Securing a hyperconnected world

How to prepare for and respond to cyberattacks targeted at critical infrastructure.

KPMG International

home.kpmg/cybersecurity

Foreword

The future is hyperconnected and cyber-physical

The world has gone digital and the profound impact of revolutionary technology continues to grow at an accelerating pace.

As the World Economic Forum notes in its 2020 report *Cyber security, Emerging Technology and Systemic Risk*[1], transformational technologies now shaping the current and future connected society include ubiquitous digital connectivity, artificial intelligence, advanced machine learning and quantum computing. Simply put, society is speeding into a bold new hyperconnected world that promises historic social, economic and environmental advances.

As the reliance on technology grows, however, so does the critical need to ensure security and protection in the face of soaring cyber threats — accidental or intentional — that can put infrastructure, businesses, even human lives, at risk.

Malware, a catch-all term for any type of malicious software designed to harm or exploit digital devices, services or networks, has proliferated in reach and sophistication to exert a costly toll on businesses, with ransomware currently dominating headlines in the wake of destructive attacks. A type of malicious software that typically blocks access to computer systems or valuable data, paralyzing business-critical processes ransomware is allowing cyber criminals to cash in by extorting businesses, large or small, for massive cryptocurrency payments.

According to blockchain analytics firm Chainalysis[2], ransomware-linked extortion exploded to a record US$406 million in 2020, from US$92.9 million in 2019 and reached an estimated US$81 million in cryptocurrency payments as of May 2021. Chainalysis notes that the true toll is probably much higher, as businesses often fail to report or publicize costly ransomware attacks as this menacing trend continues to unfold at an alarming rate.

Colonial Pipeline, operator of the largest US fuel pipeline, suffered a vicious May 2021 ransomware attack that disrupted oil and gas supplies in the US, with the firm paying about US$5 million in bitcoin to unlock its network. This is not the only example; there have been many more high-profile ransomware attacks on businesses worldwide in which substantial payments have been made to resume operations quickly.

As costly and destructive attacks multiply, the race is now on to respond with security and threat management systems that can stem the tide of disruption.

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

[1] Future Series: Cyber security, emerging technology and systemic risk, World Economic Forum, 2020.

[2] Danny Nelson, Ransomware Attacks Growing More Profitable: Chainalysis, Coindesk, May 19, 2021.

Contents

The growing threat landscape

Ransomware and other forms of malware can unleash havoc in diverse and increasingly creative ways, including paralyzing attacks on infrastructure, businesses, government and even global internet services. The growing threat of sophisticated cyberattacks is creating significant challenges to the promise and potential of the digital revolution.

Threats become particularly critical when involving operational technology (OT) controlled environments, which are typically used in the production and distribution of goods and services critical to national infrastructure and broader society. Cyberattacks affecting OT environments have become a harsh and troubling reality in recent years and a growing concern as their potential to create massive disruption increases.

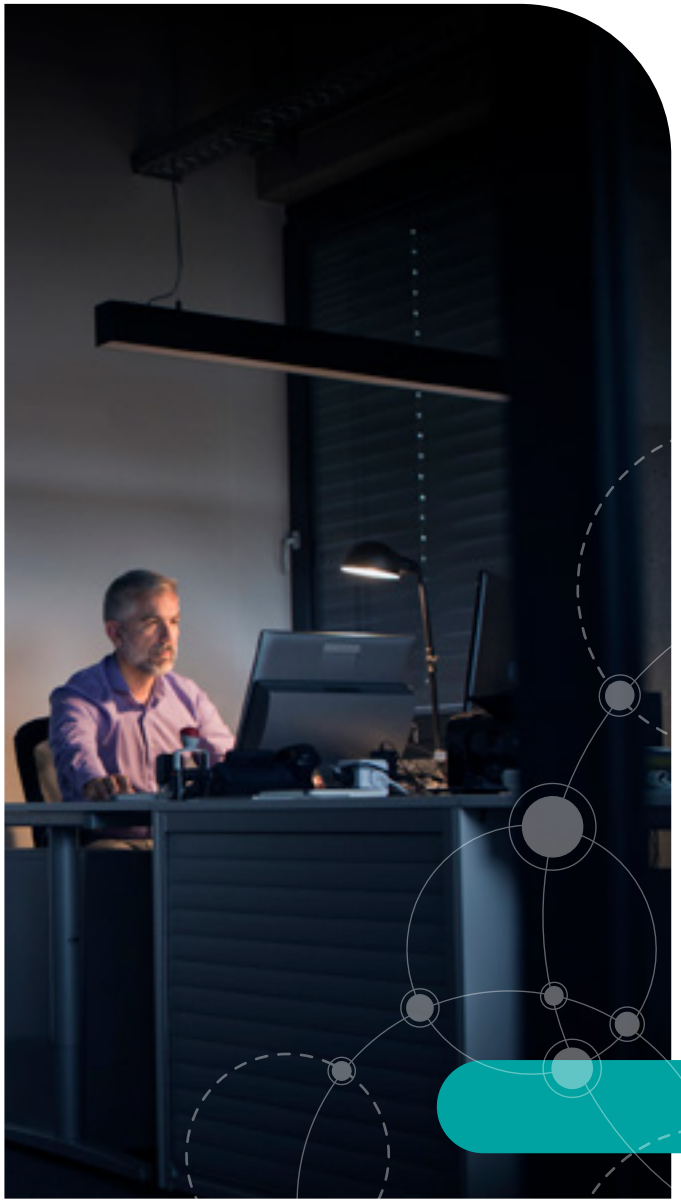
While attacks on OT environments have escalated in recent years, they are unfortunately gaining momentum as the rapid shift to online services and remote working during the global pandemic creates new opportunities to launch lucrative ransomware attacks. Organized crime groups are raising the ransomware stakes in terms of the sophistication and costs of attacks, and increasingly targeting national infrastructure across an array of sectors, including healthcare, manufacturing, energy, and oil and gas.

The reality is that ransomware attacks can deliver high returns for criminals, and the rapid growth of liquidity in cryptocurrency markets is creating more opportunities for large payoffs.

Ransomware attacks on OT networks soared by 500 percent from 2018 to 2020[3]. Out of these, manufacturing entities comprised over one-third of confirmed ransomware attacks on industrial organizations, followed by utilities, which made up 10 percent[4].

The estimated costs of these ransomware attacks has skyrocketed — it's predicted to reach US$20 billion in 2021, up from $325 million in 2015[5]. The operational disruption due to ransomware in OT environments has led to a 23-fold[6] increase. In 2020, there was a 32 percent increase in ransomware attacks against energy and utilities organizations.

As OT environments are increasingly digitized to help optimize efficiency, the lines between air-gapped OT systems and corporate information technology (IT) environments are blurring. Ongoing integration of Industrial Internet of Things (IIOT) devices and remote management systems — which has accelerated since the start of the pandemic — has increased the exposure of OT environments and the risk of attack (for the sake of simplicity, the acronym OT refers to both traditional OT as well as IIOT). The attack this year on the Oldsmar, Florida water treatment plant, where an intruder remotely infiltrated the plant's control system and water chemistry, potentially poisoning local residents, is just one recent example of how OT-IT integration is posing significant new risks.

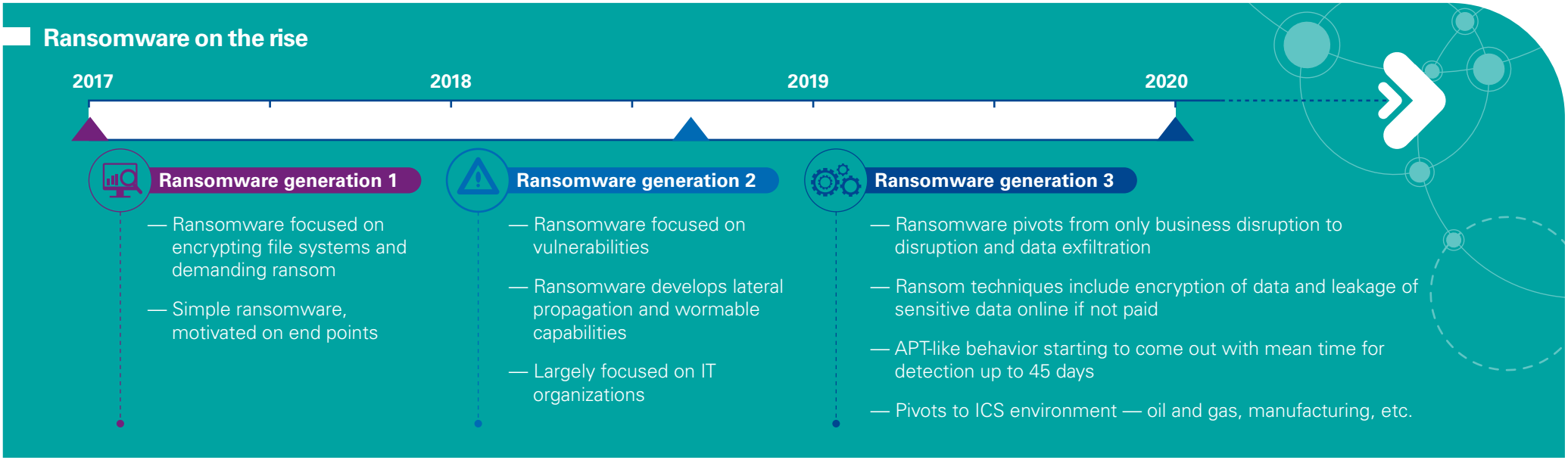


[3] Ransomware in ICS Environments, Dragos, December 2020.

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

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

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



What makes malware in all its forms a particularly dangerous threat is that it encapsulates harmful capabilities in software format, allowing hackers with limited expertise to launch destructive and costly attacks. 'Egregor' ransomware and others are following the ransomware-as-a-service (RaaS) model, which conveniently provides criminals with tools that can empower even the most inexperienced of hackers to launch complex and devastating attacks.

Malware can also be reused and enhanced, allowing malicious actors to build upon existing capabilities and ultimately expand their destructive power. A software weapon such as malware stays in the digital terrain for others to use, reuse and improve. That was the case with MIRAI, which spawned a series of variants after its initial attack. Finally, malware can cause unexpected damage beyond the intentions of its authors. This is especially true for self-replicating malware — worms or viruses — that can propagate indefinitely and unpredictably unless specific 'kill-switches' are included in the software by their authors. Nothing prevents future perpetrators from disabling that kill switch.

Addressing the threat — an overview of the approach

Given the growing threat and devastating impact of malware, the obvious — and formidable — challenge is how to effectively combat this digital menace. For the purpose of this paper, there is a summary of advice in two large domains, *Prepare* and *Respond*, which in actual field practice map to industry standards and frameworks[7].

[7] The Prepare and Respond domains that are referenced in this paper are mapped to highly regarded industry standards/frameworks: ISA-62443-1 and NIST Cyber Security Framework.

Preparing to address the threat

The *Prepare* phase aims to establish a foothold on the OT cyber security program and define the organization's capabilities to deal with today's fast-evolving cyber threats. This involves asking key questions to understand the current state, set the baseline, and implement controls and processes to identify, protect and defend against attacks.

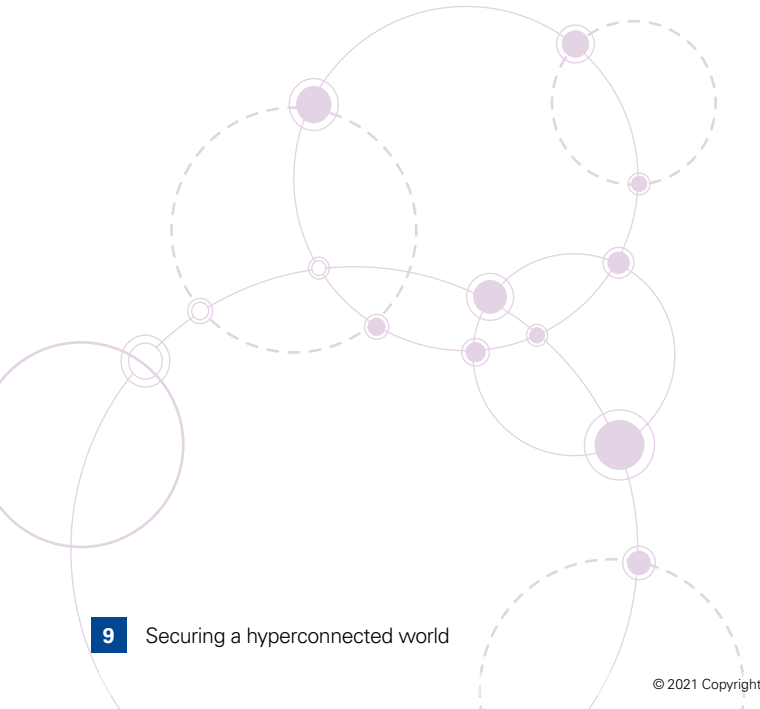
Seven key questions to ask

1. Have you identified the cyber-related risks to which your control network is exposed and are you actively working to mitigate them?
2. Does an up-to-date asset inventory of your control network exist?
3. What is the integration level between the OT and corporate network?
4. How is remote access to the control network managed?
5. Is there a solid backup mechanism in place and is it consistently tested for integrity?
6. What methods are used to apply security patches?
7. What are your current anti-malware solutions?

This first foundational step could turn into an uphill task for many organizations, for reasons including: a lack of skills required to set the wheel in motion and execute projects, or a lack of senior leadership support to push ahead with the OT cyber security program and assign the required budget and team.

This can be addressed through strategic development of a business case, heightened awareness of the challenge among the C-suite and key stakeholders and the sponsorship of senior leaders. Implementing a well-structured, fully supported program is crucial in laying the foundation for a successful OT cyber security program.

Having established the foundation, each of the preparation-phase questions above should be approached with an OT lens, understanding that some aspects differ from the common best practices of traditional IT environments. Here are some instructive insights and responses to the seven key questions.



1. Have you identified the cyber-related risks to which your control network is exposed and are you actively working to mitigate them?

While this may sound obvious as a first step, understanding the current state of the organization's overall OT security is fundamental to giving management clear visibility into the current challenges and the required responses. An OT security-risk assessment, coupled with an OT cyber maturity assessment, can provide management with a high-level view of what needs to be addressed both at the technical and governance levels. Action plans can then be prioritized and organized to progress from lower to higher maturity and, at the same time, cover the highest-priority risks.

While doing risk and maturity assessments, identifying the assets that are critical to business continuity is essential. For an electrical utility or distribution company, for example, guaranteeing delivery of electrical power is indispensable, while for a food-and-beverage company, ensuring that production is not compromised will be crucial. Mapping risk and maturity levels to critical business scenarios and needs puts security in the appropriate context and helps raise awareness among leadership.

2. Does an up-to-date asset inventory of your control network exist?

It's vital to know exactly what needs protection within your production environment. This step usually begins with an asset identification or inventory, which can be performed automatically via scans or manually by asset owners. Since the environment is typically complex and multi-vendor, manual identification tends to be difficult and error prone, making automatic detection preferable. As mentioned later in this paper, many commercial solutions now combine threat-detection and discovery capabilities.

Having a detailed and comprehensive asset inventory is vital to creating a current and complete picture of your industrial network, as well as a clear understanding of assets that are vulnerable to modern threats. After this, a business impact analysis (BIA) of assets follows. The BIA defines the criticality of assets and, in turn, helps decide what kind of cyber security defenses and controls should be implemented. Where patching and other countermeasures can't be installed, a BIA is particularly useful.

3. What is the integration level between the OT and corporate network?

Ransomware commonly spreads throughout the network it attacks. Therefore, to protect critical assets, and those no longer receiving updates, assets should be isolated. Successful segmentation can limit ransomware's movement. By creating zones and conduits, communication between assets can be closely monitored and limited to only essential communication between assets and the OT/IT network.

Due to business integration purposes, this may not be possible, meaning that some other form of network segmentation should be implemented, such as the Purdue model. Successful implementation of the Purdue model requires complete knowledge of all assets, protocols, connections, interfaces and communications between industrial control system (ICS) and IT networks. Industrial intrusion detection systems (IDS) tools have helpful features that identify these points to allow for successful modelling of a network according to the Purdue model.

4. How is remote access to the control network managed?

Secure remote access is a vital topic when it comes to maintaining and repairing assets from a distance, especially in the COVID and post-COVID world. Common remote access types include Remote Desktop Protocol (RDP) and virtual private network (VPN), both of which, it's important to note, are common attack vectors today. Secure remote access software is now commonly available on the market and should be considered when it comes to securing access.

5. Is a solid backup mechanism in place and consistently tested for integrity?

Even while implementing these measures outlined, ransomware may infiltrate OT assets. Once this occurs, the only option for recovering these assets, apart from paying the ransom, is to restore a backup.

Organizations should consider the types of assets they need to back up. Backups of proprietary operating systems are more complex compared to operating systems such as Windows or Linux. One also needs to consider whether the systems are connected to the network or are stand-alone. The medium where the backup is stored is critical to preventing the backups from being infected with malware. To prevent this, tapes can be stored in vaults.

6. What methods are used to apply security patches?

This project is a tough topic in ICS environments. Ideally, you never want to touch the system in order to remain productive 24/7. Unsurprisingly, a common saying among engineers is "Never change a running system." There has been a disconnect between engineers and security professionals for a long time and the challenge for the latter is to understand the particularities of an OT-running system.

A business impact analysis comes in handy on patch-management issues. Assets deemed critical should have a short time frame for patches to be applied. If an asset has a low criticality, patches may be applied in the next maintenance interval.

7. What are your current anti-malware solutions?

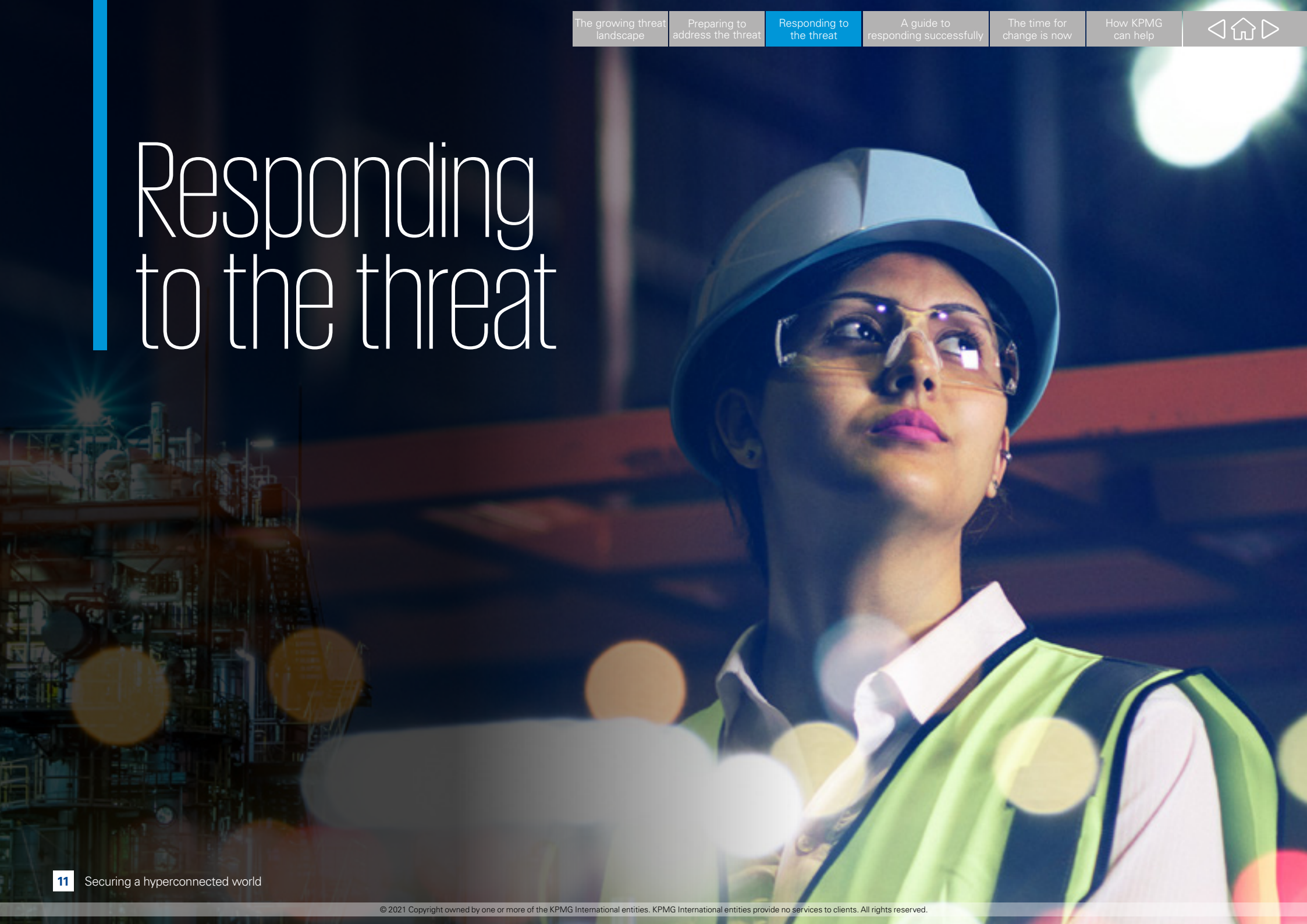
Finally, to defend against ransomware, early detection is crucial. As noted, intrusion detection systems (IDS) are helpful in detecting ransomware in the network. They can inspect and monitor network traffic for malicious activity — including ransomware. Several OT-specific IDS-like systems in the market today typically combine detection functionality with a discovery capability which, when paired with Configuration Management Database (CMDB) or asset-management software, can also help address the inventory problem mentioned.

Detection tools that inspect and monitor network traffic for malicious activity are helpful in identifying ransomware in the network. The detection tool should be connected to a Security Incident and Event Management (SIEM) tool. The SIEM should log multiple sources, including firewalls, assets and remote access tools. By collecting all sources, the SIEM tool should be able to alert the responsible team to respond to a ransomware attack.

A word on tools

There is a common adage that tools come after good governance mechanisms are in place. That does not apply easily to OT security. Threat actors, particularly ransomware, will not wait until your OT security-management system is in place. It's encouraged to approach an OT security-management program in a top-down/bottom-up fashion. Start by understanding risk and incrementally addressing the topics mentioned above but, almost simultaneously, establishing visibility through OT-specific tools, which can allow rapid threat detection and also help with some remediation steps mentioned. The less mature your environment is, the earlier you need to know if malware is lurking in your network.

Responding to the threat



The *Respond* phase aims to ensure that organizations are prepared for potential high-impact incidents and disruption to critical processes. Attacks on cyber-physical environments can be catastrophic if critical infrastructure is affected, due to the potential for far-reaching social, business and economic impacts. The more you prepare and rehearse, the less damage that this threat can cause.

Consider for a moment a possible scenario affecting your company's operations network. A workstation in the operations network displays this message: 'Blue Screen/Dumping Physical Memory' and, 5 minutes later, the central operations system is under attack. A critical decision looms: disconnect and lose total visibility of the operation or keep diagnosing while the malware spreads. This is unfolding while the whole company is under extreme stress, the nervous board is asking questions, probing journalists are requesting interviews, and someone might be spreading the news of the attack via social media. Often, the response team is faced with a series of questions that must be answered quickly.

Questions that need answers

- Can we isolate the affected network areas? Have we done that before? What would be the impact in that case?
- Are human lives in danger?
- Is it possible to operate manually if we disconnect the operational network from the IT network? If so, do we have the proper and trained team to do it? Can we get back from manual operation?
- Should we involve law enforcement?
- Should we make this public? When? What are we going to tell the press?
- Should we involve the regulator?
- Are public services (light, electricity, water, etc.) affected? If so, what is the impact? Are there contingency plans?
- And probably above all — should we pay the ransom?

Alarming scenarios like this not only demand technical preparation and resolution, they include critical factors to address in the response strategy. Some examples include:

Communication

In this type of critical situation, it's essential to control internal and external communications. Being in control means disseminating the right message, at the right time, to those who should receive it. It's therefore crucial to have the first containment messages prepared; identify appropriate internal and external communication channels; identify who will communicate; and prioritize who will receive the communication — employees, customers, regulators, media and/or others. It might be necessary to prepare different messages for various recipients.

Third parties

The attack could spread to third parties such as suppliers, customers or regulators, making it necessary to disconnect third-party processes and prevent further spread. A preconfigured 'kill button' is therefore indispensable in order to isolate critical networks immediately.

To pay or not to pay?

This decision is critical. Certain conditions should be defined, and a pre-established decision should be made by senior leadership. Paying the ransom may seem like the easy way out, but this is not necessarily the case. Firstly, paying the ransom does not guarantee retrieval of data or the non-disclosure of stolen confidential information. Paying the ransom can also send the message that you are likely to pay again, making you more susceptible to future attacks. The US Department of Treasury recently stated that they may sanction those who pay ransom demands. Others are likely to follow suit in the near future.

Compromised information

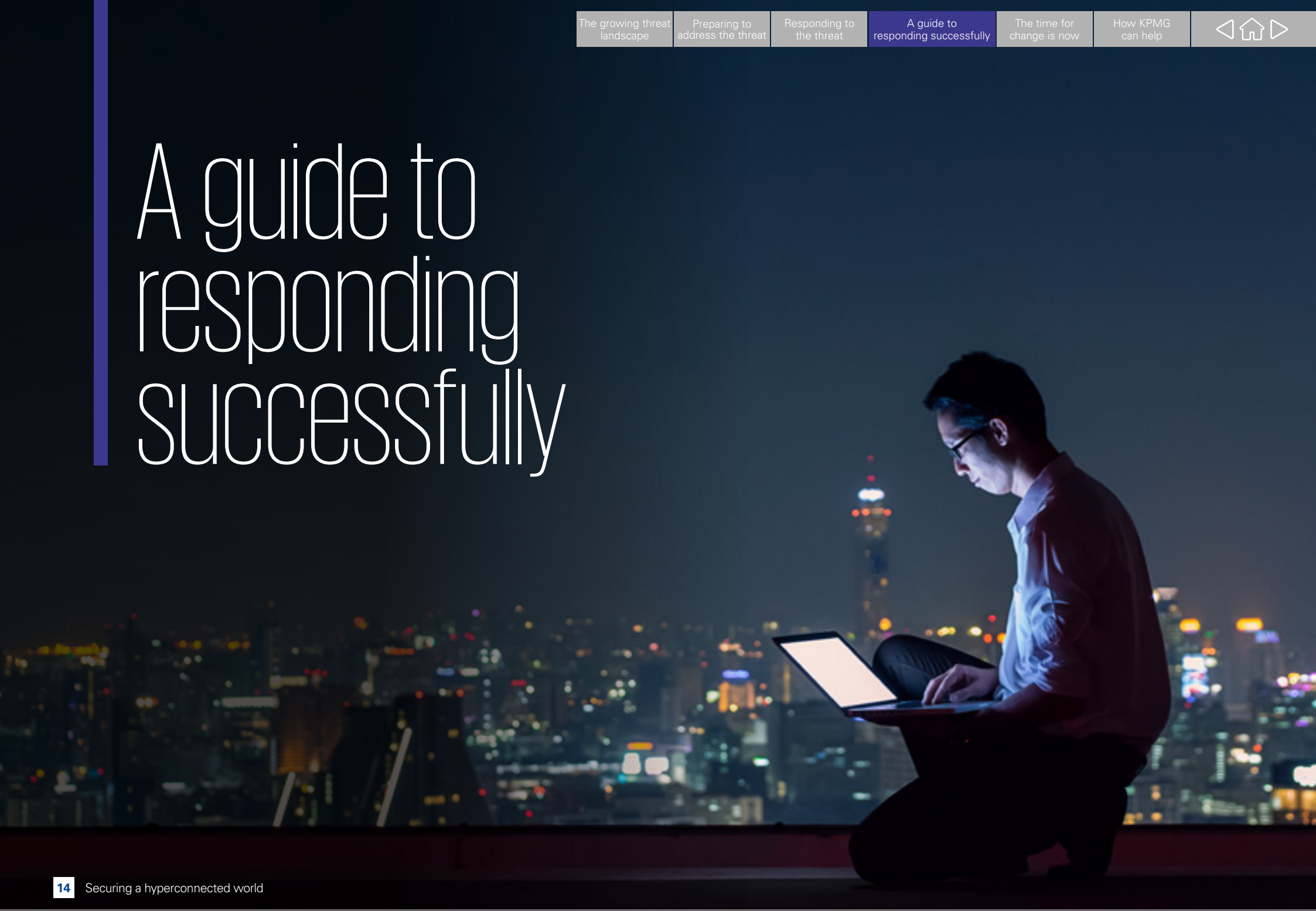
During a ransomware attack, information obtained by the attacker often consists of confidential or sensitive business data. There should be a classification at a high level to know what and where that information is and what the organization should do if compromised.

Recovery

Paying the ransom does not necessarily guarantee a prompt recovery of operations, either because there is no guarantee from criminals, or — as in the Colonial case — the decryption tool used could be slow and impractical. In any case, having a backup and recovery mechanism up-to-date and tested is crucial as a foundation for successful recovery.

All these situations imply the need to make high-impact decisions for the organization in a short period of time. That is why the response process should be defined, in advance, by the executive committee. It's common to see organizations place responsibility for this process on technology teams, but it's essential to orchestrate a distributed and coordinated business-wide effort that is governed by company leaders.

A guide to responding successfully



It can be said that many industrial companies share the same concerns regarding the maturity needed to respond to highly disruptive events. In most cases, an isolated and superficial idea of what should be done exists, but with no defined process involving the entire organization, much less a process that has been tested over time. Organizations typically face significant challenges in responding to these events, including:

Excessive confidence in the ability to respond

Industrial companies that have managed crisis scenarios in the past can become overly confident in their ability to manage a cyber incident. But beware — a cyber incident, especially ransomware, is an active, complex and ever-evolving threat that behaves nothing like a typical industrial accident or interruption.

Irregular regulatory demands

Unlike the financial sector, with cyber security regulation in place for more than a decade, regulatory requirements on cyber security are inconsistent in sectors using OT. They often differ by geography and in some cases are non-existent.

Excessive delegation to cyber security and IT teams

For years, industrial companies have delegated cyber security and other technology risk factors to cyber security and IT teams. But an incident requires strategic and well-coordinated action between cyber security, operations technology, engineering and other areas of the business.

Skepticism on the economic impact

Companies with a long-standing engineering tradition may find it challenging to picture how an incident in the digital realm could compare to a large-scale physical incident such as an oil spill or explosion at an industrial site. They may therefore be hesitant about investing the resources needed to prepare a comprehensive response.

Now is the time to respond seriously

With the proliferation of ransomware attacks in industrial sectors, organizations are finally coming to terms with the critical need to take response strategies seriously. To set the foundations for a strong cyber incident response program in OT environments, organizations should consider the following:

Responding successfully starts at the top

The C-suite should be responsible for ensuring operational continuity and should appoint a cyber security team to manage the necessary tools for success. This is especially true in industrial environments.

Key decisions before an event are not technical

Critical decisions cannot be made exclusively by cyber security and technology teams. Some are strategic and may require government coordination, for example when critical national infrastructure is concerned.

Smart preparation demands training

Preparation is key. Failure to formulate a plan risks serious consequences when an attack strikes. Issues and challenges are often not discovered until a scenario is rehearsed — and even then, the harsh reality typically surpasses simulations. The more scenarios that can be rehearsed in advance, the lower the chance of encountering something unpredicted.

Everyone has a role to play in a crisis

Often, the recovery process relies on highly skilled individuals with extensive knowledge of the network and industrial processes. They can identify smart solutions and workarounds based on their unique experience. With such high demand for skills in the cyber security industry, many businesses are now realizing that they cannot rely solely on a select few individuals.

Responding to large-scale ransomware attacks requires everyone in the organization to fully understand their role in a crisis. To help prepare and raise awareness of the implications of an effective response, it's highly encouraged for organizations to engage in testing and rehearsal exercises.

Bring a 'table-top' exercise to the boardroom

A well-defined 'table-top' exercise should help C-level leaders understand the importance of effective decision-making during a cyberattack. The exercise can expose opportunities for improvement and drive projects that have not been a priority in the past. It can also: define the team responsible for managing a cyber incident; identify how existing crisis management processes need to be adapted for a cyber incident; and reveal communications deficiencies and needs between board members, technical teams and corporate stakeholders.

Do not improvise

When the moment arises, have a well-designed and rehearsed plan with the right specialists to support with contention, forensics and recovery. Consider having a trained team either in-house or secured through a specialized firm on demand contract.

Cover for damage

Cyber insurance is becoming more widespread and even required in some settings. Although insurance may not cover for all potential damage (e.g. it doesn't cover all physical events, and it's unlikely that it will pay the ransom), it's a good method to reduce the economic impact of an incident.

Mandatory testing

On the other hand, in operations environments, it's mandatory to understand in advance the relationship between cyber security processes and physical processes. It's impossible to set up an effective response plan without considering the cyber-physical actions required in a cyberattack. These cyber-physical dependencies and their degree of cohesion are a key part of defining the Cyber Incident Response stage. These processes should be tested within a pre-approved time window, which adds to the complexity. Still, these tests can provide important and timely metrics.

Tested processes = critical metrics

- **The efficiency and effectiveness of the IT/OT communication chains**
- **The effectiveness of the technical and functional scripts**
- **The expertise of the cyber response team to deal with highly complex situations**
- **The proper functioning of the physical sub-processes achieved during the tests**

Another interesting testing scenario to consider involves simulating a system recovery from a cyberattack. The scope of operation for this type of test is very wide — from simply restoring a backup to the recovery of a process in a maintenance window. These tests can be useful in order to evaluate the correct operation of backups, assess the team's ability to recover a sub-process from scratch, review internal communications and generate 'realistic' training to the team in charge.

Finally, as demonstrated in all the examples, IT/OT teams should be one hundred percent integrated, working collaboratively and seamlessly as a unified team. Without this, the only one who will succeed will be the cyberattacker.

The time for change is now

It has been only a few months since a cyberattack attempted to harm the water supply in Oldsmar, Florida by gaining remote access to the system's control station and tried to increase the levels of sodium hydroxide. Had these cyber terrorists been successful, this attack would have put the health of thousands at risk.

Colonial Pipeline was not that lucky — operations were proactively shut down and the company paid a ransom estimated at US$5 million, only to discover the hacker's decryption tool was almost useless, leaving Colonial to execute its own backups to restore the system. And while Colonial was able to recover some of its extorted Bitcoins with the help of the FBI, the damage was done[8].

Today's harsh reality is that ever-evolving malware targeted at critical cyber-physical infrastructures is possibly one of the most dangerous threats to global infrastructure. Unlike cases akin to the water supply attack in Florida, an ad hoc action of limited reach, malware's tactics can be reused and enhanced over time. Furthermore, the slower rate of updates of cyber-physical infrastructure compared to pure digital infrastructure makes malware a threat for which timely preparation is key.

Given the highly connected nature of businesses today, it's no longer enough to protect infrastructure alone. This is particularly relevant to malware threats that benefit from the interconnectivity and weaker links in the chain. As organizations move farther and faster into a hyperconnected digital world, the protection of society is a shared responsibility, and everyone is required to play a part.

[8] US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers, CNN, June 8, 2021.

How can KPMG 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 expertise across the continuum — from the boardroom to the data center. In addition to assessing your cyber security and aligning it to your business priorities, we 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 expertise, deep business knowledge and creative professionals who are passionate about enabling you to protect and build your business. We will help you create a trusted digital world, so you can push the limits of what's possible.

Contributors

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

Anish Mitra
Associate Director, Cyber Security Services
KPMG in India

Sundeep Singh Kang
Manager, Cyber Security Services
KPMG in Germany

Nicolás Manavella
Partner, Cyber Security Services
KPMG in Argentina

Pablo Almada
Director, Cyber Security Services
KPMG in Argentina

Contacts

Walter Risi
Global Cyber IoT Leader and Partner, Cyber Security Services
KPMG in Argentina
E: wrisi@kpmg.com.ar

Akhilesh Tuteja
Global Cyber Security Leader and Partner
KPMG in India
E: atuteja@kpmg.com

Dani Michaux
EMA Cyber Security Leader and Partner
KPMG in Ireland
E: dani.michaux@kpmg.ie

Matt O'Keefe
ASPAC Cyber Security Lead and Partner
KPMG Australia
E: mokeefe@kpmg.com.au

Prasad Jayaraman
Cyber Americas Leader and Principal
KPMG in the US
E: prasadjayaraman@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name: Securing a hyperconnected world
Publication number: 137669-G
Publication date: October 2021