



# Industrial cyber defense

Assessing and bracing against  
cyber vulnerabilities in the energy  
and natural resources sector

October 2021  
KPMG in Saudi Arabia

# Table of contents

- 3** Introduction
- 4** Why this matters
- 6** The evolving threat landscape
- 7** Cyber resiliency
- 10** The process hazard analysis (PHA) method
  - Facilitating a cyber PHA
  - Expanded automation
  - Regulatory framework
  - Outcomes of a cyber PHA
  - Benefits of a cyber PHA
- 16** Case study: implementing cyber PHA for an industrial organization
- 17** Glossary
- 18** Contacts

# Introduction

The cybersecurity threat to industrial operations has evolved and rapidly expanded over the last year. A number of factors, including a shift to more engineering and maintenance remote activities, more remote operation work on production lines and incomplete digitalization efforts, have led to this rise.

Public awareness of the threat is growing. Colonial Pipeline, the largest pipeline operator in the United States, was compromised earlier this year, temporarily shutting down access to the pipeline's fuel for a large swath of the country. As this directly affected consumers, calls for action from the public rang loud following the attack.

Despite the growing threat and public pressure, organizations remain unprepared. Organizations may be facing a paradox of choice. The cybersecurity industry includes myriad services, many of which are relatively new and sometimes untested. Confounded by choices, many organizations end up unprotected.

This publication reviews the current threat landscape and presents directions for organizations to take action today and be better prepared for the evolving threat. Core to the recommendation of this paper is the cyber PHA – process hazard analysis – as a toolset for industrial organizations.



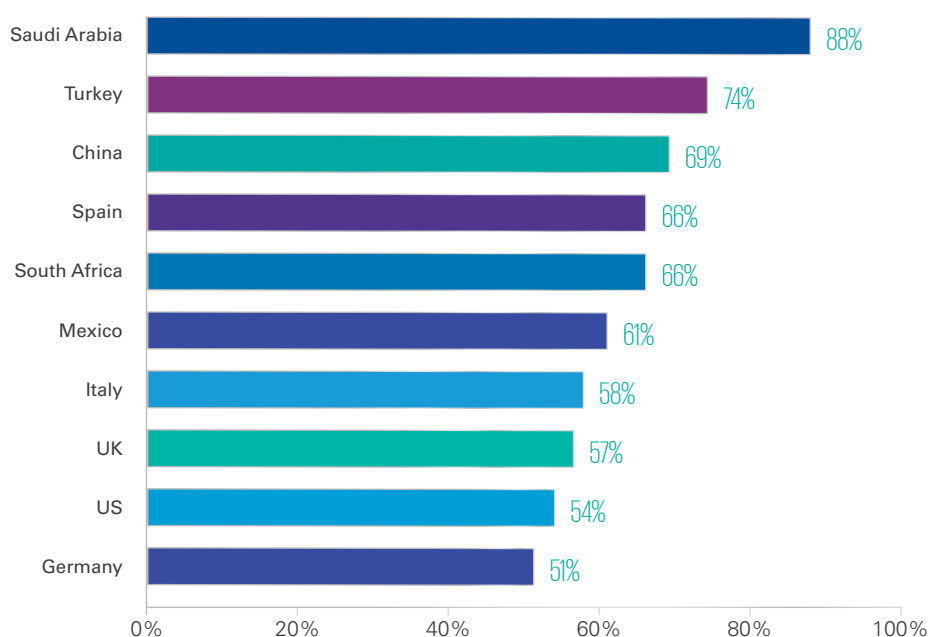
**Hossain Alshedoki**  
IT/OT Cybersecurity ENR Lead  
KPMG in Saudi Arabia

# Why this matters

Evidence from a number of studies suggests that business and government leaders recognize industrial cyber threats, but are not yet prepared to fend them off.

Cyberattacks are often cross-border and the threat to industrial companies is global. However, due to geopolitical realities and the concentration of industrial activity in certain countries, the threat is more acute in some countries than in others. In Saudi Arabia, the threat is particularly acute:

**Figure 1: Number of organizations that reported a ransomware attack by country<sup>1</sup>**



Ransomware attacks on OT networks soared five-fold from 2018 to 2020. Out of these, manufacturing entities comprised over one-third of confirmed ransomware attacks on industrial organizations, followed by utilities, which made up 10 percent. The estimated global costs of these ransomware attacks has skyrocketed — climbing from US\$8 billion in 2018 to US\$11.5 billion in 2019 and hitting US\$20 billion in 2020. The operational disruption due to ransomware in OT environments has led to a 23-fold increase. In 2020, there was a 32 percent increase in ransomware attacks against energy and utilities organizations.<sup>2</sup>

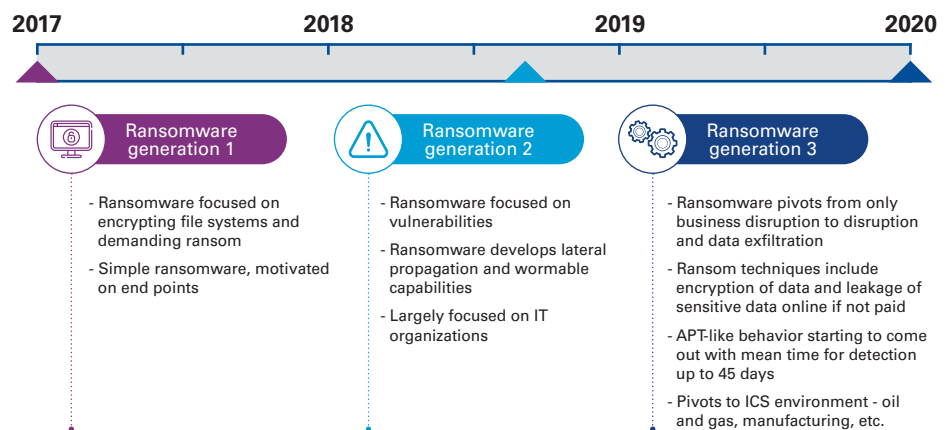
<sup>1</sup> Cybersecurity Magazine, Global Ransomware Damage Costs Predicted To Exceed \$265 Billion By 2031 (2021);

2021 Ransomware Statistics, Data & Trends, PurpleSec (2021)

<sup>2</sup> Ibid

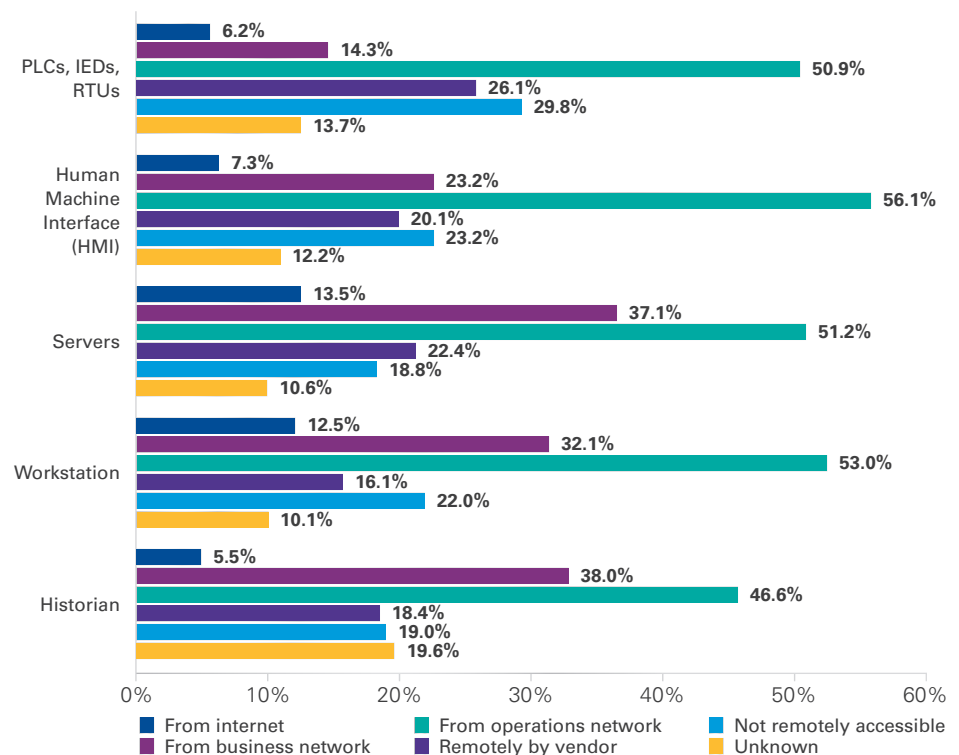
Over time, ransomware attacks have become more sophisticated and have changed to achieve their ends by different methods. Additionally, these kinds of attacks have increasingly targeted industrial control systems (ICS) environments like oil and gas and manufacturing.

**Figure 2: Ransomware on the rise<sup>3</sup>**



A study by (CS)<sup>2</sup>AI and KPMG, the Control System Cyber Security Survey 2020 indicated that 10 to 20 percent of respondents did not know whether any given component from the below graph was remotely accessible.

**Figure 3: Components that are accessible remotely<sup>4</sup>**



<sup>3</sup> KPMG - Securing a hyperconnected world (2021)

<sup>4</sup> (CS)<sup>2</sup>AI-KPMG 2020 Control System Cyber Security Survey

# The evolving threat landscape



## Evolving threat actors

Cybercriminals adapt, diversify and are behaving more like state actors. Criminal operations are changing their tactics to reduce risks of detection and disruptions. They are attempting to maximize the return on their effort in several ways such as: shifting away from partnerships to operating within close-knit syndicates; taking advantage of familiarity with the local environment; increasing the precision of targeting by using legitimate documents to identify likely victims before delivering malware; or selling and buying direct access to networks for ransomware delivery rather than carrying out advanced intrusions.



## Targeted ransomware

Hybrid motives pose new dangers in ransomware defense and response. The ransomware threat will be exacerbated further by the sale of access to corporate networks. While the motives behind such attacks may appear to be financial, targeted ransomware attacks may at times serve hybrid motives, whether financial, ideological, or political. Regardless of motive, while the ransomware threat remains, organizations must ensure they take adequate measures to prepare, prevent, detect, respond, and contain a corporation-wide ransomware attack.



## Supply chain threats

Improved ecosystem hygiene is pushing threats to the supply chain, turning friends into enemies. The global interconnectedness of business, the wider adoption of traditional industry cyberthreat countermeasures and improvements to basic cybersecurity hygiene appear to be pushing cyberthreat actors to seek new avenues to compromise organizations, such as targeting their supply chains—including those for software, hardware and the cloud.



## Life after meltdown

Vulnerabilities in OT/ICS infrastructure demand costly solutions. The discovery of vulnerabilities in PLCs, HMI, Historian or Engineering work station in recent years could pose a high risk to organizations which could lead to loss of life.



## Compromising geopolitics

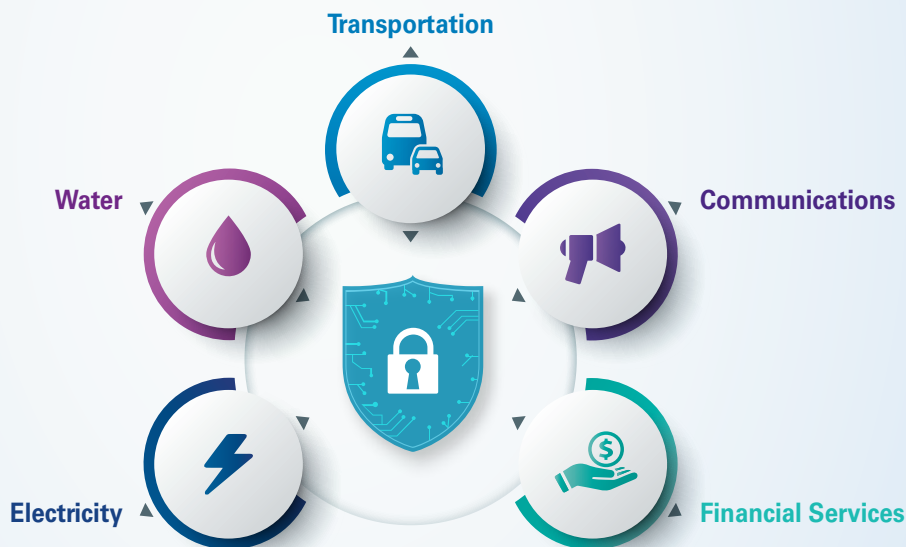
As new threats emerge from disinformation and technology evolution, global businesses may find themselves in the crosshairs as geopolitical tensions persist. Cyberthreat actors will not only sustain current levels of activity but also take advantage of new capabilities as new technologies enable more sophisticated tactics, techniques and procedures (TTPs) which are focused to OT/ICS environments.<sup>5</sup>

<sup>5</sup> Security magazine, Five factors influencing the cybersecurity threat landscape (2019)

# Cyber resiliency

The United States Department of Homeland Security developed a report on cyber resilience techniques and design principles, focused specifically on the capability to withstand adversarial activity, with an excerpt of that publication below.<sup>6</sup>

Cyber resiliency is that attribute of a system that assures it continues to perform its mission-essential functions even when under cyber-attack. Cyber resiliency is particularly important for a subset of critical infrastructures known as lifeline sectors or strategic infrastructures.



## Distinguishing cyber resiliency from cybersecurity

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

The many functions that cyber resiliency can serve post-compromise can be viewed as a handbook for achieving cyber resiliency outcomes based on a system engineering perspective on system life cycle processes. The tailorable nature of the engineering efforts and the life-cycle processes ensure that the systems resulting from the application of the cyber resiliency design principles are sufficient to protect stakeholders from suffering the unacceptable losses of their key assets and the associated economic and national security consequences.

<sup>6</sup> US Department of Homeland Security, Cyber Resilience and Response (2018)



Engineering cyber-resilient systems involves the following characteristics that should be considered when designing new systems or enhancing existing ones.



**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 maximize mission assurance.



**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, systems engineers can design systems that anticipate, withstand, recover from and adapt to a broad and diverse set of adverse conditions and stresses.



**Assume that the adversary will 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 will always have weaknesses and flaws that attackers will be able to target and exploit.



**Assume that the adversary will maintain a prolonged presence in the system or organization**

It may be difficult for the organization to be sure that a stealthy threat has been completely 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 containing an adversary's presence enough for the organization to achieve its primary mission objectives before losing the critical systems capabilities.



### Cyber resiliency value at the enterprise level

Deploying and maintaining cyber resiliency costs more than deploying and maintaining traditional cybersecurity measures. That is due to the inherent complexity and dynamic nature of cyber resiliency techniques. Despite the increased deployment and maintenance costs, on a lifecycle-cost basis, cyber resiliency costs the enterprise less than traditional cybersecurity measures. The primary reason for this belief is the ability of cyber resiliency to withstand cyber-attacks and thereby avoid enterprise downtime and lost revenues.

A sophisticated cyber-attack intending to shut down a critical infrastructure enterprise could shut-down the enterprise for several weeks, rather than just several days, as is typically the case with less sophisticated cyber-attacks. Calculating the cost of lost revenue and possible customer abandonment from a several week outages, compared to the cost of implementing cyber resiliency design principles and techniques, is what determines whether cyber resiliency is cost effective for the enterprise.

### Cyber resiliency value at the societal level

Even if a cyber resilience-specific 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 are located should be able to make that case to their governments. When an enterprise in any of these strategic infrastructures finds that it cannot make the business case for cyber resiliency for itself yet recognizes how dependent other enterprises are upon them, they can make the business case at the regional societal level.

Below are examples demonstrating the changing nature of cyberattacks in the industrial sector.

## United States pipeline attack

In May 2021, the United States saw one of the more significant cybersecurity breaches when one of the nation's largest pipelines was forced to shut down due to a ransomware attack. The US fuel pipeline had to pay the hackers \$5 million in ransom. The incident is considered one of the most disruptive digital ransom operations and has drawn attention to the vulnerability of energy infrastructure in the United States.

## Data leak at global energy giant

In mid 2021, A global energy company faced a data leak from one of its contractors. One terabyte of data was held by extortionists in an attempt to extort funds from the company. Such incidents highlight the importance of investing in cybersecurity and taking measures against cyber-attacks, as these attacks are not uncommon.

# The PHA method

## Facilitating a cyber PHA

A cyber PHA is a safety-oriented methodology to conduct a cybersecurity risk assessment for an industrial control system (ICS) or safety instrumented system (SIS). A cyber PHA is typically performed in phases, is scalable, and can be applied to individual systems, or entire facilities or enterprises. There are six phases to a cyber PHA.

01

The site personnel and threat assessor - the Hazard and Operability team (HAZOP) must align and agree on the focus area that will be assessed.



02

Gather information about the OT components with the OT network and the safety instruments systems (SIS), and its connections to identify vulnerabilities.



03

Analyze the data and document potential vulnerabilities that may be exploited during a cyber event.



04

Conduct a cyber PHA workshop where all information is gathered and analyzed, and integrated with threat scenarios to develop a complete picture of risks.



05

Once the cyber PHA is completed, a comprehensive report is produced showing the risks to the enterprise and a plan to mitigate risk to the organization's acceptable level.



06

An effective remediation plan includes a prioritized list of actions, budgetary estimates, schedule and resource requirements, which provides levels of resiliency.





## Expanded automation

Cybersecurity measures should not be seen simply as protection for old or vulnerable assets. Certainly, it can be difficult to retrofit cybersecurity for systems such as power grids with their limitations to be upgraded, patched or even maintained. But for newer industrial systems that integrate automation, cybersecurity protocols are just as, if not more, important.

Cybersecurity measures should not be seen simply as protection for old or vulnerable assets. As automated manufacturing systems are introduced and as IT and OT systems converge, organizations must build in cybersecurity within core functions.

Maturity models for future developments of automated manufacturing systems with IT functionality are being developed. One effective model, developed in Germany, outlines the five steps towards a new generation of self-acting and self-optimizing automation systems, which require a large degree of autonomy.<sup>7</sup> The first three steps involve the procurement of data and their systematic analysis.

- ① Automated manufacturing systems would be “connected”, i.e. be composed of networked components which can exchange data with one another.
- ② Sensors are used to gather data.
- ③ Obtaining of transparency of the manufacturing processes through functions of interpretation and recognition.
- ④ Further evaluation of these data following the concepts of artificial intelligence. The interpretation and recognition of data can be done in various levels of complexity of the future could be self-optimizing or even self-acting.

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 benefits such as smart analytics, predictive maintenance and remote monitoring. But 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 information.

As the lines blur between IT and OT, a cyber PHA can help provide appropriate access to control and production data while preventing cybersecurity events that could cause shutdowns, safety threats and process disruptions.

<sup>7</sup> Micheal Weyrich, Towards future Automation Systems – Cyber physical, intelligent, flexible and efficient (2018)



## Regulatory framework

Automation of industrial systems and IT/OT convergence. As the implementation of cyber systems grows across industries, it is crucial to set safety standards and regulatory measures to 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 interrelated elements such as, employee involvement, training, process hazard analysis and process safety information.



Figure 5: Illustration of occupational health and safety stands<sup>8</sup>

Organizations have already begun taking regulatory measures to safeguard against attacks. For example, the International Electrotechnical Commission (IEC) 61511 Functional Safety standard now requires a safety instrumented system (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 environment (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 be used to assess the risks linked to identified cybersecurity escalation factors and recommended mitigations to reduce risks to a certain level. By creating a bridge between PHA methods and cybersecurity risk assessment methods, safety systems become more robust against cybersecurity 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 consequence of risk to people, assets, community, and environment, and bow-tie models to visualize the various elements of risk scenarios.

<sup>8</sup> US Department of Labor, Occupational Safety and Health Administration, 1910.119 - Process safety management of highly hazardous chemicals

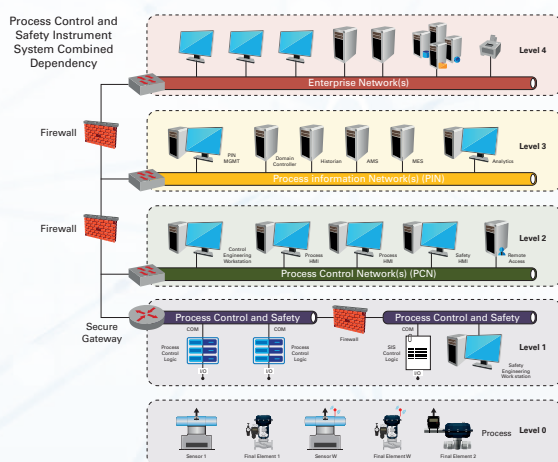


A cyber PHA risk tool can help to facilitate a holistic cyber PHA exercise. This includes an existing documentation review, a listing of all cyber assets, site walk-downs, previous PHA analyses, and subsequently a list of all the types of cyber assets used within each specific process or utility unit where different process safety, environmental or financial hazards exist.

In order for a cyberattack to take place, both the initiation and the safeguard must be hackable. By making one of the two non-hackable, the risk would be reduced and by making both non-hackable, the risk would be completely eliminated. Although evaluating vulnerability is crucial, it is not enough to protect against cyberattacks. Another essential factor to consider is understanding the various types of potential cyber threat. Training staff on cybersecurity awareness is an essential part of the process as it creates a larger understanding of cyber threats and methods to safeguard against them.

It is critical to perform a network path analysis, 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**





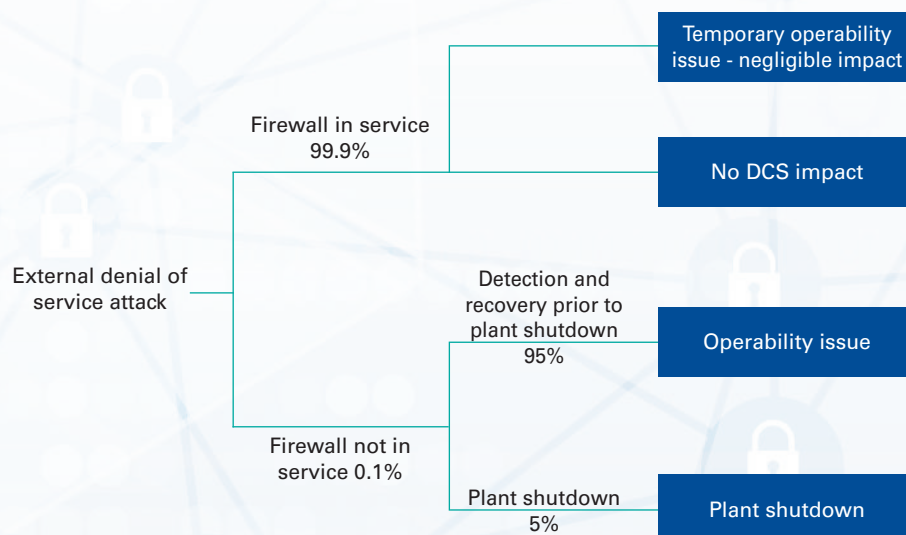
## Outcomes for a cyber PHA

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

- 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 exemplifies how this works in practice, considering DCS residual risk and countermeasure deployment.

**Figure 8: DCS residual risk and countermeasure deployment**





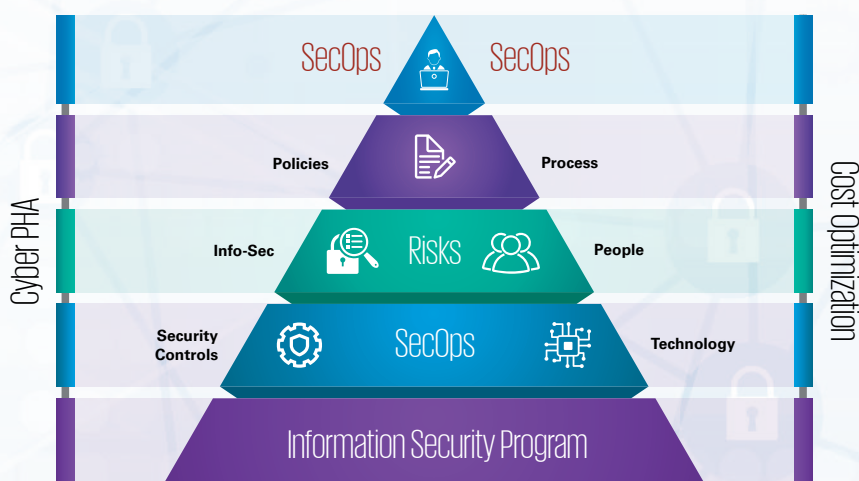
## Benefits of a cyber PHA

Considering the cyber risk at hand, which is demonstrably increasing for industrial companies, the benefits of cyber PHA are numerous. The most obvious benefit is system security. A cyber PHA methodology, when implemented correctly, instills practices throughout an industrial system that will prevent most cyberattacks.

Beyond the obvious benefit of security, cyber PHA also benefits 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.

- Clearly defined and articulation of the information security strategy based on organization and business unit objectives.
- Engineering knowledge defined and 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


## Client challenge and response

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




**No CSMS in place**

Absence of a defined cyber security management system (CSMS) cybersecurity for the manufacturing environment



**Disconnected processes across operations**

Presence of multiple plants operated by multiple stakeholders with 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

## Gap assessment report and interviews

Essential to understand the current security posture per ISA guidelines. Subsequent creation of a standardized and common security framework and standard CSMS program for the entire organization.

### Designed monitoring dashboards

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

### Designed a 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 SCADA applications

Assessed the overall technical security posture of the embedded devices and PLCs in the plant. The threat scenarios and business logic threat cases designed to perform the assessment provided the client a view of the existing attack surface and the possible areas of compromise in case of an attack.



### Process hazard analysis based on cyber PHA

Reviewed cybersecurity gaps in the environment based on the HAZOP and LOPA procedures and mapped the assessment to the risk categories defined across Health and Safety, Environment, Finance, Operations and 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.

# Glossary

<b>APT</b>	Advanced Persistent Threat
<b>CSMS</b>	Cyber Security Management System
<b>DCS</b>	Distributed Control System
<b>HAZOP</b>	Hazard and Operability Team
<b>HMI</b>	Human-Machine Interface
<b>HSSE</b>	Health, Safety, Security and Environment
<b>ICS</b>	Industrial Control System
<b>IED</b>	Intelligent Electronic Device
<b>IT</b>	Information Technology
<b>LOPA</b>	Layers of Protection Analysis
<b>OT</b>	Operational Technology
<b>PCN</b>	Process Control Network
<b>PHA</b>	Process Hazard Analysis
<b>PIN</b>	Process Information Network
<b>PLC</b>	Programmable Logic Controller
<b>RTU</b>	Remote Terminal Unit
<b>SCADA</b>	Supervisory Control and Data Acquisition
<b>SIS</b>	Safety Instrumented System
<b>TTP</b>	Tactics, Techniques and Procedures

# Contacts



**Ton Diemont**

Head of Cybersecurity  
KPMG in Saudi Arabia  
E: antondiemont@kpmg.com  
T: +966 56 860 8393



**Hossain Alshedoki**

IT/OT Cybersecurity ENR Lead  
KPMG in Saudi Arabia  
E: halshedoki@kpmg.com  
T: +966 50 014 7879

## [kpmg.com/sa](https://kpmg.com/sa)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

## Disclaimer

This report is solely for information purposes. Accordingly, KPMG does not and shall not assume any responsibility for the information presented herein or the nature and extent of use of this report.