Cyberrisk Management in the Operational Technology (OT) Environment

A Guide for Boards of Directors

Cybersecurity Best Practices

A.10

Volume A:
A methodological approach

IDB

Cyber Israel
National Cyber Directorate

This document was originally published by the Israel National Cyber Directorate (INCD) in Hebrew. Its translation into English was carried out by the cybersecurity team of the Innovation in Citizen Services (IFD/ICS) division of the Inter-American Development Bank (IDB), and it is included as a chapter of the "Cybersecurity Best Practices" collection.

The reader should keep in mind that cybersecurity is a rapidly evolving field. Although these documents reflect established principles, they may be periodically updated as necessary to reflect developments in this field. Additionally, while every effort has been made to present the recommendations and resources in a way that is universally applicable to organizations around the world, the reader may find references that are specific to Israel's cyberecosystem and context (such as the amounts indicated in New Israeli Shekels [NIS], or references to Israeli law or government agencies).

The original document is available at: **https://www.gov.il/he/Departments/General/ot**. Please note that it includes the following disclaimer:

Contents

Foreword

Digital Transformation and the Challenges of Cybersecurity

As digital transformation continues to expand throughout the world, governments, organizations, individuals, and even objects are increasingly connected to the internet. Although digitalization offers undeniable benefits, such as efficient public service delivery, economic growth, and essential connectivity, it also contributes to our growing collective exposure to cybersecurity risks. Recently, the global COVID-19 pandemic has been an important driver of this phenomenon. As a result of widespread social distancing policies, the number of e-commerce transactions and online personal communications grew sharply in a short period of time, along with the number of employees who began teleworking for the first time. In this unprecedented situation, many internet users undertook novel online interactions without enough awareness of the security risks involved. Organizations had to quickly adapt to these challenges by setting up fully remote workflows, often without all of the necessary security measures in place or appropriate guidance to employees.

Cybercriminals are quick to exploit the uncertainty and vulnerability of unsuspecting individuals. Phishing and other social engineering scams proliferated, taking advantage of the global need for information related to the pandemic and the massive use of videoconference applications. In April 2020, Google reported more than 18 million daily malware and phishing emails related to COVID-19 in only a week. Hackers posing as the World Health Organization sent phishing emails and massively spread malicious links to fake videoconference meetings and attachments containing malware. According to the Check Point Research 2021 Security Report, in the first few months of 2020, almost a million attack attempts against Remote Desktop Protocol (RDP) connections, widely used among organizations for employees' remote connections, were observed every day. In fact, RDP attacks were the most popular form of cyberattack, surpassing even phishing emails. In the second half of the year, as more organizations strengthened the security of their remote platforms, hackers focused their efforts on exploiting vulnerabilities in employees' private assets and remote access devices to penetrate their organizations. Although such threats were maximized by this global context, they are not novel and will not go away; we continue to live in an environment of heightened risk, which is particularly serious in regions of the world where cybersecurity policies and technology are less developed and where citizen education and awareness around this issue are lacking. In other words, although the shifts due to the COVID-19 pandemic may revert to what they were before the pandemic, they have brought to light the urgent need to strengthen individual and collective protections against cyberrisks.

Strengthening cybersecurity is essential to safeguard citizens' rights to privacy and property in the digital sphere, promote citizens' trust in digital technologies, and support economic growth through safe digital transformation. In particular, citizens must be assured that the digital systems they use for their personal or professional activities, as well as those that involve their personal data, possess adequate security measures to guarantee the integrity, confidentiality, and availability of their information and the services that they need. Moreover, security breaches have a significant negative economic impact. A recent report by McAfee estimated that cybercrime costs the world economy around US$6 trillion annually, or 0.8 percent of global GDP.

Israel: A Global Leader in Cybersecurity

Israel's innovation and entrepreneurship ecosystem is globally recognized as one of the most vibrant in the world, earning it the name Startup Nation. According to the March 2021 OECD Science and Technology Indicators, Israel is the country that invests the highest percentage of its GDP (4.9 percent) in research and development (R&D). The country is host to more than 300 research and development and innovation (R&D&I) centers of multinational companies. Of these, dozens are dedicated to cybersecurity.

It is no surprise that 40 percent of all private investment in cybersecurity worldwide takes place in Israel, which also has one of the world's largest private ecosystems in this area, second only to that of the United States. According to 2021 data, in that year US$8.8 billion were invested in around 131 Israeli companies from this sector, and more than 40 were acquired for a total of US$3.5 billion. Israel has more than 500 cybersecurity startups, and by 2021, 33 percent of the world's "unicorns" were Israeli. Overall, Israel's export of cybersecurity products was estimated in 2020 at US$6.85 billion.

The Israel National Cyber Directorate (INCD) is responsible for securing Israel's national cyberspace and for establishing and advancing its cyberresilience. The INCD operates at the national level to constantly raise the level of security of organizations and citizens, to prevent and manage cyberattacks, and to strengthen cyberemergency response capabilities. Its positioning as part of the Prime Minister's Office clearly demonstrates the centrality and importance of its responsibilities. Its goals include to prepare and enable the Israeli private sector and general public to protect themselves from cyberthreats by adopting cybersecure technologies, publishing best practices, training personnel, and raising awareness. Furthermore, it aims to establish and strengthen the cyberscience and -technology base by developing highly qualified human capital, supporting advanced academic research, engaging in deep technological R&D, and fostering the cyberindustry. The INCD strives to maintain a protected, safe, and open cyberspace for all of the State of Israel's population and businesses and to facilitate the country's growth and its scientific and industrial base.

The State of Cybersecurity in the Latin American and Caribbean Region

The Inter-American Development Bank (IDB) carries out periodic assessments to capture the evolving capacities of its member states to defend themselves against the growing threats in cyberspace. The 2020 Cybersecurity Report, "Risks, Progress, and the Way Forward in Latin America and the Caribbean," developed in partnership with the Organization of American States (OAS), showed that countries were at varying stages of development in their preparedness to face cybersecurity challenges, but generally still had ample room for improvement.

While in 2016, the year of the report's first edition, 80 percent of the countries in the region did not have a national cybersecurity strategy in place, this number had only fallen to 60 percent by 2020. Furthermore, only a few countries manage the exposure of their critical infrastructure, such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors, to cyberattacks. As revealed by the 2020 report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrisome findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

In terms of countries' capacity to manage and respond to cybersecurity incidents, the same study found that 63 percent of countries had security incident response teams in place, such as computer emergency response teams (CERTs) or cybersecurity incident response teams (CSIRTs). However, of the 20 countries that did, only 3 had reached advanced maturity in their ability to coordinate such responses. In fact, 23 out of the 32 countries were still in an initial stage of maturity in this respect. This finding underscored the general need for countries to strengthen the capacity of their teams to effectively coordinate their responses to cyberincidents. Moreover, the report examined the availability of educational and training opportunities in cybersecurity and found that fewer than half of the countries in the region offered formal education in cybersecurity, such as postgraduate, master's, or technical degrees. Needless to say, having sufficient trained professionals is essential to design and implement the cybersecurity policies and measures that are necessary to ensure a country's resilience in the face of increasingly sophisticated and complex cyberattacks.

The Inter-American Development Bank's Support to Strengthen Cybersecurity Capacity in the Region

For the past few years, the IDB has actively supported the region in the development of cybersecurity capacity, the design and implementation of national-level cybersecurity policies, and the strengthening of cybersecurity capabilities in the sectors it helps develop. This support takes a number of forms. The IDB has provided financial assistance amounting to tens of millions of dollars to develop national cybersecurity capabilities through more than 15 public sector investment loan operations, as well as significant additional funding to ensure the cybersecurity of digital transformation investment projects.

It also provides technical guidance and conducts cybersecurity projects across the region through consultancies, assessments, and tailor-made cybersecurity-strengthening projects on topics that include critical infrastructure protection, cybercrime and forensic analysis, design and strengthening of CSIRTs and security operations centers (SOCs), and national and sectoral cybersecurity strategies. In addition, the IDB has made substantial efforts to provide opportunities for Latin American and Caribbean professionals to strengthen and update their skills in this field by regularly offering workshops and training opportunities. These have included two-week cybersecurity executive courses, offered jointly with the Hebrew University of Jerusalem, as well as tailor-made courses on critical infrastructure protection and others targeted for specific sectors. Finally, the IDB has produced several high-impact publications dealing with national and sectoral cybersecurity issues, and continues to update and add to this body of knowledge regularly.[1]

1. See the website of the Data and Digital Government Cluster (DDG) of the IDB's Innovation in Citizen Services (ICS) division: **https://www.iadb.org/en/reform-modernization-state/data-and-digital-government-cluster**.

The IDB and the INCD: Joining Forces

The challenges of cybersecurity, like those of the internet itself, are global. Thus, sharing the knowledge and tools to meet these challenges benefits everyone. In recognition of this reality, the INCD and the IDB have partnered to make Israel's expertise in this area accessible to LAC countries. This collaboration has supported the LAC region in the form of executive and technical trainings on advanced cybersecurity topics, cutting-edge conferences for LAC public officials and professionals in the field, and innovative technical assistance projects. This publication is a product of this collaboration. It consists of a series of cybersecurity methodological guides for organizations, developed by the INCD in light of its analysis of risks, attack methods, cyberincidents, and globally accepted standards. These guides have been translated into Spanish and English as a joint activity of both organizations. They are being made available in these languages with the aim of providing access to this body of knowledge to audiences throughout the LAC region and contributing to strengthening cyberresilience in the region.

The challenge of protecting the digital space will continue to grow, along with the need for proven expertise to confront it. The insights contained in these guides are a resource to promote much-needed professional training in cybersecurity in the LAC region. These guides will contribute to raise organizational standards, promote greater awareness and a culture of cybersecurity within organizations and among the general public, and inform decision makers, managers, and leaders in their cybersecurity initiatives. It is our hope that these guidelines will serve as a roadmap for professionals and leaders throughout the LAC region, working together to build a more secure and prosperous future.

Background

In recent years, there has been an increase in the number of reported cyberincidents in operational technology network environments (hereinafter "OT networks"). In a study conducted among 300 industrial companies in 2018, about 49 percent of the companies surveyed indicated that they experienced cyberincidents in the OT environment; about a year later, this number rose to 60 percent (Kaspersky Labs, 2019a). Similarly, a study conducted in 2019 among 700 companies found that in the last two years, 90 percent of them experienced at least one cyberevent in the OT environment, with 37 percent of companies experiencing four or more events (Ponemon Institute, 2019).

Another survey conducted among about 350 IT and OT officials from around the world found that about 83 percent of them defined the level of cyberrisk posed by the OT environment as moderate and above, and of them, about 13 percent stated that it was critical (Filkins, Wylie, and Dely, 2019).

It follows that cyberrisks are becoming a significant part of the total operational risks to which organizations are exposed. If realized, they may have various business consequences including damage to human life, environmental damage, reputational harm, loss of revenue, and legal exposure. The vast scope of cyberevents is forcing senior management to study the issue in depth and ask educated and strategic questions about it. Cyberprotection is no longer a concern only of the IT department.

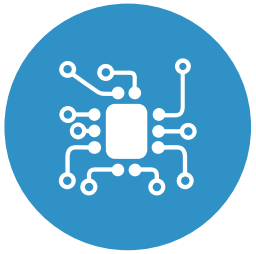
The sharp increase in the number of cyberincidents in OT in recent years is due, among other things, to the availability of attack tools and the ability to use them, as well as the ability to take advantage of the connectivity between administrative networks (hereinafter "IT networks") and OT (Kaspersky Labs, 2019b).

In the past, when OT networks were designed and built, cyberprotection considerations were not always taken into account. This was, among other reasons, because these networks were supposed to be cut off from the outside world. Today, in the era of Industry 4.0—a modern management concept that advocates for the integration of technologies and diverse communication interfaces—OT network systems are connected to the IT network's information systems and are also exposed to remote access by support and maintenance factors. These communication channels expose the control systems of operational processes to cyberrisks to which they were less exposed in the past.

This guide presents the key protection objectives that characterize OT networks and provides the board of directors with tools for conducting a discussion to obtain an initial picture regarding management of the cyberrisks that can affect OT networks. Along with a concise review of the principles of cyberrisk management and a focused explanation of the typical protection objectives, this guide includes material questions that the board of directors is required to ask in order to assess the effectiveness of the cyberrisk management process in the OT network environment.

/01. Impact of a Cyberincident on Operational and Business Objectives

The realization of cyberrisk in the OT environment may harm one or more of the following operational and business objectives of the organization (Stouffer et al., 2017: 8):



01

Employee safety: For example, utilizing an access and remote control channel in favor of disrupting settings in an industrial controller leads to a steam boiler explosion.

02

Environmental protection: For example, disruption of sensor function causes excess sewage flow or an uncontrolled chemical process that leads to the spread of toxic gas.

03

Product quality: For example, unauthorized modification of production data may shorten the shelf life of a food product.

04

Production targets: For example, shutting down a production line for a significant period of time as a result of the intrusion of ransomware may lead to a violation of the organization's production targets and obligations to its customers.

05

Trade secrets: For example, a document describing the unique manufacturing process is leaked.

In general, unlike in an IT environment, the focus in the OT environment is on maintaining the integrity of the operational process and protecting human life. In light of this fact, there is a need for an appropriate risk management process and identification of appropriate security controls. Therefore, the challenge is making changes that include implementing new cybercontrols or enforcing existing ones.

To encourage a gradual process, focusing on the main risks, the following are the protection objectives typical of the OT environment that should be considered first:

- Cyberprotection governance.
- Cyberrisk management in the OT environment.
- Cyberrisk areas typical for the OT network.
- Monitoring and responding to cyberincidents.

In the future, organizations are advised to focus further on additional areas of activity and protection objectives depending on their importance to the organization. In order to get a complete picture of the cyberresilience of the OT environment, a comprehensive risk survey should be conducted. For more details, see the template for conducting a risk survey in the OT environment.[2]

2. The document *Working Template for Conducting a Cyberrisk Survey in Industrial Control Systems (ICS)* is available as part of this "Cybersecurity Best Practices" collection.

/02. Cyberprotection Governance

Cyberrisk management in an OT environment is a unique challenge because a typical OT environment combines up-to-date technologies from the field of IT alongside older technologies used in industrial control systems. Therefore, the responsibility for operating systems in OT networks is divided between control engineers and other operations personnel and the cyberprotection management and information systems personnel. As a result, the knowledge required to identify and manage cyberrisks in an organization is distributed among several bodies within the organization.

To simplify this management, in many organizations the distribution of knowledge among these officials is as follows:

01

Control engineers and operations personnel (usually in the OT environment). These factors focus mainly on ensuring the availability and integrity of operational processes. They are deeply familiar with the OT network and its technological components and are aware of the sensitivity of these components to changes and other external influences. Such a sensitivity can lead to failure and impairment of the availability of operational processes. In many cases, these factors lack the full knowledge required to identify cyberrisks and assess the likelihood of their realization, which may also lead to impairment of the availability of operational processes.

02

Cyberprotection management and IT personnel, who focus mainly on cyberrisk management in the IT environment. These factors are familiar with the map of cyberthreats and are proficient at controlling, operating, and maintaining cyberprotection systems in the administrative network environment. Often, these factors lack the knowledge required to understand the OT network environment and the sensitivities that characterize it.

Because of this division, many organizations lack clarity about the division of authority and responsibility between the various factors. This division may impair the effectiveness of the cyberrisk management process in the OT environment, resulting in a possible compromise of the organization's operational and business objectives.

In light of the above, the organization's management should appoint an agent that will be in charge of cyberprotection in the OT network environment, define its areas of authority and responsibility, and ensure that it has all the necessary skills to manage cyberrisks in the OT network environment.

It is recommended that this agent have knowledge in the following areas (Weiss, 2017):

01
Understanding the operational process.

02
Understanding control systems and their unique characteristics.

03
Familiarity with risk management methodologies in general and cyberrisk management in the OT environment in particular.

04
Understanding the threat map and common attack methods.

05
Familiarity with professional standards and how they are implemented among people, processes, and technological components.

06
Ability to practically bridge the differences between information systems and the world of operations.

The agent in charge of cyberprotection in the OT environment may be an operations person who has been trained in the field of cyberprotection or, alternatively, an IT person who has received training in the field of OT.

Part of the activity of the agent in charge of cyberprotection in the OT environment is assisting management in setting policies and formulating procedures (ISACA, 2015: 6).

Questions for the Board of Directors

These questions focus on cyberrisk management policies.

01
What is the status of cyberdefense in the organization and in the OT environment?

02
Has the organization appointed a person responsible for cyberprotection in the OT domain?

03
To whom does the person in charge of cyberprotection in the OT domain report: to a factor from the operational domain, the business domain, or the cyberprotection domain?

04
Have the limits of authority and responsibility of the person in charge of cyberprotection been defined in a way that will ensure the effective implementation, enforcement, and monitoring of cyberprotection controls in the OT environment?

05
Was the person responsible for the cyberprotection domain given the skills required to manage and implement cyberprotection in the OT environment?

06
Have the resources and tools required to fulfill the role been allocated to the person responsible for cyberprotection?

07
Have policies and procedures for cyberprotection in the OT environment been formulated?

/03. Cyberrisk Management in the OT Environment

Guiding Principles for Cyberrisk Management in the OT Environment

To effectively monitor the cyberrisk management process, the National Association of Corporate Directors has defined five principles that board members are required to apply (NACD, 2020: 6):

01

Addressing cyberprotection in the context of general organizational risk management and not as an issue relevant in aspects of information systems only. In this context, the organization should also analyze the impact of cyberattacks on the achievement of operational and business objectives.

02

Understanding the legal consequences of cyberattacks with respect to compliance with the Privacy Protection Bill and its regulations or requirements.

03

Acquiring the knowledge required to periodically conduct effective discussions in the field of cyberrisk management, allocating an appropriate time frame for this purpose.

04

Presenting their expectations for management regarding the need to implement a cross-organizational risk management policy to which adequate resources and staffing have been allocated.

05

A management discussion on how to handle major risks and approval of the risk map.

Prominent Frameworks for Cyberrisk Management in the OT Environment

There are various methodologies for managing cyberrisks in the OT environment, including the following (International Organization for Standardization, 2018; NIST, 2018):

01

NIST Cybersecurity Framework Manufacturing Profile (Stouffer et al., 2017).

02

ISA/IEC 62443.[3]

03

Reducing Cyberrisks for Industrial Control Systems (ICS), available as part of this "Cybersecurity Best Practices" collection.

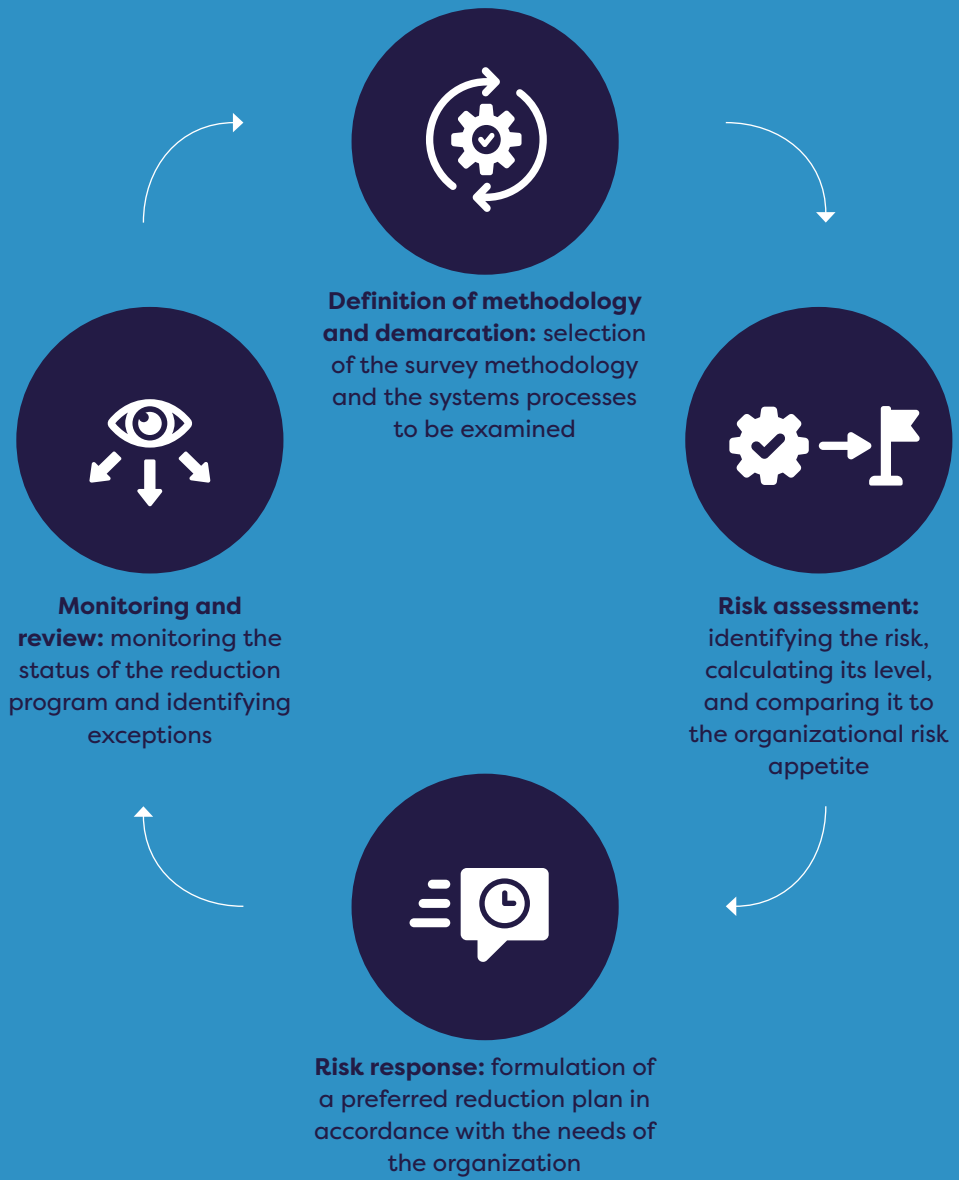
04

Cyber Defense Methodology for an Organization (INCD, 2017).

According to leading methodologies, the main steps in the risk management process are shown in Figure 1.

3. More information about this standard is available at **https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/**.

Figure 1. Main Steps in the Risk Management Process



Formulation of Key Risk Indicators

Key risk indicators (KRIs) are measurable data that can be compared to predefined thresholds. Their purpose is to identify shifts in trends, thus enabling the organization to respond before those trends materialize as a result of a malfunction or a cyberincident.

By identifying shifts in trends over time, KRIs constitute an additional tier to the risk surveys that are conducted periodically. The following are some examples of the usefulness of KRIs in the OT environment:

01

Several intrusion attempts halted by the organization's firewall (FW) in a month.

02

Calculation of the relative share of downtime in the production line.

03

Number of virus outbreaks and other malware in a quarter.

Questions for the Board of Directors

These questions focus on cyberrisk management in the OT environment.

01
Has a framework or methodology been adopted for managing cyberrisks in the OT environment?

02
Are there cyberrisks in the OT environment?

03
How is cyberrisk management in the OT environment integrated into the organization-wide risk management process?

04
How was it decided which protection objectives and areas of organizational activity would be included in cyberrisk management activities in the OT environment?

05
Have risks with potential legal consequences been identified and mapped?

06
Does the organization conduct proactive resilience tests?

07
Do the resources allocated to reducing cyberrisks in the OT environment meet the needs of the organization?

08
What is the status of the work plan in relation to the risks identified, and are they treated in accordance with the set timelines?

09
Have KRIs been defined that make it possible to identify shifts in trends and take effective action to reduce the likelihood of a cyberincident occurring?

/04. Typical Cyberrisks for the OT Network

Today, OT networks are frequently linked to additional networks: for example, the IT network is linked to the internet network. This link may allow an attacker who gains a foothold in the organizational/managerial network to extend their attack to other networks.

This is a departure from past practice, where traditionally the OT network and the IT network ran separately and without interfaces, so that the OT network was completely isolated from the organization's administrative network and the public internet network.

In recent years, in the context of the Fourth Industrial Revolution (Industry 4.0), this configuration has changed. Modern computing and communication technologies are converging with manufacturing technologies, leading to a new phase of value creation. The availability of information in real time through communication between all factors involved in the process leads to dynamic networks, which improve in real time, are independently organized and cross-organizational, and add value (VDMA, 2016: 3).

To realize the vision of a converged organization, many organizations choose to set up interfaces between the OT network and the organization's IT network and internet network. In addition, the trend of connecting end components through wireless communication—the Industrial Internet of Things (IIoT)—leads to the establishment of many additional interfaces between the OT network and other organizational networks and public networks.

In addition to the operational and business benefits, these interfaces constitute a possible attack vector for hostile elements. Therefore, it is extremely important to map and secure these interfaces.

Remote Access

The operational need for employees, suppliers, and manufacturers outside the organization to maintain and support the systems involves, among other things, granting remote access permissions. Sometimes, the possibility of remote access to the OT network for the purpose of providing service and support is based on a collaboration agreement, as a requirement of the equipment suppliers.

To ensure that remote access is secured and granted to authorized parties only, care must be taken to grant access against a dedicated network component enforcing strong identification and encrypting communication channels, while avoiding granting direct access to controllers and other components in the OT network. This process should be carried out proactively and under full supervision.

Using an Insecure Communication Channel

For communication between the control room and the OT network components located in different buildings or at remote sites, wireless communication channels are often used with technologies such as radio (VHF, UHF), cellular communication, satellite, and Wi-Fi. Some of these technologies have inherent weaknesses and gaps.

Mapping Systems and Components in the OT Environment

Mapping systems and components in OT networks is a challenge, since in many cases these are decentralized networks that were established decades ago, and they include a variety of components from different manufacturers. The lack of such mapping complicates the process of identifying vital assets carried out as part of a cyberrisk survey and impairs the ability of ongoing monitoring to identify exceptional events in the OT network that may result from an operational malfunction or cyberattack.

/05. Monitoring and Responding to Cyberincidents

Changing Perception in Cyberdefense

In the past, the concept of information security action focused on **preventing intrusion** into the organization's information assets. As a result, many organizations focused their resources mainly on **identification actions** such as conducting risk surveys, implementing tools, and taking **protective actions** such as controlling access to information, installing firewalls and antivirus, and increasing employee awareness.

Today, as the intensity and sophistication of attacks have increased significantly, a new approach to cyberdefense has been developed, which assumes that a determined attacker will eventually hack into the organization. Thus, the emphasis in dealing with cyberrisks combines **prevention** capabilities alongside a combination of detection, response, and proactive defense capabilities.

In light of the above, in addition to the identification and protection activities that need to be continued, organizations are required more than before to strengthen their **detection** capabilities such as the implementation of monitoring systems, and their **response** capabilities, including formulating a procedure and establishing an event response team and offering training. This will enable the organization to identify attacks as soon as possible after their onset and respond effectively to minimize the damage of the attack.

Monitoring and Identifying Faults and Cyberincidents

Monitoring, as defined by the U.S. National Institute of Standards and Technology (NIST), is: "Inspection, supervision and constant examination or determination of status for the purpose of identifying a change in the level of activity required or expected" (NIST, n.d.). Further to this, cyberincident monitoring needs to identify anomalies that may indicate the realization of a risk that was maliciously caused by a hostile factor and not the result of a malfunction.

The usual practice in manufacturing environments is to monitor abnormality or malfunction of component activity to ensure the integrity of the operational process. The increase in the scope of cyberthreats requires expanding monitoring capability so that it will also provide a solution for identifying cyberincidents.

Response to Cyberincidents in the OT Network Environment

Many organizations have formulated response procedures and established dedicated teams to deal with extreme events resulting from operational or safety failures in the OT network environment. These procedures focus on reducing the damage to human life and/or harm to the environment as well as restoring the operational process to proper functioning within the shortest time possible.

In most cases, the response procedures formulated do not address cyberscenarios, and therefore response teams do not include cyberdefense personnel and do not address the unique characteristics of cyberincidents. Unlike an operational malfunction, a cyberincident in the OT network environment may be continual and cause further damage due to the inability to identify the root cause, contain the attack, and formulate an appropriate response. Thus, when formulating response procedures, it is advisable to also consider cyberscenarios and involve cyberprotection personnel both in the process of formulating the procedures and as part of the response team.

An effective response to a cyberincident addresses, among other things, the following aspects (NIST, 2012: 21):

01

Integrating a cybersecurity team into an event from the first stage of reporting it.

02

Event analysis and treatment prioritization in cases of multiple events.

03

Stopping the spread of the attack, identifying its source, and gathering relevant evidence.

04

Drawing conclusions and retaining evidence gathered.

Questions for the Board of Directors

These questions focus on monitoring and responding to cyberincidents.

01

How and with what tools does the organization monitor cyberevents in the OT environment?

02

How is the organization prepared for dealing with and responding to cyberincidents in the OT environment?

03

Were criteria defined for immediate reporting to management and to the board of directors following the occurrence of an extreme incident?

04

Was a process formulated for conducting an investigation, drawing conclusions, and implementing solutions following cyberincidents in the OT environment?

References

- CISCO. 2018. IT/OT Convergence Moving Digital Manufacturing Forward. **https://www.cisco.com/c/dam/en_us/solutions/industries/manufacturing/ITOT-convergence-whitepaper.pdf**.
- Filkins, B., D. Wylie, and J. Dely. 2019. SANS 2019 State of OT/ICS Cybersecurity Survey. June. **https://www.forescout.com/resources/2019-sans-state-of-ot-ics-cybersecurity-survey/**.
- INCD (Israeli National Cyber Directorate). 2017. Cyber Defense Methodology for an Organization, Version 1, June. **https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf**.
- International Organization for Standardization . 2018. ISO 31000:2018 Risk Management: Guidelines. **https://www.iso.org/iso-31000-risk-management.html**.
- ISACA. 2014. Cybersecurity: What the Board of Directors Needs to Ask. August. **https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoGFEA0**.
- ———. 2015. The Cyberresilient Enterprise: What the Board of Directors Needs to Ask. **https://assets.ctfassets.net/82ripq7fjls2/5VE6C6a3ABbbp3e8cfZVx3/de4d299f3c-46f82a248925796b16af8a/ISACA_The-Cyberresilient-Enterprise_eBook-2015.pdf**.
- Kaspersky Labs. 2019a. The State of Industrial Cybersecurity. **https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf**.
- ———. 2019b. Threat Landscape for Industrial Automation Systems. **https://ics-cert.kaspersky.com/media/KL_ICS_CERT_H2_2018_REPORT_EN.pdf**.
- NACD (National Association of Corporate Directors). 2020. NACD Director's Handbook on Cyber-Risk Oversight. February. **https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298**.
- NIST (National Institute of Standards and Technology). 2012. SP 800-61 Rev. 2: Computer Security Incident Handling Guide. August. **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**.
- ———. 2018. SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. December. **https://doi.org/10.6028/NIST.SP.800-37r2**.
- ———. n.d. Glossary. **https://csrc.nist.gov/glossary/term/monitoring**.
- Ponemon Institute. 2019. Cybersecurity in Operational Technology: 7 Insights You Need to Know. March. **https://static.tenable.com/marketing/research-reports/PonemonReport-Cybersecurity_in_Operational_Technology.pdf**.
- Stouffer, K. A. et al. 2017. National Institute of Standards and Technology Interagency Report (IR) 8183, Cybersecurity Framework Manufacturing Profile. September. **https://doi.org/10.6028/NIST.IR.8183**.
- VDMA. 2016. Guideline Industrie 4.0: Guiding Principles for the Implementation of Industrie 4.0 in Small and Medium Sized Businesses. May. **https://www.vdma.org/documents/34570/0/Guide%20to%20Industrie%204.0.pdf/1ca94350-1631-465a-e73c-47cd1d5b412d**.
- Weiss, J. 2017. What Executives Need to Know About Industrial Control Systems Cybersecurity. International Society of Automation (ISA) White Paper. April. **https://www.isa.org/getmedia/4b3f6d2e-8d9e-45ed-a563-6ddfc42d0ae3/ISA_WP_Executives-Cybersecurity.pdf**.

In recent years, there has been an increase in the number of reported cyberincidents in operational networks, which has intensified awareness of the issue and its importance. Cyberrisks are occupying an important place in the management of organizational risks in light of the possible consequences: harm to human life, environmental damage, reputational harm, loss of revenue, and legal exposure. This document was written especially for the use of boards of directors as part of a comprehensive project of the INCD in the field of industrial control systems (ICS). It includes a professional extension document[4] and a working template for conducting a cyberrisk survey in the industrial sector. This document is intended to provide a framework for an ongoing dialogue between the board of directors and management regarding the management of cyberrisks in the operational technology (OT) environment.

4. The document *Reducing Cyberrisks for Industrial Control Systems (ICS)* is available as part of this "Cybersecurity Best Practices" collection.

Cyberspace is a field of opportunities in terms of technological progress, connectivity, integration, and global connection to the internet. But it is also a field of threats and risks. Cyberattacks can harm organizations and inflict significant financial and image damage. To be prepared to defend against cyberthreats, an organization must master a large number of specializations, whether they are technological, organizational, or process centered. The list of documents presented below reflects the state of the collection at the time of publication of this document.

Volume A: A methodological approach

- **A.01** Cyberdefense Methodology for an Organization 1.0
- **A.02** Cyberdefense Doctrine 2.0
- **A.03** Use of Cloud Services: Addendum to the Organizational Cybersecurity Methodology
- **A.04** Organizational Coping in Cyberspace: The Insider Threat
- **A.05** Organizational Preparedness for a Cybercrisis
- **A.06** Supply Chain
- **A.07** Focus Questions for Cybersecurity Policymakers
- **A.08** Recommendations for Information Security and Reduction of Cyberrisks for Small Businesses
- **A.09** Cyberpractice: Creating and Conducting Cybersecurity Exercises for the Organization
- **A.10** Cyberrisk Management in the Operational Technology (OT) Environment
- **A.11** Risk Assessment Template: Retail Sector
- **A.12** Cyberpractice: How to Plan a Cybersecurity Awareness Program

Volume B: A technical approach

Volume C: Secure software development