Why remediating OT vulnerabilities requires a different approach than IT vulnerabilities
- What next steps executives should take to assess and address unique OT cybersecurity threats

The evidence of OT cybersecurity weakness isn't just anecdotal, either. The following statistics confirm that many organizations have not yet paired their OT digital initiatives with appropriate security investments.

Key Trends

of organizations had extremely limited to no visibility into their OT environments, including ICS networks, assets, and flow of information between them

Dragos Year In Review

of organizations exhibit poor security perimeters around ICS networks, meaning they're at increased risk of attack through IT networks or the internet at large

Dragos Year In Review

KPMG Cyber Security Annual Report

Sixty-three percent of respondents say OT and IT security risk management efforts are not coordinated making it difficult to achieve a strong security posture in the OT environment

Ponemon Sullivan Report

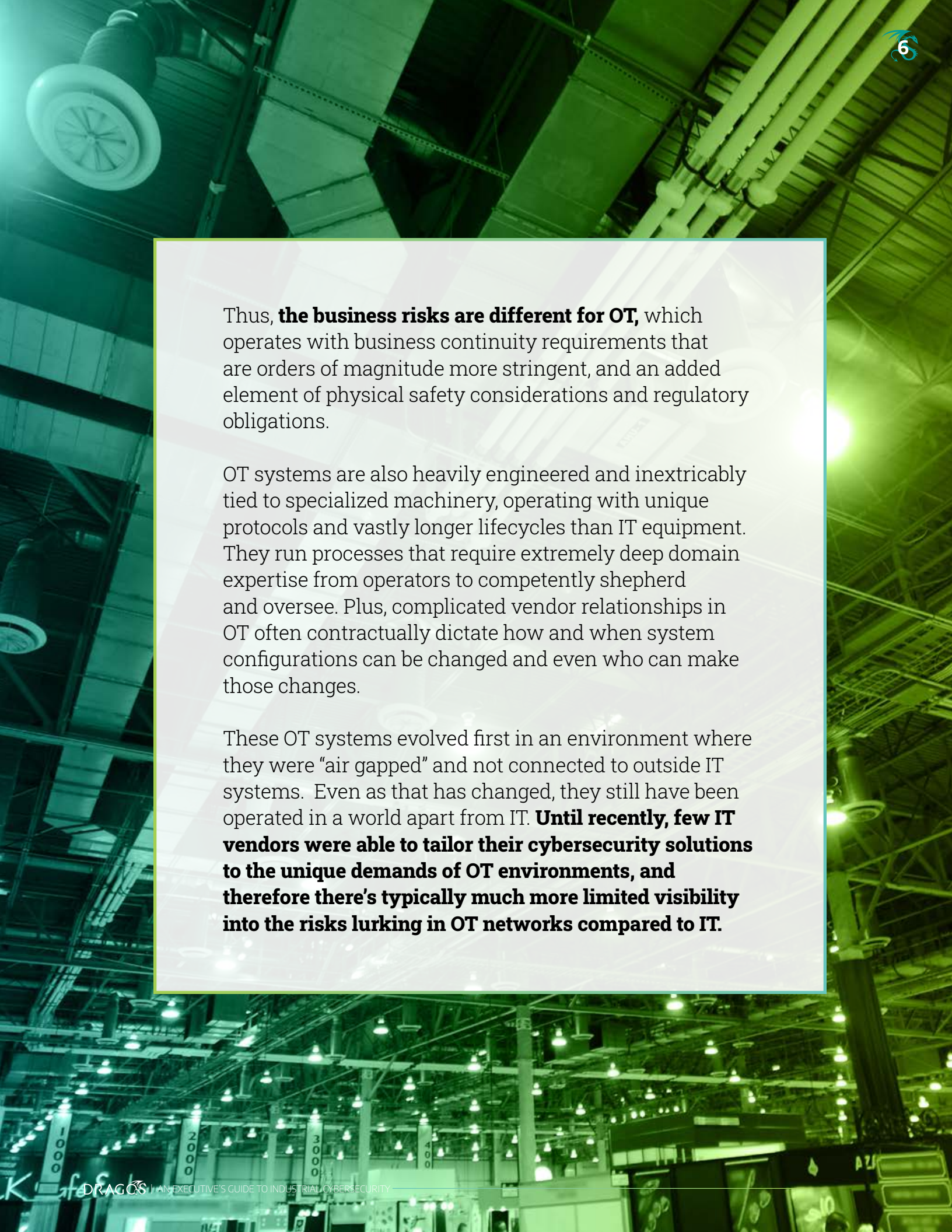
Defining Operational Technology in the Industrial Environment

Industrial control systems (ICS) and operational technology (OT) are the systems and networks that control physical processes across the enterprise. ICS/OT systems bridge the gap from the software world to the physical world.

Prevalent in industrial settings, ICS/OT systems are the ones that control physical processes including electricity generation, oil and gas refining and pipelines, automated mining rigs, and factory automation. But OT is actually present in a much broader range of use cases than that. It's crucial for operating warehousing and distribution systems, transportation lines, and even HVAC systems in data centers, large buildings, and campuses. In short,

OT is to physical systems what IT is to business systems.

Often OT and IT share similar technologies, running on similar operating systems, network connections, and digital architectures. But OT is not a direct one-to-one equivalent to its IT counterpart. OT working environments are very different than IT and are tied to the core function of the business: producing electricity, manufacturing products, transporting products, and keeping facilities open and functional.



Thus, **the business risks are different for OT,** which operates with business continuity requirements that are orders of magnitude more stringent, and an added element of physical safety considerations and regulatory obligations.

OT systems are also heavily engineered and inextricably tied to specialized machinery, operating with unique protocols and vastly longer lifecycles than IT equipment. They run processes that require extremely deep domain expertise from operators to competently shepherd and oversee. Plus, complicated vendor relationships in OT often contractually dictate how and when system configurations can be changed and even who can make those changes.

These OT systems evolved first in an environment where they were "air gapped" and not connected to outside IT systems. Even as that has changed, they still have been operated in a world apart from IT. **Until recently, few IT vendors were able to tailor their cybersecurity solutions to the unique demands of OT environments, and therefore there's typically much more limited visibility into the risks lurking in OT networks compared to IT.**

QUICK GLOSSARY

Understand the Lingo

Operational Technology (OT): The broad range of programmable systems or devices that interact with the physical environment or manage devices that interact with the physical environment. Examples include industrial control systems (ICS), building management systems, fire control systems, safety control systems, and physical access control mechanisms.

Industrial Control System (ICS): A subset of OT control systems that manage how physical components act together to achieve an industrial objective. ICS is a general term that encompasses several types of control systems that typically integrate hardware and software to monitor and control operation of machines and equipment in industrial processes. ICS is often synonymous with OT.

Industrial Internet of Things (IIoT): A loose term for the emerging class of wirelessly or cloud-connected devices and sensors in industrial environments meant to improve telemetry and control of machinery or equipment. IIoT adds more connectivity and complexity to OT environments. IIoT devices have cropped up in parallel and some have integrated with ICS systems.

Supervisory Control and Data Acquisition (SCADA): An ICS architecture that uses computers and networked communication to supervise a variety of local control modules across a large geography. It offers a non-real time view and control function and includes energy distribution/transmission, natural gas pipelines, and water distribution.

Understand the Lingo, cont'd.

Distributed Control Systems (DCS): An ICS comprised of autonomous controllers distributed through a system with no centralized operator supervisory control. DCS control loops are designed for reliability and are often real-time operations (sub-millisecond). Refineries, power generation plants, and water treatment facilities use distributed control systems.

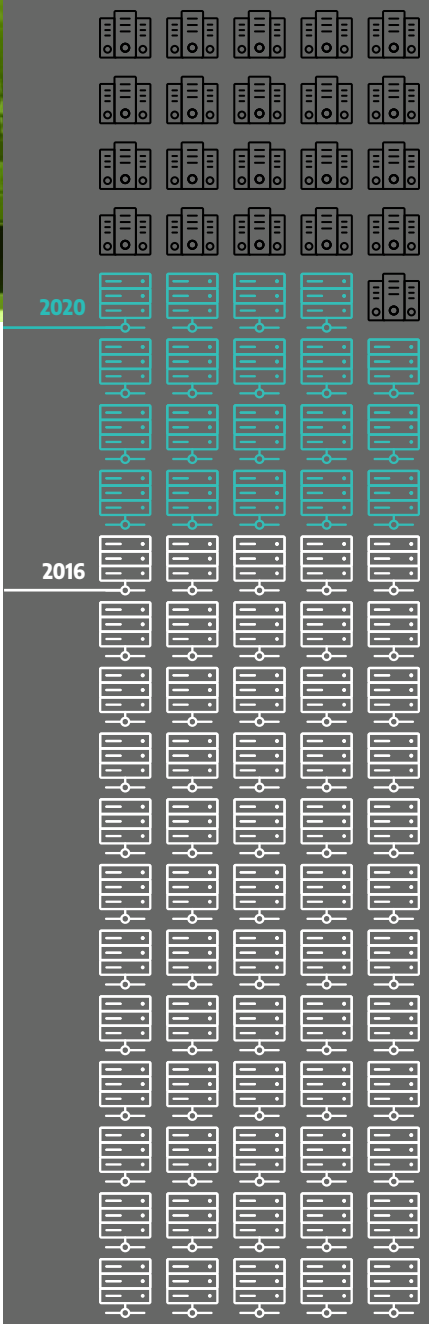
Programmable Logic Controllers (PLC): A type of ICS device, a PLC is a rugged computer used in industrial settings to directly apply logic based on input/output data. PLCs interact with sensors and actuators as part of the overall control loop and industrial process.

IT/OT Convergence: The growing integration and interconnection between IT and OT systems to improve automation and efficiency and facilitate the exchange and analysis of relevant data within industrial settings.

Purdue Model: An architecture reference model to create data flows for manufacturing environments and their connectivity to the larger enterprise. It is commonly used across many verticals and models the infrastructure into six functional levels from Level 0 to Level 5. At the bottom is the physical level of equipment like pumps, compressors, and valves at Level 0. At the top is the enterprise network equipment of Level 5. The model is often used to help visualize and conceptualize the layers of restrictions and security controls between levels of connection and traffic. This model was codified into the ASCII/ISA-95 standard.

Air Gap: An age-old term used to describe the disconnection of a device or system from a network or the internet at large. Air gaps were once the primary means of industrial cybersecurity protection. Today they're not only ineffective and outdated, they rarely exist with the rise of IT/OT convergence and digital transformation.

79 percent of global operational assets are connected to a network, up from 60 percent in 2016, according to a 2020 IDC survey of 1,014 manufacturers. Much of the remaining 21 percent of operational assets have no digital capabilities at all.
CIO Article



The Importance of OT Cybersecurity Today

As digital transformation initiatives accelerate, enterprises that depend upon industrial processes to propel their core business collectively stand at a cyber risk crossroads.

In the digital era, CEOs push their organizations to use advanced technology to increase productivity, efficiency, quality, and safety. However, the digital advancement and hyperconnectivity required to achieve those objectives opens the door to new cyber risks and exacerbates existing ones.

While IT and OT systems converged years ago using similar technologies, cybersecurity has been primarily focused on IT systems, creating an IT-OT cybersecurity gap. The reasons for this lag have been multi-faceted, as many stakeholders operated under common misapprehensions:

- that OT systems remained air gapped, or that air gaps are still sufficient,
- that physical risk management measures were enough to keep industrial systems secure,
- that cybersecurity measures always incur disproportionate operational risks, and
- that existing tools fail to address the unique nature of OT cybersecurity.

In the face of these persistent OT cybersecurity myths, digital transformation marches on, further increasing the connectedness of OT systems with the broader enterprise and internet. Consequently, OT cyber risks and exposures keep growing.

Many IT cybersecurity strategists are preoccupied with privacy concerns, diverting scarce resources from more existential risks in OT, such as risks to safety, business continuity, intellectual property, and to the company's reputation and brand.

To move forward safely and minimize risk exposure to core business functions and operational processes, organizations should seek partners to help them advance cybersecurity in lockstep with OT innovation.

> Critical infrastructure providers are being targeted by ransomware actors because, when hit with ransomware, they need to choose between indefinite suspension of critical business processes or paying the ransom.
> **Allie Mellen & Steve Turner Analysts with Forrester Research**

> The convergence of IT and OT systems is challenging many security practices to define the best security architecture that aligns with transforming and modernizing environments. The air gap is eroded for operational technology owners.
> **Barika Pace, Analyst, Gartner**

> Critical infrastructure was always designed to have the control systems isolated and physically separate from the corporate network and the internet. Initially for automation and accelerated by the pandemic, these systems are now connected to the internet. The known vulnerabilities make them an easy target.
> **Eric Cole, former cybersecurity commissioner to the Obama administration and author of the new book *Cyber Crisis***

Understanding Today's Industrial Cyber Threat Landscape

Meanwhile, industrial attacks are increasing in frequency and sophistication. Not only is there crossover from threats and attack vectors aimed at IT assets, but there exists a growing number of threat activity groups specializing in the targeting of ICS/OT environments. In its 2020 Year in Review, Dragos's threat intelligence team reported that active threats explicitly trying to gain access to ICS networks and operations are growing at a rate three times faster than they're going dormant.

The rise in OT-specific ransomware offers a glimpse into the acceleration of risk that's occurring right now in this space. In 2020 Dragos intelligence analysts observed the first evidence of ransomware designed to target ICS assets, with the frequency of attacks building over the course of the year. By the first half of 2021 the industrial world was rocked by two very public disruptions from ransomware attacks. In the past 18 months, Dragos has witnessed a range of other threat campaigns targeting industrial environments that have included:

- Watering hole credential harvesting attacks and subsequent use of valid accounts to launch intrusions in European critical infrastructure
- Initial access and reconnaissance activities across the U.S. electric sector
- Campaigns against U.S. utilities involving remote access trojan (RAT) malware
- Full compromise of a European energy organization's IT network and its Active Directory instance

> Remote connectivity to OT networks and devices provides a known path that can be exploited by cyber actors. External exposure should be reduced as much as possible.
> **US Cybersecurity & Infrastructure Agency (CISA)**

Executives should understand that **a lot of the OT adversary behavior today is focused on quiet prepositioning and reconnaissance work that wouldn't be evident without the right visibility in place.**

Industrial adversaries often build programs and campaigns slowly over time, with later campaigns being more successful and disruptive due to previous efforts. Many threats tracked by Dragos analysts may not induce headline-causing disruption, but they often lay the groundwork for evolving into future attacks with potential to be disruptive and destructive.

How OT and IT Security Differs

Many cybersecurity risk management patterns and practices are relevant across both OT and IT domains. The ideas of limiting risk exposure by reducing attack surfaces and hardening configurations around crown jewel assets, for example, hold just as true in OT environments.

However, many fundamental differences materially impact cybersecurity strategy and execution in the OT world. Effectively managing cybersecurity risk in OT environments requires recognizing some key differences.

Risk profile is different: The highest risks posed by OT vulnerabilities tend to be the ones that threaten the availability or integrity of systems rather than the confidentiality of data they deal in. While IT is often consumed by privacy and data breach concerns, the thing that keeps OT operators up at night is disruption or malfunction of systems that could threaten the business or even people's safety.

Strategy and approach are different: The consequences of both security incidents and downtime caused by security measures inappropriate for OT run far deeper than for IT systems. While still possible in IT, an OT attack could more easily impact the brand, stock price, and revenue generation. But it is simply not feasible to pause operation of a hydroelectric dam, or a continuous process in a manufacturing facility to implement security controls or patch operating systems. Additionally, strict safety regulations add additional constraints in how systems can be handled.

Technology is different: OT systems use different protocols, fit-for-purpose hardware and software with configurations unique to each organization, arcane embedded technology, and a diverse range of endpoints—many of which run unsupported versions that cannot be changed due to the operational risk. Legacy systems are entrenched when the lifecycle of expensive OT machinery is measured in decades rather than years.

Approaches to vulnerabilities and patching are different: For many OT and ICS systems, there's no such thing as weekly or monthly maintenance windows where administrators can easily push through a patch. In many cases, vulnerabilities deep within the ICS environment are better resolved with mitigations focused on network configuration changes versus patching. Additionally, the traditional active scanning approach used to detect vulnerabilities in IT systems could lead to major process disruptions in OT environments.

Required skills are different: The distinctive nature of OT systems means that operators must come to the table with a set of extremely specialized domain expertise in process management and engineering. This means security teams will need to be especially careful to work closely with the specialists to coordinate security execution.

Stakeholders are different: With the business stakes so high, OT cyber risk management is an organization-wide activity. The CISO plays a pivotal role as risk advisor but the risks are owned by each business unit lead and, ultimately, the CEO and board of directors. Planning and strategy must be done with constant collaboration with all the relevant stakeholders, particularly operations engineers with specialized expertise in keeping OT equipment running and maintaining complex ICS vendor relationships.

Next Steps for Assessing and Addressing the Risks

Because of the unique nature of OT security, an industrial cybersecurity program can't be a copy-and-paste of the IT cybersecurity program. ICS environments need cybersecurity strategies and tools tailored specifically to the different missions, challenges, and threats faced by industrial organizations.

Make an OT Cybersecurity Roadmap: Effective industrial cybersecurity programs tend to be driven by threats and consequences to OT assets—prioritized by the business value of the asset and the likelihood of a given attack scenario.

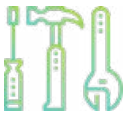
Ideally an organization should be able to gain visibility, control, and minimum cybersecurity hygiene across the entire OT environment, but that takes time and money. In order to develop a solid cybersecurity roadmap that can incrementally phase in good cybersecurity practices, organizations should start first with a discovery process that gathers input from the board, executive stakeholders, and asset owners on the highest business priorities tied to OT processes and then survey the environment to understand all the OT assets in place and how those map to high-priority processes.

The team then identifies and ranks the OT assets involved, based on business importance. From there the team should chart out the threat-driven and consequence-driven scenarios most likely to impact high-priority assets:

Threat-driven: Threat-driven scenarios are those which threat intelligence reports have shown to impact organizations like yours.

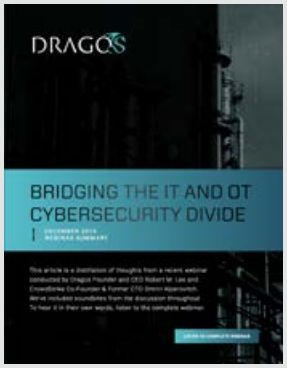
Consequence-driven: Consequence-driven scenarios are constructed by moving backwards from the worst consequences of an attack that you would want to avoid in high-priority ICS environments, and sketching out the common attack techniques that could be used to trigger them.

With these scenarios in mind, the team should examine existing controls and how they stack up against the tactics, techniques, and procedures (TTPs) used by attackers in each situation. Use this to identify gaps compared to an ideal set of controls and this provides the basis for setting out a roadmap. Don't try to boil the ocean, break it down into a multi-year plan for continuous improvement, prioritizing coverage and speed of investment based on that asset ranking gleaned from the stakeholders.



Get the Right Tools: Many IT detection and monitoring tools don't translate well to ICS environments. Often IT detection tools simply don't interface well with OT systems or are impractical when placed within an ICS environment. For example, endpoint protection won't work for PLCs.

RESOURCES FOR GETTING STARTED



WHITEPAPER >>
Bridging the IT-OT Security Divide

COMPREHENSIVE GUIDE >>
Industrial Cyber Risk Management: A Guideline for Operational Technology

WEBINAR >>
Developing a Strategic ICS/OT Cybersecurity Roadmap Using Intelligence- and Consequence-Driven Analysis

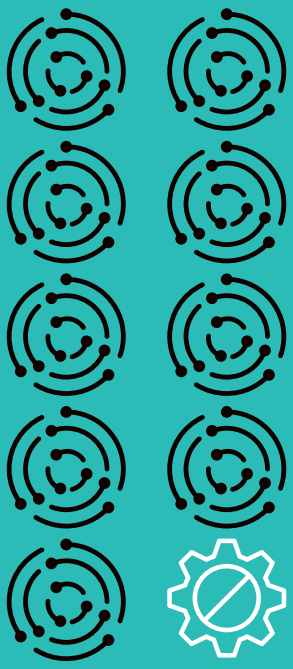
What's more, the detection mechanisms and output are all based on IT-focused threats, so the context and correlation of what matters to OT operators will be missing. The machine learning models are not useful in ICS environments, since they were designed and tuned for IT. Dragos experts are repeatedly called to incidents where they've found that Windows AV destroyed ICS applications because they looked odd to heuristics engines unaccustomed to the way ICS functions operate.

This is why an organization will need OT-specific cybersecurity tooling that can support the management of risks that matter most in industrial settings.

Skill Up: OT cybersecurity is a specialized endeavor. While the enterprise cybersecurity team may be able to take the lead on strategic planning—with heavy OT stakeholder collaboration—and even shoulder some of the day-to-day work, the team will need additional resources to execute on a plan. For many organizations, the best way to quickly build up the requisite skills will be by leveraging partners and third parties to bridge internal gaps, for example by putting a firm on retainer for rapid incident response.

The conversation should be 'We've all bought into this together.' You tie it to the business problem. Instead of it being some ephemeral problem, it's based on real scenarios that either the threats have shown you or your people are concerned about, and so you're able to present real information to the executives.

Robert Lee, CEO, Dragos



Because of board-level mandates on security risk, by 2023 90% of all industrial companies will develop IT-driven OT security governance to support rapid innovation by engineers through connected assets

IDC Research report

Partnering with Dragos Industrial Cybersecurity

Building and maturing an effective OT cybersecurity program requires long-term investment in resources and expertise. There's no replacement for dedicated OT cybersecurity staffing, but the right technical and professional allies can help you more quickly scale and mature processes.

With a team comprised of some of the foremost experts in ICS/OT cybersecurity, Dragos arms industrial defenders around the world with the knowledge, tools, and expert resources they need to protect OT systems as effectively and efficiently as possible. Dragos can provide organizations help on numerous fronts, including:

Technology: Built by OT cybersecurity practitioners for practitioners, the Dragos Platform provides teams with visibility into ICS/OT assets and their vulnerabilities, in the context of current threat conditions, with best practice guidance for responding to incidents before they become significant compromises.

Threat Intelligence: Backed by a world class team of ICS cybersecurity analysts, Dragos Threat Intelligence provides organizations with in-depth visibility of threats targeting industrial environments globally.

Professional Services: With a deep pool of OT engineering and cybersecurity practitioners, the Dragos Professional Services team can help organizations at all stages of maturity respond to immediate incidents, conduct architecture and vulnerability assessments, hunt for threats, establish technology roadmap and response plans, and conduct tabletop exercises.

Managed Services: Dragos's managed ICS/OT network visibility and threat hunting service helps organizations extend existing security operations center (SOC) capabilities without hiring an internal army of security pros with OT expertise. Dragos OT Watch provides access to an elite team of analysts who can help organizations reduce mean time to discovery and enhance situational awareness.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more at **Dragos.com**