KPMG

# A pathway to industrial cyber resilience

**Assessing and bracing against cyber vulnerabilities in industrial sectors.**

KPMG International

home.kpmg/cybersecurity

# Foreword

Cyber security is being tested in bold and unprecedented ways as the frequency, sophistication and devastating impact of cyber-attacks increase worldwide. As businesses in every sector race toward solutions, industrial organizations in the energy and natural resources sector are facing their own harsh reality as they recognize their lack of preparedness — and the potentially catastrophic consequences they now risk.

The cyber security threat to industrial operations has evolved and rapidly expanded over the last year. The Colonial Pipeline ransomware attack saw hackers take down the largest fuel pipeline in the US, leading to major fuel shortages in May 2021 and forcing the company to pay a ransom demand of USD4.4 million. According to the cyber security firm responding to the incident — considered the largest cyber-attack on a US infrastructure target to date — the attack was the result of a single compromised password. Hackers breached Colonial's business systems through a virtual private network account that gives employees remote access to the company's computer network.[1]

A number of factors, including a shift to remote work for engineering, production-line and maintenance activities — combined with inadequate digital capabilities — have contributed to the alarming sector-wide trend. And public awareness of the threat is growing in the wake of the Colonial Pipeline breach and its disruptive impact on businesses and consumers. Public calls for action rang loud following the attack.

Unfortunately, amid the growing threat and rising public pressure for solutions, industrial organizations remain largely unprepared to effectively manage and respond to today's fierce threats. Organizations may be facing a paradox of choice. While the cyber security industry is providing an array of solutions to global markets, many are relatively new and sometimes untested. As a result, many organizations appear confounded by potential solutions and thus are delaying action on the security innovations they inevitably need to make.

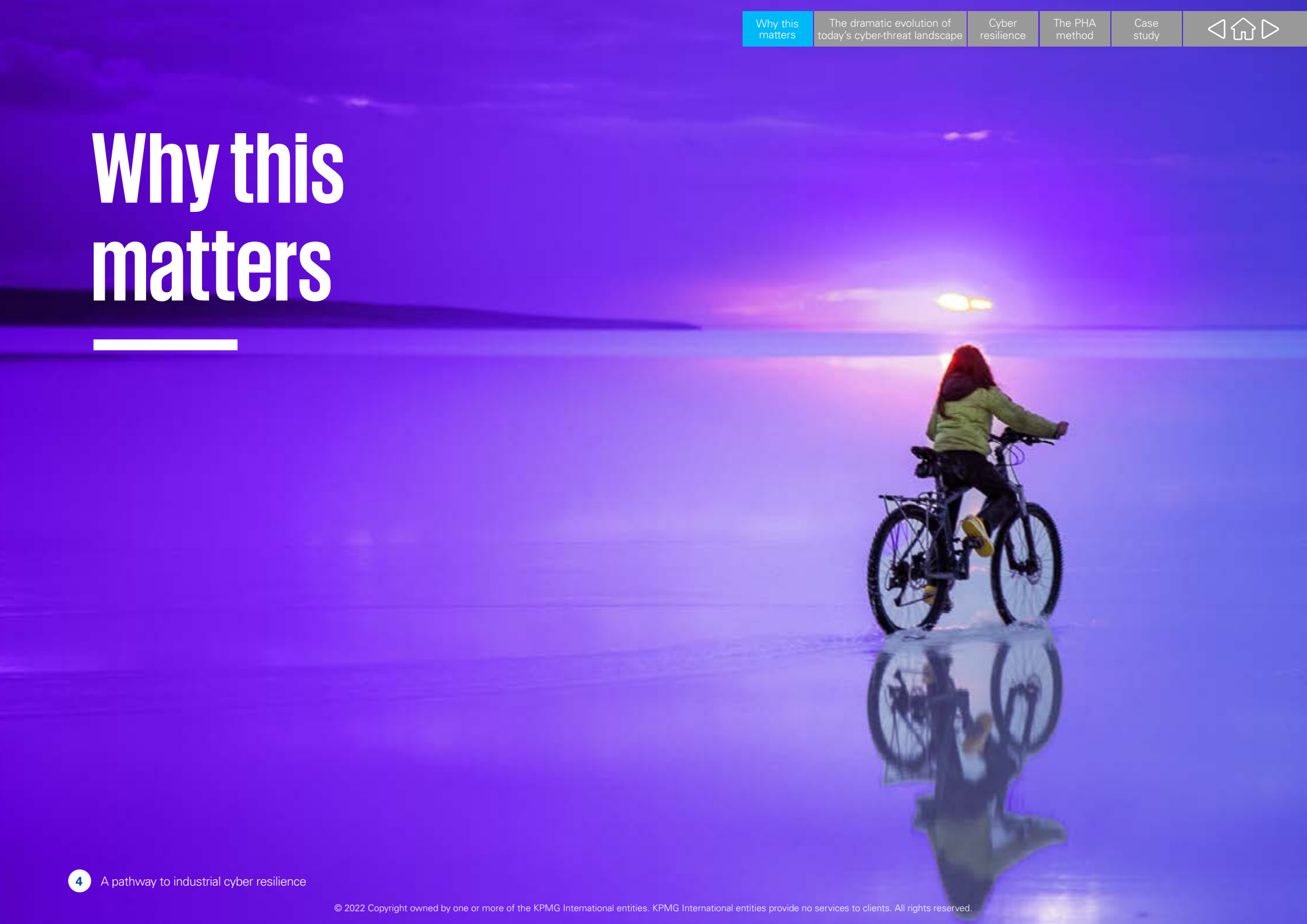
This publication reviews the current threat landscape and presents guidance on how to be better prepared for today's potentially costly and destructive threats. Core to the recommendation of this paper is the cyber-process hazard analysis (PHA) as a toolset for industrial organizations.

[1] William Turton and Kartikay Mehrotra, "*Hackers Breached Colonial Pipeline Using Compromised Password*," Bloomberg online, June 4, 2021.

# Contents

Click on the topics to learn more.

# Why this matters



A number of studies suggest that business and government leaders recognize today's industrial cyber threats but are not yet prepared to fend them off. While cyber-attacks are often cross-border and the threat to industrial companies is global, geopolitical realities and the concentration of industrial activity in certain parts of the world have made threats more acute in some countries.

The numbers are staggering. Ransomware attacks on operational technology (OT) networks soared five-fold from 2018 to 2020. Out of these, manufacturing entities comprised more than one-third of confirmed ransomware attacks on industrial organizations, followed by utilities, which made up 10 percent.[2]

The estimated global cost of these ransomware attacks? It too has skyrocketed and is predicted to reach USD20 billion in 2021 — up from USD325 million in 2015.[3] Operational disruption due to ransomware in OT environments has seen a 23-fold increase. In 2020, there was a 32 percent increase in ransomware attacks against energy and utilities organizations.[4]

Adding to the bad news for the sector, of course, is the fact that ransomware attacks continue to grow in sophistication. Additionally, attacks have increasingly targeted industrial control system (ICS) environments like oil-and-gas and manufacturing.

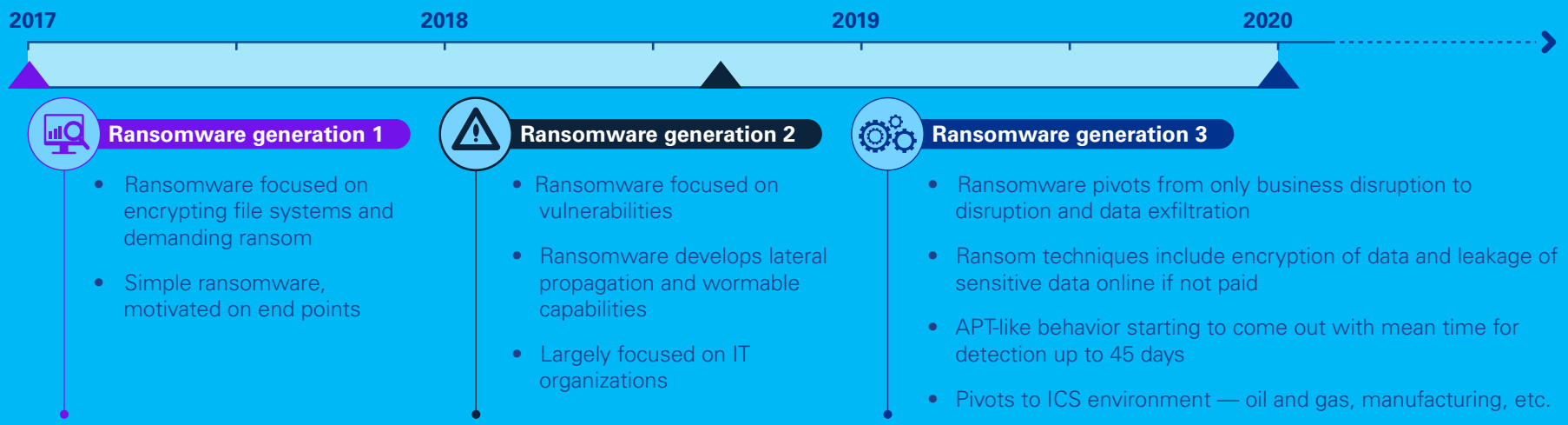
[2] Ransomware in ICS Environments, Dragos, December 2020.

[3] Global ransomware damage costs predicted to exceed $265 billion by 2031, Cybersecurity Ventures, June 3, 2021.

[4] Claroty Biannual ICS Risk & Vulnerability Report: 1h 2020, Claroty, 2020.

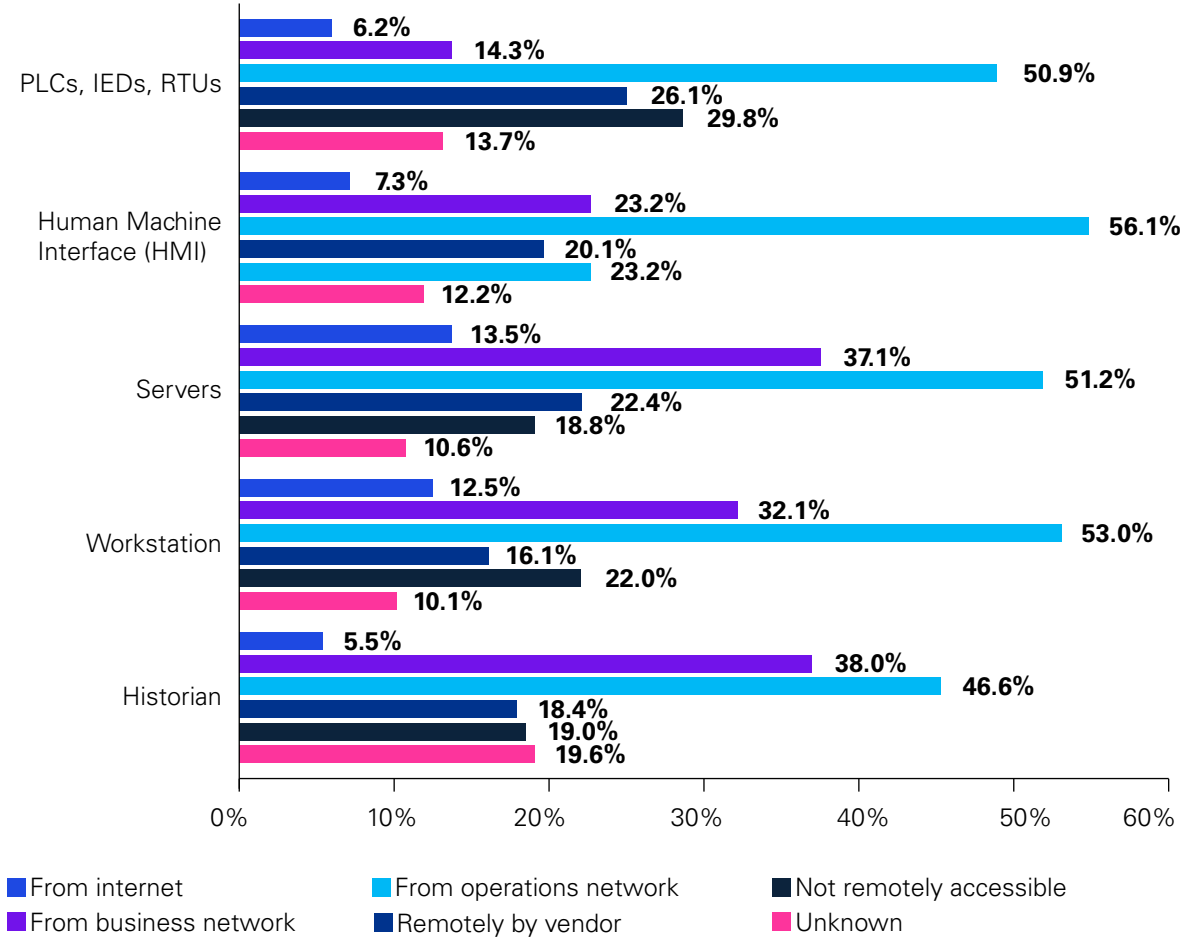
[5] Securing a hyperconnected world, KPMG International, 2021.

**Figure 1: Ransomware on the rise[5]**



*The Control System Cyber Security Survey 2020* study by KPMG and (CS)²AI — Control System Cyber Security Association International — indicated that 10 to 20 percent of respondents did not know whether any component/capability named in the graphic below was remotely accessible for their business.

**Figure 2: Components that are accessible remotely[6]**




[6] (CS)²AI-KPMG 2020 Control System Cyber Security Survey, KPMG International, 2020.

# The dramatic evolution of today's cyber-threat landscape

### Threat actors continue to raise their game.

Cybercriminals are continually changing tactics in an effort to avoid detection, increase their prospects for success and maximize their returns on ransomware attacks, including:

— The increasing use of close-knit syndicates of organized crime groups;

— Taking time to become more familiar with the operations of potential victims;

— Targeting attacks more precisely using legitimate documents that identify potential victims for malware delivery;

— Selling and buying direct access for rapid ransomware attacks instead of conducting advanced intrusions which are often more time consuming and costly.

### The motives for attacks can vary.

How do attackers choose their victims? Motives can vary and they are often supported by the illegal sale of passwords, tools and techniques to access corporate networks, which is also on the rise. Beyond financial gains, targeted ransomware attacks can involve diverse motives such as ideological or political factors. Regardless of motive, however, adequate security measures remain indispensable in order to effectively manage attacks.

### Supply chains are enduring new threats.

Improved ecosystem hygiene is pushing threats to the supply chain, turning friends into unsuspecting 'enemies.' Global inter-connectedness of businesses, wider adoption of traditional cyber-threat counter measures, and improvements to basic cyber security are prompting threat actors to pursue new approaches that increasingly target supply chains — including software, hardware and cloud services.

### OT/ICS infrastructure vulnerabilities demand costly solutions.

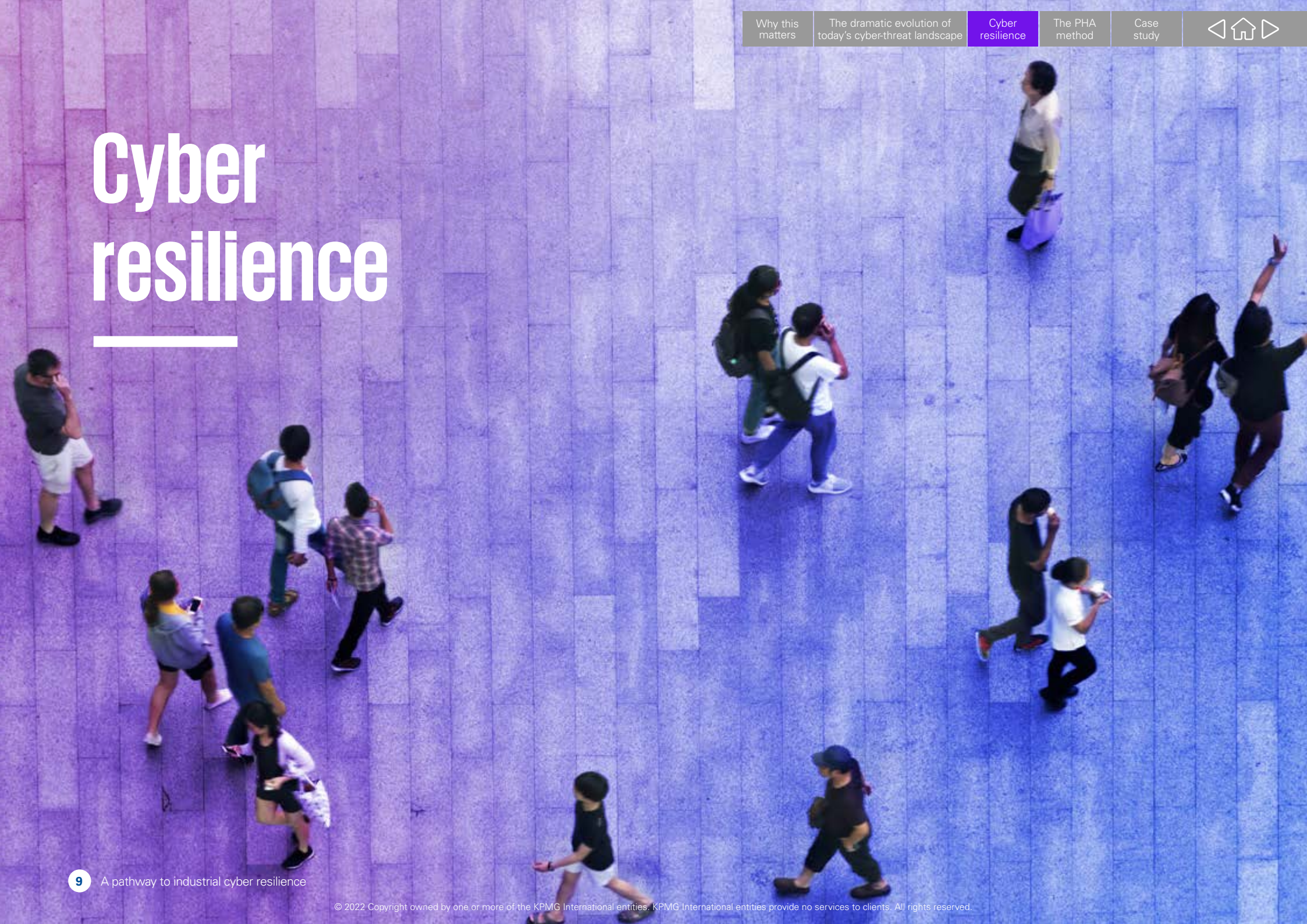
The discovery in recent years of vulnerabilities in programmable logic controllers (PLCs), human-machine interface (HMI), historian or engineering workstations all represent a high risk to organizations. In some cases, where vulnerabilities in critical infrastructure are targeted, operations could be impacted physically — causing safety hazards and even lead to loss of life.

### In the crosshairs of geopolitics.

As new threats emerge, businesses may be facing the negative impact of geopolitical tensions and nation-state cyber threats. These cyber-threat actors can take advantage of new capabilities as new technologies enable more sophisticated tactics, techniques and procedures (TTPs) which are focused to OT/ICS environments.[7]

[7] Security magazine, Five factors influencing the cyber security threat landscape, 2019.

# Cyber resilience



According to the US Department of Homeland Security, cyber resilience is meant to ensure that business systems continue to perform mission-critical functions during a cyber-attack. Cyber resilience is particularly important for a subset of critical infrastructures known as lifeline sectors or strategic infrastructures.[8] And it's not just the US putting extra emphasis on the cyber resilience for critical infrastructure.

The EU's 2016 NIS Directive is continually evolving to enhance cyber capabilities among critical infrastructure. The EU is also preparing to launch the Digital Operational Resilience Act (DORA), which aims to bolster cyber resilience for financial services among the lifeline sectors shown in figure 3.

Additionally, the National Cybersecurity Authority in Saudi Arabia has mandated all sectoral regulators to develop sector specific frameworks to support the country's cyber security strategy and regulation.

## Distinguishing cyber resilience from cyber security

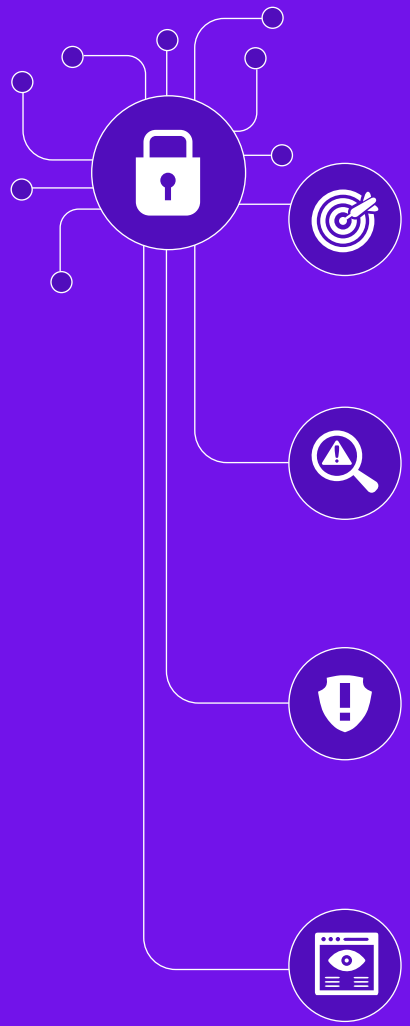
A key point that differentiates cyber resilience from cyber security is that cyber resilience capabilities continue to function even after an adversary has penetrated the security perimeter of a network to compromise cyber assets. Even at the later stages of the cyber-kill chain, cyber resilience can help to prevent adversaries from gathering intelligence on, exfiltrating data from, or taking control of mission-essential systems.

A tailored cyber resilience program can serve post-compromise along with a designed handbook for achieving cyber resilience outcomes based on a system engineering-perspective on system lifecycle processes. The tailorable nature of engineering efforts and lifecycle processes ensures that systems that apply cyber resilience design principles are sufficient to protect stakeholders from the loss of key assets and the associated economic and national security consequences.

Engineering cyber-resilient systems to combat today's evolving threat landscape involves the following characteristics that should be considered when designing new systems or enhancing existing ones.

**Figure 3: Lifeline sectors**


[8] US Department of Homeland Security, Cyber Resilience and Response (2018)



## Characteristics for engineering cyber-resilient systems

**Focus on the mission and business objectives.**

This involves the ability to support business continuity despite being compromised. In some cases, system components that are less critical to mission or business effectiveness may be sacrificed to contain a cyber-attack and to help maximize mission objectives.

**Focus on the effects of advanced persistent threats (APT).**

An APT's resources, stealth and ability to adapt make it a dangerous threat. By focusing on APT activities and their potential effects, engineers can design systems that anticipate, withstand, recover from and adapt to a broad and diverse set of adverse conditions and stresses.

**Assume an adversary is likely to compromise or breach the system or organization.**

This belief is fundamental to the design of cyber resilience. This assumption acknowledges that modern systems are large and complex entities that are likely to always have weaknesses and flaws that attackers can target and exploit.

**Assume that the adversary will likely maintain a prolonged presence.**

It may be difficult to determine that a stealthy threat has been eradicated. The APT can adapt to mitigation or rendering tactics that were previously effective against the threat. In some situations, the best outcome may be to contain an adversary's presence enough that the organization can achieve its primary mission objectives before losing critical systems capabilities.

## Cyber resilience value at the enterprise level

Due to the inherent complexity and dynamic nature of cyber-resilience techniques, initially deploying and maintaining appropriate cyber resilience can cost more than deploying and maintaining traditional cyber security measures. But despite their higher deployment and maintenance costs, cyber resilience can cost the enterprise less than traditional cyber security measures when assessed on a lifecycle-cost basis, given the ability of cyber resilience capabilities to withstand attacks and ultimately avoid costly enterprise downtime and lost revenues.

A sophisticated cyber-attack designed to shut down a critical infrastructure enterprise could paralyze the enterprise for several weeks, rather than just several days with less-sophisticated attacks. Calculating the estimated potential loss of revenue and customers, compared to the cost of implementing cyber resilience design principles and techniques, is what determines whether cyber resilience is cost effective for the enterprise.

## Cyber resilience value at the societal level

Even if a cyber resilience investment does not yield a net economic benefit at the enterprise level, it may still yield an economic benefit at the societal level. Critical infrastructure firms who know that a shutdown of their enterprise would have ripple effects throughout the region in which they operate should be able to make that case to their governments. When an enterprise cannot make the business case for its own cyber resilience, but recognizes how dependent other enterprises are upon them, they can make the business case at the regional societal level.

## Two examples demonstrating the changing nature of cyber-attacks in the industrial sector

### United States pipeline attack

In May 2021, the US experienced a major cyber security breach when Colonial Pipeline's Texas-to-New York petroleum pipeline, the nation's largest, was forced to shut down during a ransomware attack. As noted, the company had to pay the hackers USD4.4 million in ransom. The incident affecting millions of consumers and businesses is considered one of the most disruptive and costly digital ransom operations to date in the US and has provoked intense scrutiny toward the vulnerability of the country's current energy infrastructure.

### Data leak at global energy giant

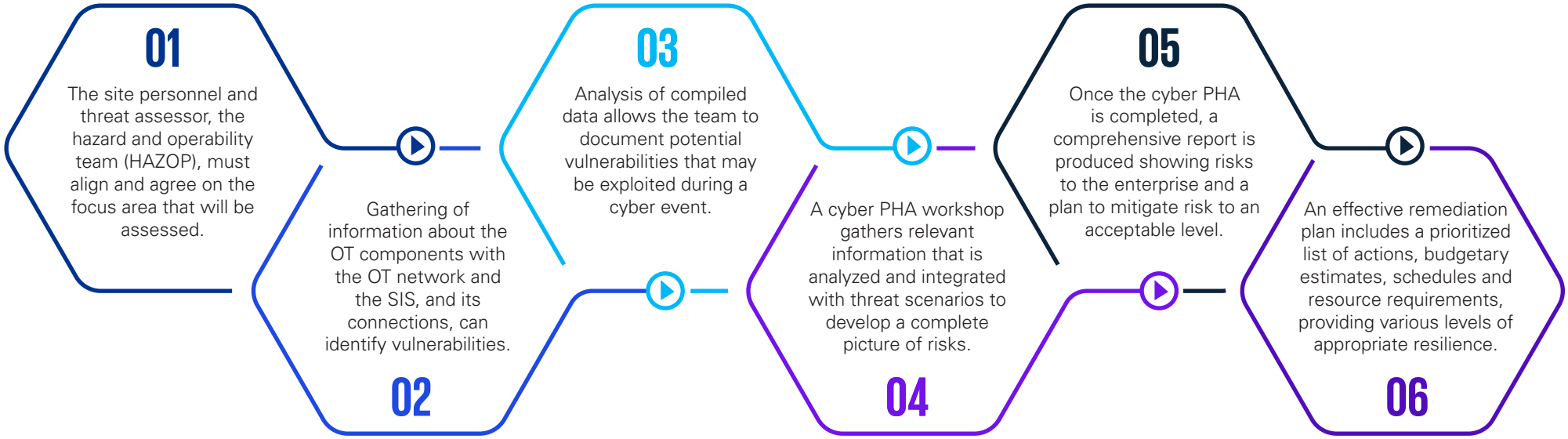
In mid-2021, a global energy company faced a data leak involving one of its contractors. One terabyte of business data was held by attackers in an attempt to extort funds from the company. Such incidents yet again highlight the critical importance of investing in modern cyber security amid the ongoing rise in cyber-attacks.

# The PHA method

## Facilitating a cyber PHA

A cyber process hazard analysis (PHA) is a safety-oriented methodology to conduct a cyber security risk assessment for an ICS or safety instrumented system (SIS). It is typically performed in phases, is scalable and can be applied to individual systems or entire facilities or enterprises.

## The six phases to a cyber PHA



## Expanded automation

Cyber security should not be seen simply as protection for old or vulnerable assets. Certainly, it can be difficult to retrofit cyber security for systems such as power grids amid limitations to upgrade, patch or even maintain them. But for newer industrial systems that integrate automation, cyber security protocols are just as important, if not more so today.

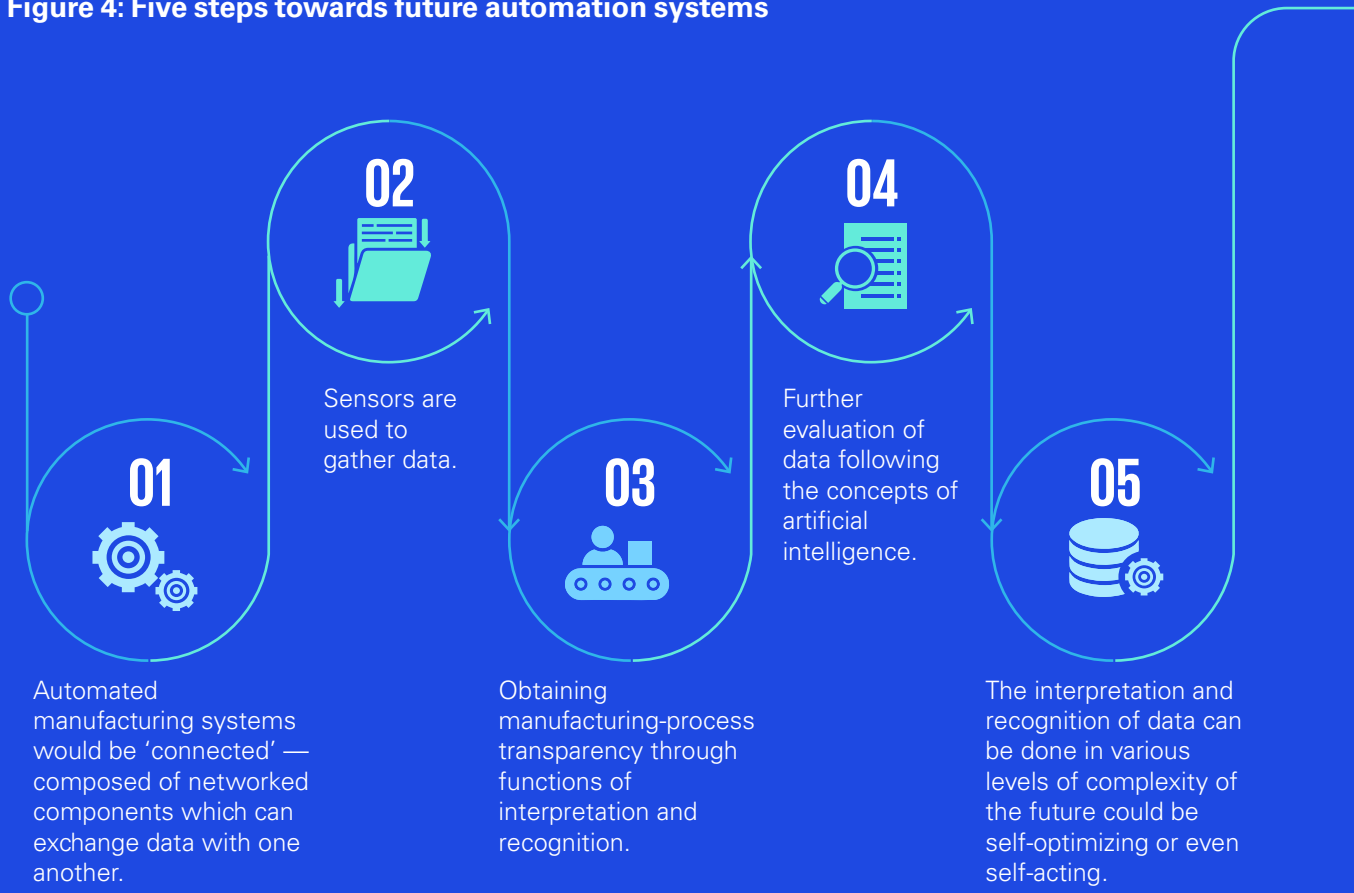
As automated manufacturing systems are introduced and as IT and OT systems converge, organizations should build in cyber security within core functions.

Maturity models for future development of automated manufacturing systems with IT functionality are continually emerging. One well-established model defined a few years ago in Germany and applicable today outlines five steps toward a new generation of self-acting and self-optimizing automation systems, which require a large degree of autonomy, see figure 4.[9] The first three steps involve the procurement of data and their systematic analysis.

Automation of industrial systems and IT/OT convergence means industrial systems — once isolated and secure — are becoming increasingly integrated with corporate networks, sometimes on commercial off- the-shelf platforms. This connectivity can create potential benefits such as smart analytics, predictive maintenance and remote monitoring. But it also exposes ICS, process-control systems and other operational technology to malware attacks, hacktivism, employee sabotage and other security risks that previously affected only corporate IT information.

As the lines blur between IT and OT, a cyber PHA can help provide appropriate access to control and production data

**Figure 4: Five steps towards future automation systems**




[9] Michael Weyrich, Towards future Automation Systems – Cyber physical, intelligent, flexible and efficient, 2018.

while preventing cyber security events that could cause costly shutdowns, serious safety threats and significant process disruptions.

## Regulatory framework

As the implementation of cyber systems grows across industries, it is crucial to set safety standards and regulatory measures that can help ensure the protection of data and systems. The process-safety management method was enacted in 1992 and is a comprehensive program which prevents the release of hazardous materials, typically underpinned by management commitment, and includes 14 related elements such as employee involvement, training, process-hazard analysis and process-safety information. See figure 5.

Organizations have already begun taking regulatory measures to safeguard against attacks. For example, the International Electrotechnical Commission (IEC) 61511 Functional Safety standard now requires an SIS security risk assessment. The updated report summarizes the risk-assessment procedure called cyber PHA. The link to PHA here is a step in the risk assessment to, firstly, review the output of the PHA to identify worst-case health, safety, security and environmental (HSSE) consequences for the asset and, secondly, to identify any hazard scenarios.

Another example comes from the User Association of Automation Technology in Process Industries (NAMUR), who have already published a worksheet (NA 163) titled Security assessment of SIS. Here, a cyber PHA methodology can assess risks linked to identified cyber security escalation factors and recommended mitigations to help reduce risks to a certain level.

**Figure 5: Illustration of occupational health and safety standards[10]**


[10] US Department of Labor, Occupational Safety and Health Administration, 1910.119 - Process safety management of highly hazardous chemicals

By creating a bridge between PHA methods and cyber security risk assessment methods, safety systems can become more robust against attacks.

Some global energy companies have long implemented methods to evaluate risk and increase safety. Such efforts include the use of risk-assessment matrices that consider the consequence of risk to people, assets, community and environment, and bow-tie models to visualize the various elements of risk scenarios. A cyber PHA risk tool can help to facilitate a holistic cyber PHA exercise. This includes the following:

— An existing documentation review;

— A listing of all cyber assets;

— Site walk-downs;

— Collection and review of previous PHA analyses; and subsequently

— A list of all types of cyber assets used within each specific process or utility unit wherever different process safety, environmental or financial hazards exist.

For a cyber-attack to take place, both the initiation and the safeguard should be hackable. By making one of the two non-hackable, the risk can be reduced. And by making both non-hackable, the risk can be eliminated. Although evaluating vulnerability is crucial, it is not enough to protect against cyber-attacks. Another essential factor to consider is understanding various types of cyber threats. Training staff on cyber security awareness is an essential part of the process, as it creates a deeper understanding of cyber threats and safeguards.

It is critical to perform a network path analysis, and validate network segmentation and functional isolations. The communication system architecture should always be verified against the required security level for the zone with which it interacts.

**Figure 6: One-line topology example**

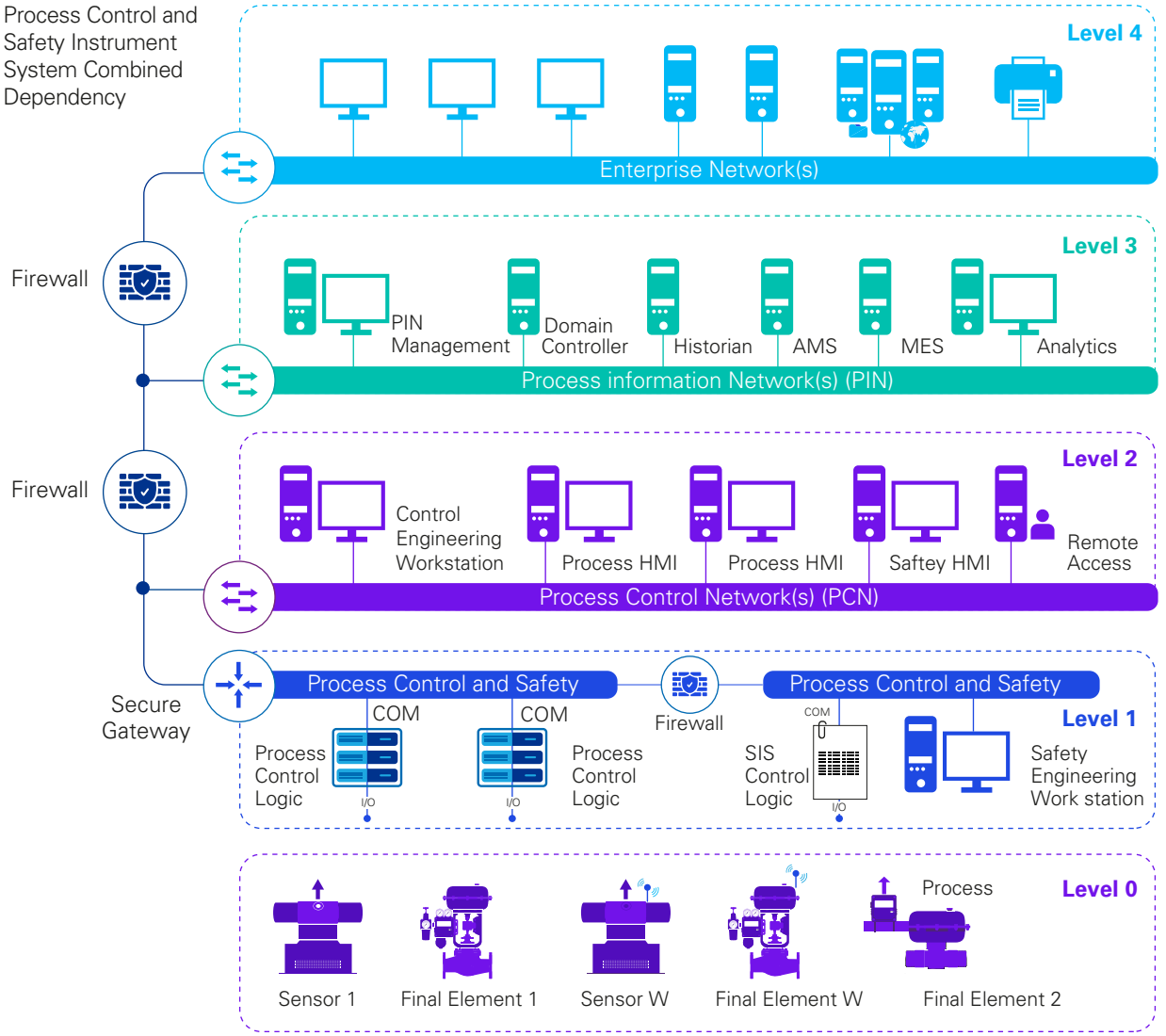
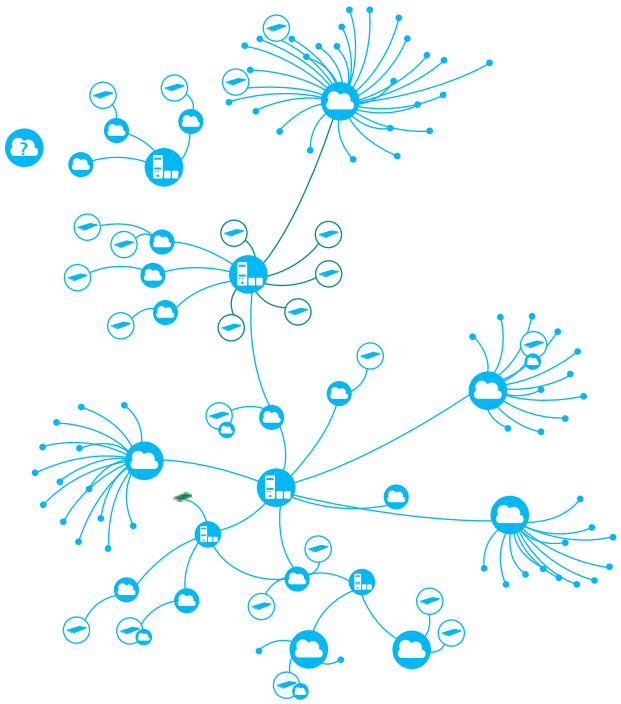


**Figure 7: Output of network topologies demonstrating interconnections and path analysis example.**



## Outcomes for a cyber PHA

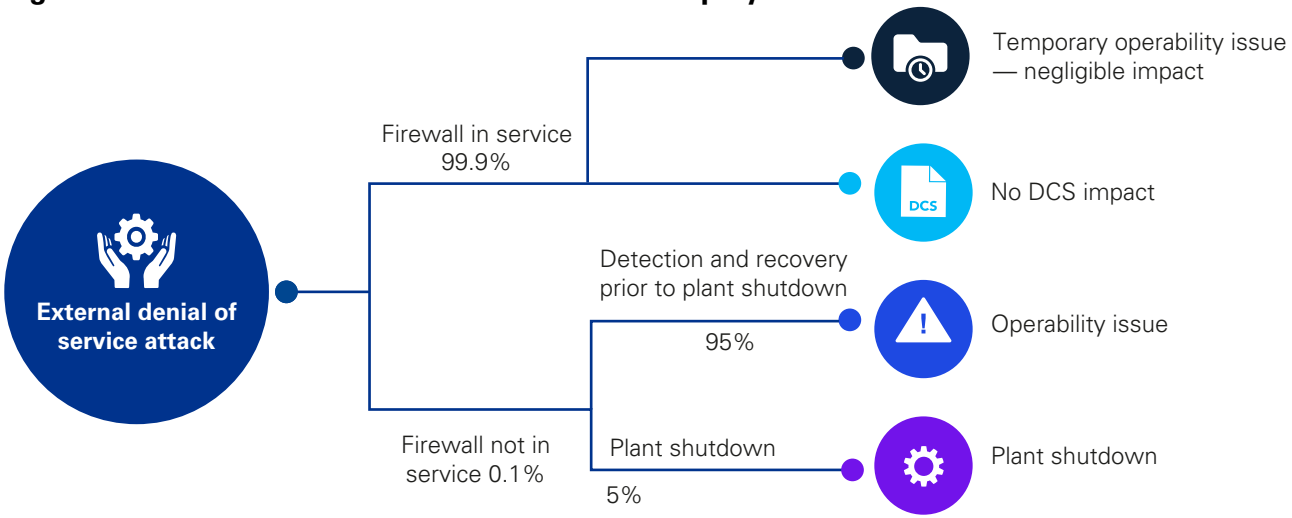
The outcome of the hazard and risk analysis should identify potential hazards and vulnerabilities while providing actionable risk themes that facilitate practical recommendations for implementation. Although the threat landscape is continually changing, there are general classifications of potential threat agents or sources for an organization to consider.

### Potential threat agents/sources

1. External attack — technical
2. Internal attack — non-technical
3. Internal misuse and abuse
4. Unauthorized access
5. Compromise of information (Logic Mod)
6. System malfunction
7. Process interruption
8. Safety-system interruption
9. Human error
10. Unforeseen effect of changes

Figure 8 illustrates how this works in practice, considering distributed control system (DCS) residual risk and counter-measure deployment.

**Figure 8: DCS residual risk and counter-measure deployment**




## Potential benefits of a cyber PHA

As cyber threats and impacts soar among industrial companies, the potential benefits of cyber PHA are numerous. The most obvious is system security. A cyber PHA methodology, when implemented correctly, can instill practices throughout an industrial system that can help prevent most cyber-attacks.

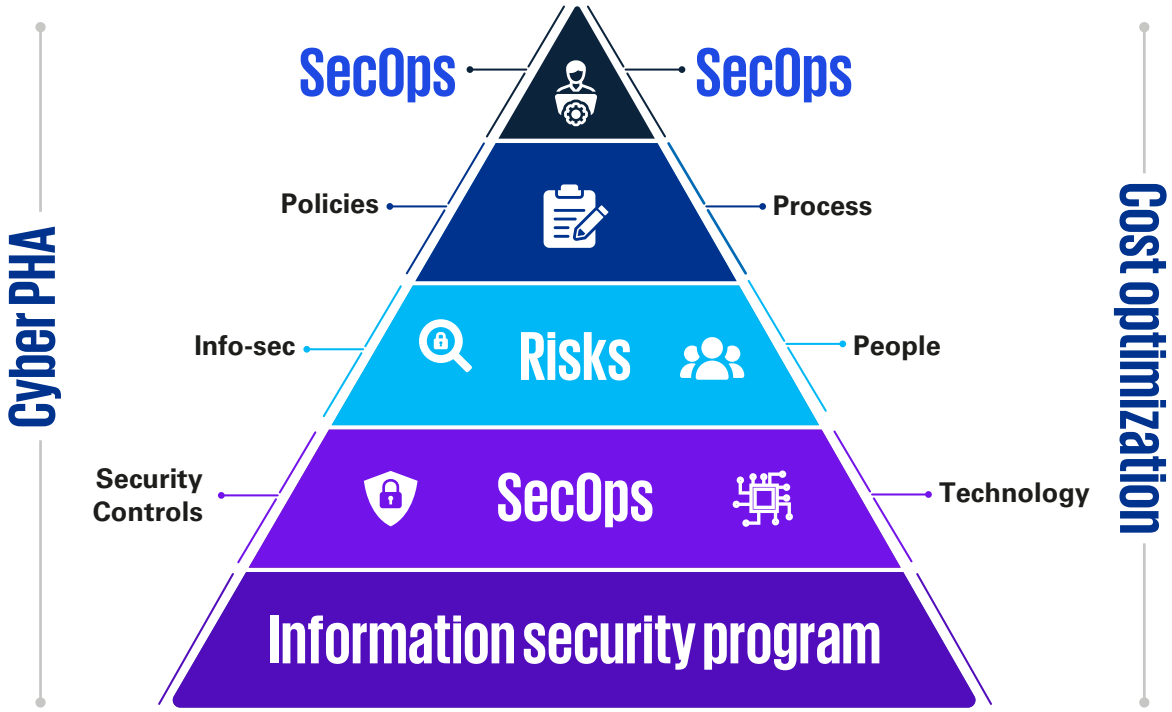
Beyond the obvious expected benefit of security, cyber PHA can also benefit an organization's broader business practices. Applying a cyber PHA methodology documents an organization's business processes and requires the creation of integrated information-security policies, procedures, standards and controls used within an organization.

## Potential business benefits of cyber PHA

The following are possible business benefits of cyber PHA:

- Articulation of the clearly defined information security strategy based on organization and business unit objectives.
- Definition of engineering knowledge with aligned security controls based on risk and business objectives.
- Confident effective staffing resulting from established roles and responsibilities.
- Interconnected system cause-and-impact identification, facilitating vulnerability and risk management.
- Targeted and prioritized cyber response and incident management.
- SecOps defined metrics, reporting and technology requirements to meet business objectives.

**Figure 9: Cyber, safety and cost optimization through SecOps**



# Case study

## Implementing a cyber PHA for an industrial organization

The client needed to standardize its processes across a heterogenous environment of systems and multiple vendors, bringing all to the same operating security level.

# Client challenges

**No CSMS in place**
Absence of a defined cyber security management system (CSMS) for the manufacturing environment.

**Disconnected processes across operations**
Presence of multiple plants operated by multiple stakeholders using separate processes and systems.

**No model reference network**
Absence of a standard and model reference network diagram in accordance with Purdue model and ISA 62443 guidelines for its different plants.

# The response

**Gap-assessment report and interviews**
This is essential to understanding the current security posture per International Society of Automation (ISA) guidelines. Subsequent creation of a standardized and common security framework and standard CSMS program for the entire organization.

**Design of monitoring dashboards**
Allowing senior management to represent the current state versus the target security state of the ICS environment to understand exposure level.

**Design of roadmap to implement identified security initiatives**
Allowing the client to track and implement the desired roadmaps across the ICS environment in terms of priority.

**Technical security assessment of PLCs and supervisory control and data acquisition (SCADA) applications**
Assessed the overall technical security posture of embedded devices and PLCs in the plant.

The threat scenarios and business logic threat cases designed to perform the assessment provided the client with a view of the existing attack surface and potential compromise areas in case of an attack.

**Process hazard analysis based on cyber PHA**
Reviewed cyber security gaps based on the HAZOP and layers of protection analysis (LOPA) procedures, and mapped the assessment to the risk categories defined across Health and Safety, Environment, Finance, Operations, thereby assigning overall risk to the deviations.

**System security levels assessment report**
Assessed security levels for each system in a zone and conduit in the ICS network.

**Developed a network architecture report**
Designed zones and conduits for two plants with two different types of ICS network. The gaps identified were presented to plant vendors to enhance the overall security architecture design of the plant.

# How can KPMG professionals help

KPMG firms can help you create a resilient and trusted digital world — even in the face of evolving threats. KPMG cyber security professionals can offer a multidisciplinary view of risk, helping you carry security throughout your organization, so you can anticipate tomorrow, move faster and get an edge with secure and trusted technology.

No matter where you are on your cyber security journey, KPMG firms have experience across the continuum — from the boardroom to the data center. In addition to assessing your cyber security and aligning it to your business priorities, KPMG professionals can help you develop advanced solutions, assist with implementing them, advise on monitoring ongoing risks and help you respond effectively to cyber incidents.

KPMG firms bring the uncommon combination of technological experience, deep business knowledge and creative professionals who are passionate about enabling you to protect and build your business. KPMG professionals can help you create a trusted digital world, so you can push the limits of what's possible.

# Contributors

**Ton Diemont**
**Head of Cyber Security & Privacy Services**
KPMG in Saudi Arabia

**Hossain Alshedoki**
**IT/OT Cyber security & Privacy ENR Lead**
KPMG in Saudi Arabia

**David Ferbrache**
**Global Head of Cyber Futures**
KPMG International

**Ronald Heil**
**Global Cyber Security Lead for ENR Partner and National Cyber Security Co-Leader**
KPMG in The Netherlands

**Jason Haward-Grau**
**Managing Director, Cyber Security Services**
KPMG in the US

**Walter Risi**
**Global Cyber IoT Leader and Partner, Cyber Security Services**
KPMG in Argentina

**Dani Michaux**
**EMA Cyber Security Leader Partner and National Cyber Security Leader**
KPMG in Ireland

# Your contacts in Switzerland


**KPMG AG**
Badenerstrasse 172
PO Box
8036 Zurich

**Dr. Matthias Bossardt**
Partner
Head of Cyber Security &
Digital Risk Consulting

+41 58 249 36 98
mbossardt@kpmg.com

**Dr. Thomas Bolliger**
Partner
Cyber

+41 58 249 28 13
tbolliger@kpmg.com

**Nicolas Tinguely**
Director
Cyber

+41 58 249 21 44
ntinguely@kpmg.com

**Yves Bohren**
Director
Cyber

+41 58 249 48 95
ybohren@kpmg.com


**kpmg.ch/cyber**