KPMG

IT/OT convergence

Efficiency and cybersecurity in the energy and natural resources sector

December 2021

KPMG in Saudi Arabia

Table of contents

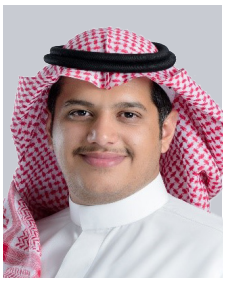
Introduction

Information technology (IT) and operational technology (OT) environments have traditionally assumed distinct roles in industrial organizations. Separated both in purpose and in practice, IT and OT also differ in their culture and their norms around security and efficiency.

However, as new technologies are introduced to the OT environment it is becoming necessary for the two environments to be converged. Without convergence, the new technologies and the data gathered will be vastly underutilized — making it difficult to justify the investments needed to modernize OT environments. Convergence requires organizations to bridge the gaps between IT and OT environments' people, processes and systems and to build a smarter, more secure network with high visibility to monitor and control both environments.

This paper considers the challenges and opportunities and presents a toward better convergence of people, systems and strategies between these two functions of an organization in the energy and natural resources sector.

Ton Diemont
Head of Cybersecurity & Data Privacy
KPMG in Saudi Arabia



Hossain Alshedoki
IT/OT Cybersecurity & Data Privacy
ENR Lead
KPMG in Saudi Arabia

Starting from behind

Transformational change is not just about execution or follow-up but is also about preparation. IT/OT convergence requires the right preconditions—in both an organization's environment and culture—to be successful and lasting.

Though some of the world's most successful industrial and energy and natural resources (ENR) companies are well along the path of IT/OT convergence, many of their smaller or less ambitious peers are not. Each in their own way, systems, people and strategy are holding them back from starting or are limiting their progress with IT/OT convergence.

Systems

OT systems are usually quite a bit older than IT systems due to their capital-intensive nature and safety protocols that prefer consistency to change. Newer OT environments are, in the most part—by design—already prepared for convergence. These systems can support full automation and remote monitoring and IoT devices can easily be integrated.

Taken alone, system age is not necessarily a hindrance to IT/OT convergence. An OT environment can be upgraded to support automation, monitoring and IoT devices. However, OT systems that use outdated equipment or are only patched on a minimal level are not secure. Many organizations don't secure these systems because of a desire to separate them from the internet and other networks. Securing OT systems is a prerequisite to IT/OT convergence. Cybersecurity capabilities need to be implemented to evaluate existing systems for threats and to continually monitor them in the future.

Another system prerequisite for IT/OT convergence is separation. This may seem counterintuitive, but if an IT and OT architecture are clearly separated prior to convergence, their eventual integration will be easier to conduct. It is critical this is done at the beginning of the convergence project execution lifecycle rather than midway through it.

People

Preparing an organization's people and culture for IT/OT convergence is critical for success. In fact, it is often the first step.

Building a strategy for convergence should start at the top. Unfortunately, simply bringing the idea of IT/OT convergence to the board room is a struggle for some companies. When the long-term benefits of convergence are not fully understood, it is difficult for its proponents to articulate the need for convergence to management or the board.

Poor understanding also results in inaccurate evaluations of return on investment (ROI). To remedy these difficulties, it is important for organizations to include both IT and OT administrators in the evaluation of an IT/OT convergence proposal. At industrial companies, too often are IT administrators left out of these conversations.

In the same vein, COOs' opinions are often heard before CIOs' opinions at industrial organizations. However, both executives have important contributions to make towards the planning of an IT/OT convergence strategy. Thus, for organizations hoping to explore IT/OT convergence, CIOs should be empowered on management teams and in board rooms and not be seen as a second fiddle to COOs.

Cybersecurity should be integral to an IT/OT convergence project from its inception. Responsibility for IT/OT convergence cybersecurity will often fall on a CISO. In many cases, CISOs are brought into a convergence project in the middle or even late stages, which can mean systems and processes are not integrated securely. When CISOs are included in the planning stages, they can identify the areas most vulnerable to threats and develop the plans to secure them early on.

Strategy

A good practice for organizations considering IT/OT convergence is to clearly define what use cases they want to solve by converging environments. Do you want your systems to operate more efficiently, deliver faster insight to leadership on production data and analysis, or do you want to improve maintenance and servicing of equipment?

If organizations fail to define clear objectives for IT/OT convergence, they may also fail to implement the right processes and tools for their specific environment or they may end up with diffuse goals that cannot be accomplished. Both outcomes diminish the effectiveness of convergence and will reduce long-term morale and buy-in around convergence.

However, in defining a convergence strategy and deliverables, organizations should allow for flexibility. Especially within the cybersecurity realm, threats and protections are rapidly evolving—this should be addressed by baking flexibility into your strategy. Easier said than done, but finding a middle ground allows for adaptation when inevitable difficulties are encountered while also maintaining clear project goals and timelines.

Process and workflow convergence

Process and workflow convergence are integral to a broader IT/OT convergence plan. Introducing new technology to a converged system without adapting processes and workflows to the new system will not deliver the desired business benefit. Thus, before organizations can begin converging processes, it is important to recognize the reasons why IT and OT processes are different. Once the "why" is identified, an organization can look at how processes can be converged without compromising the effectiveness or safety of an individual IT or OT process.

IT and OT processes and workflows have always been different—for good reason.

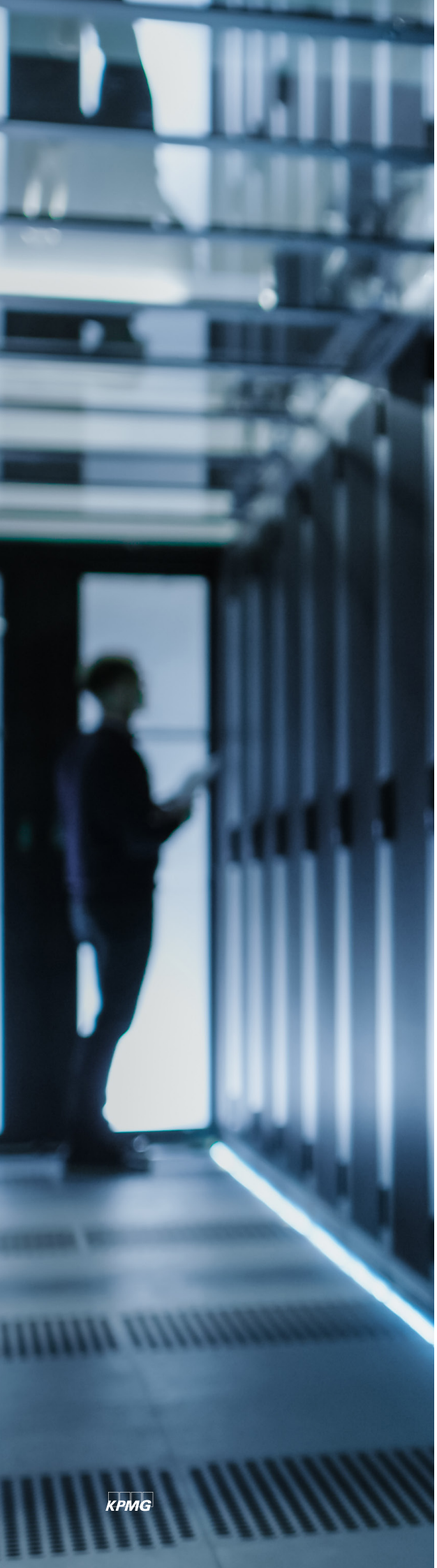
Underlying nearly every OT process is safety. Consistency is safety's best friend, and as such, OT systems favor legacy systems and processes—change is rare in applications and infrastructure and there must be a good reason to do so. IT processes are quite the opposite. To achieve greater process efficiency or to adapt to evolving risks, IT processes encourage updates and adaptation.

Both of these philosophies support cybersecurity in their own way. IT processes can be secure because they are constantly upgraded to address vulnerabilities as they emerge from the wild and use new cyber defenses. OT processes can be secure due to their strict adherence to procedures and ruthless control of change.

Before entering a converged environment, both IT and OT cybersecurity processes and workflows need to be adapted. A great deal can be learned from one another.

Stricter attitudes towards processes and a culture of safety—hallmarks of the OT environment—should be adopted within IT. Now that their work is more directly integrated with manufacturing or production systems—and the humans physically operating them—IT administrators need to recognize the elevated stakes associated with cybersecurity. The resulting cultural change within IT should better prepare IT processes and workflows for convergence.

On the other hand, OT processes and workflows should be adapted to fit a more regular schedule of updates. This approach is necessary to support cybersecurity in a converged environment that contains more connected devices and potential vulnerabilities. IT administrators are acquainted with this approach and their expertise should be utilized when designing new OT processes, systems and capabilities to support convergence.



OT processes and workflows can be prepared for convergence—and supported during and after convergence—by an OT security center for excellence. A center for excellence is important for training OT administrators and engineers to protect critical infrastructure as new vulnerabilities are introduced in IT/OT convergence. Administrators can learn through hands-on cybersecurity exercises that replicate real-world risks. In turn, these engineers can tailor their workflows around a new understanding of cybersecurity in a converged environment.

Management- and board-level thinking

People—rather than systems or technologies—may be the most important factor for IT/OT convergence success. However, while much attention is paid to the actual practitioners of IT and OT systems—those with their hands on the physical levers—often lost in the conversation is the people at the top of an organization: those at the management- and board-level.

In addition to determining an organization's budget or goals, a management team and board determine culture. Two key aspects to a culture that supports IT/OT convergence are understanding and open-mindedness. Though these may sound better suited for marriage counseling than for an industrial operation, they are practical for both.

Better understanding of each other's systems and processes is critical for preparing IT and OT teams for convergence. Such understanding will improve both the efficiency and safety of newly converged processes like data transfer and system monitoring.

Open-mindedness—to one's IT or OT counterparts—will ease the acceptance of new shared protocols or processes resulting from IT/OT convergence. If administrators are aware of the unique needs of an IT or OT system, they are more likely to buy in to the plan and accept compromises to how they think the operation should be run.

There are also some more practical steps organizations can make to their management team and board to support IT/OT convergence.

The CIO does not sit on the board for many industrial organizations. This fact is a relic of an old way of thinking—that operations trump all, especially IT. This broadly needs to change, but especially needs to change for organizations preparing for IT/OT convergence. IT needs to have a seat on the board so that their needs and insights are addressed for convergence plans.

This approach can be applied more broadly to management with a "leveling" of opinions and responsibilities. The COO's opinion at an industrial organization should not necessarily be more important than that of the CIO. CFOs should fully understand the risks and benefits of IT/OT convergence so that their decision-making supports the effort. Full management buy-in is only possible when everyone's opinion is valued.

Distributing responsibilities between IT and OT

Somewhat counterintuitively, a key for IT/OT convergence success is to know which processes to keep separate. Within this, distributing cybersecurity responsibilities between IT and OT teams is critical to ensuring convergence doesn't make an organization more vulnerable than before.

CISOs have become increasingly important for industrial companies. However, within large, diverse organizations CISOs' differing responsibilities for different divisions can become burdensome and can even be dangerous if their holistic remit prevents separation of cybersecurity responsibilities. A way to avoid unnecessary vulnerabilities resulting from an overstretched CISO is to have two CISO-like roles—one each for IT and OT—in addition to an executive CISO to which they both report. The benefit of having an IT CISO and an OT CISO is to support a cybersecurity separation strategy meant to prevent a cyberattack moving from the IT to the OT environment (or vice versa).

A two-CISO strategy is illustrative of a broader strategy to distribute cybersecurity responsibilities in a manner that prevents attacks moving from one environment to another. The administrators responsible for the IT firewall should not also be in charge of OT's firewall. This makes sense on a practical level—two teams of administrators better separates systems and controls—and on a philosophical level—using one line of thinking to create and maintain two firewalls leaves a system more "hackable" than using two lines of thinking.

A prerequisite for effective distribution of cybersecurity responsibilities is complete asset visibility. The ability to monitor assets means first getting and maintaining visibility of critical assets, then using risk-based methods when planning and implementing protective security monitoring.

Enhancing capabilities

Broadly-tested reference architectures as well as more-specialized solutions relating to data management and storage can enhance an organization's IT/OT convergence efforts.

Network security reference architectures and Zero Trust

Establishing a reference architecture for network security during IT/OT convergence will yield a multitude of benefits. Reference architectures help all stakeholders collaborate and communicate effectively throughout a process—a notoriously tricky task between IT and OT teams. With a reference architecture in place to anticipate network security questions that may arise—and provide objective guidance to answer them—the subjective differences in opinion between IT and OT will be minimized.

ISA/IEC 62443 standards can be a valuable resource for organizations undergoing IT/OT convergence. The standards address security issues unique to connected OT systems.

Among the security-related convergence tasks that IEC 62443 addresses are:

- OT cyber risk assessments
- Building cybersecurity management teams
- Patching and other protective controls
- Segmenting and securing network zones and conduits
- Creating processes and governance
- Establishing appropriate roles and responsibilities for users or resources

Additionally, choosing and managing the right connected devices for a unique OT system is important for securing networks for IT/OT convergence. IEC 62443 addresses this and provides guidance to improve existing processes for technology project scoping, vendor selection and procurement. It also contains a set of prescriptive requirements and processes for secure product development lifecycles fit for a connected OT environment.

Traditional approaches for securing OT networks have long been dependent on maintaining the separation of industrial applications from IT networks. However, for organizations undergoing IT/OT convergence, traditional separation approaches are not sufficient.

Zero Trust takes traditional separation approaches to a much more granular level. Rather than building a wall around the OT network, it assumes that every user, device, system or connection is already compromised (by default) whether they are inside or outside of the network. The goal of Zero Trust is to reduce the attack surface and prevent lateral movement with segmentation or micro-segmentation. If a breach occurs, then an intruder can't easily access other systems or sensitive data by moving laterally.

Data management

One of the greatest benefits of IT/OT convergence is the generation of previously untapped data. These data can be used to enhance the efficiency of an operation, increase security or conduct predictive maintenance—just to name a few benefits. However, without effective data management practices, much of these data's value is unrealized.

While many organizations manage their data by sending it to the cloud for storage or processing, this method does not allow organizations to tap into the full potential of IIoT capabilities. Processing a large amount of data directly in the could requires large response times and a large amount of bandwidth. An alternative solution is edge computing.

Edge computing brings data storage and processing closer to the sources of data. Edge computing processes happen on the floor of an industrial facility, meaning only some data needs to be send to the cloud for long-term storage or distribution to a different network. Bringing analysis closer to home improves response time and bandwidth consumption. It also decreases data distribution and the inherent risk of that data being stolen or damaged during data transfer.

Data management should also encompass security. In addition to data storage and processing methods like edge computing, practicing selective sharing ensures that data is accessed only as they should be. Specific data might flow one way, back and forth, or not at all. Limiting the flow of data makes it less vulnerable to threats.

Evolving cybersecurity risk factors

The OT security paradox

OT systems — rather than IT systems — are usually carrying an organization's most critical business processes. Thus, OT system downtime can be more costly for an organization than IT system downtime. Logic therefore suggests that OT system security should be more important for a business than IT system security.

However, the paradox is that most companies invest a lot more money into securing their IT systems than into securing their OT systems. This investment paradigm doesn't necessarily need be flipped, but a more balanced approach to cybersecurity planning and investment needs to be taken during IT/OT convergence.

IT/OT convergence improves cybersecurity

IT/OT convergence allows for broader monitoring and threat detection. Prior to convergence, organizations will likely have a limited view into the architecture and services running on their OT system. Convergence with IT allows for passive monitoring and vast data gathering. In analyzing these data, profiling techniques can be used to learn more about the tendencies of a system. Once data patterns are better understood, abnormal behaviors can be quickly detected with no interruption to the industrial process.

Broader data gathering has benefits beyond threat detection. New datasets can be fused with data sets from other systems across the OT system — like CCTV or building management systems — to allow for more holistic monitoring and better utilization of data.

Factory maintenance can also be improved through IT/OT convergence. Most organizations rely on preventive maintenance to decrease the likelihood of system downtime and costly repairs. IT/OT convergence allows organizations to shift from preventive maintenance to predictive maintenance. Predictive maintenance technologies gather real-time data from OT systems and can spot situations that might lead to equipment failure. In doing so, targeted repairs can be made prior to failures — a method that is often less-costly than preventive maintenance, which takes a broader approach to repairs.

Organizations must bear in mind that the cybersecurity advantages of IT/OT convergence are limited by the type and age of an organization's OT system. Older SCADA systems often don't allow for the broader monitoring, threat detection or data gathering that is necessary to build a more secure ecosystem. OT systems that employ more IoT and connected devices have the access points for monitoring and data gathering and are thus more suited for the cybersecurity benefits of IT/OT convergence.

IT/OT convergence can open cybersecurity vulnerabilities

While IT/OT convergence can allow for more robust cybersecurity, it also exposes industrial control systems (ICS), process control systems and other operational technology to malware attacks, hacktivism, employee sabotage and other security risks that previously affected only corporate IT systems.

IT/OT convergence involves integrating IP-connected devices to an OT system. These additional access points make an OT system more vulnerable to internet-based threats. Many of these connected devices use consumer-grade technology and are from multiple vendors — both qualities that make them susceptible to cyberattacks.

Often the trickiest management aspect of IT/OT convergence is organizational change. Systems don't have opinions — people do. The knowledge and cultural differences between IT and OT employees can result in vulnerabilities that can be exploited by cyber attackers. One of the key differences between the IT mindset and OT mindset is the reluctance to or acceptance of system upgrades. While IT administrators constantly update their systems for optimization and security, OT admins are more likely to stick with legacy systems because of their reliability.

A mindset clash between IT and OT administrators can lead to poor system integration. This results not only in sub-par IT/OT convergence outcomes, but also in system vulnerabilities.

Vulnerabilities created by hosting different OEMs in a single environment

Managing multiple original equipment manufacturers (OEMs) in a single environment is difficult from an operational perspective because most OEMs' systems were not designed to work optimally with systems from different vendors. Such system idiosyncrasies can also impact the safety of an environment. System administrators resultingly need to identify vulnerabilities and patch where necessary.

In a system containing devices and subsystems from multiple OEMs, it is crucial for an organization to define and limit the paths for data transfer. Data transfer is crucial for successful IT/OT convergence; without it, systems will be poorly integrated and convergence will not yield the desired system optimization. However, data transfer should be limited to paths where it can be useful. If two devices — especially from different OEMs — have no need to transfer data, they should not.

There are, however, differences in opinion about the safety of hosting multiple OEMs in a single environment. Some administrators see multiple OEMs as a protection against attackers moving easily from one system to another. Having a single OEM, in their opinion, leaves an organization vulnerable to having their entire environment compromised.

Mitigating zero-day attack risks during and after IT/OT convergence

By virtue of their definition, zero-day attacks are impossible to predict. They are, however, possible to defend against. In converging IT and OT systems, an organization is turning a closed environment into an open environment. This creates new vulnerabilities to zero-day attacks that need to be addressed.

Micro-segmentation is one practice employed by organizations to mitigate the impact of a successful zero-day attack. In a converged IT/OT environment, traditional security controls such as virtual LAN systems (VLAN) are insufficient protection from a zero-day attack. Micro-segmentation provides a more targeted control over network traffic by further partitioning the VLAN and adding security for each partition.*

Further, micro-segmentation can be tailored to a specific operating environment and for specific types of network traffic. This allows for the limitation of certain traffic without significantly minimizing the optimizing benefits of IT/OT convergence.

On a fundamental level, organizations can mitigate zero-day attack risk by implementing 'resilient by design' principles before IT/OT convergence. Instituting resiliency in your organization's people, processes and systems prior to convergence will also minimize the impact of a zero-day attack if it occurs.

* https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-securing-ot-networks-with-microsegmentation.pdf

OT/ICS cyber range labs

Simulating a cyberattack in an OT environment is a difficult process. While many IT cybersecurity professionals are well-versed in methods like penetration testing and red teaming to test the strength of their cyber defenses, OT cybersecurity professionals struggle to find widely-used practices to simulate OT cyberattacks.

In an effort to bring OT simulation efforts up to par with IT, KPMG has created OT/ICS cyber range labs using production grade equipment to simulate scale-model versions of industrial processes. The labs can be used to establish secure remote connections through KPMG's infrastructure to perform:

- Hands-on training sessions
- Cyberattack simulations
- Proof-of-concepts (PoCs)
- Industrial cybersecurity-related research

Lab simulation examples:

1 Artificial lift (oil & gas)

A production scale model of an artificial lift set up designed with a progressing cavity pump (PCP), is measuring multiple operational variables such as: pressure, flow and temperature.

2 Oil treatment plant

A narrowed version of a treatment plant, where the crude is processed and separated from the gas, and send them gas processing plants and refineries.

3 Gas-fired power plant

A simulated gas-fired power plant, which reproduces the activation of the turbine vanes caused by the influx of gas injected from the gas processing plant output pipeline.

Industrial multi-vendor ecosystem with production-grade equipment and vurtualized systems commonly used in the major industries.

No two industrial environments are exactly the same. Resultingly, training is often hyper-specialized for an organization's specific set of OT environments and systems. In the virtual environment, KPMG's OT/ICS labs can be tailored to match the specific training needs of an industrial operation as KPMG globally has invested and built different labs in Americas, European Union, Singapore and Saudi Arabia where each one of them is designed to target a specific industrial process.

KPMG's virtual labs can be built to replicate an organization's IT and OT environments by connecting proprietary devices and virtualizing OT components. This enables IT and OT professionals to cross-train their incident response strategies until mastery.

Lab use cases:

1. OT cybersecurity hands-on training sessions:
Labs can be used to perform online training sessions with production-grade equipment to learn OT/ICS cybersecurity concepts. Trainees will become acquainted with performing their daily tasks in a cybersafe way.

2. OT cybersecurity tool demos
Hands-on demos of cybersecurity tools help OT employees better understand the technical capabilities of the tools and to evaluate their use in multiple scenarios.

3. OT cyberattack demos
In the labs, multiple cyberattack scenarios can be applied to the industrial environment to show how OT assets function when crippled. The scenarios help show vulnerabilities and what equipment might be compromised in an attack.

4. OT cybersecurity remediation testing
Prior to implementation of a cybersecurity remediation plan, labs can be used to perform testing procedures to review the effectiveness and reliance of a workaround in a similar architecture.

Contacts

Ton Diemont
Head of Cybersecurity & Data Privacy
KPMG in Saudi Arabia
E: antondiemont@kpmg.com

Hossain Alshedoki
IT/OT Cybersecurity & Data Privacy ENR Lead
KPMG in Saudi Arabia
E: halshedoki@kpmg.com

Contributors

David Ferbrache, Head of Global Cyber Futures, KPMG in the United Kingdom
Dimitrios Petropoulos, Partner, Head of Cybersecurity & Data Privacy, KPMG Lower Gulf
Ronald Heil, Global Cyber Lead and ENR Partner, KPMG in the Netherlands
Dani Michaux, EMA Cyber Leader and Partner & Head of Cybersecurity, KPMG in Ireland
Walter Ariel Risi, Global Head of IIOT/OT Cybersecurity, Partner, KPMG in Argentina
Jason Haward-Grau, Managing Director, Cybersecurity Services, KPMG in the United States
Pablo Almada, IIoT/OT Cybersecurity Partner, KPMG in Argentina
Peter Bannink, Thought Leadership Lead, KPMG in Saudi Arabia

kpmg.com/sa