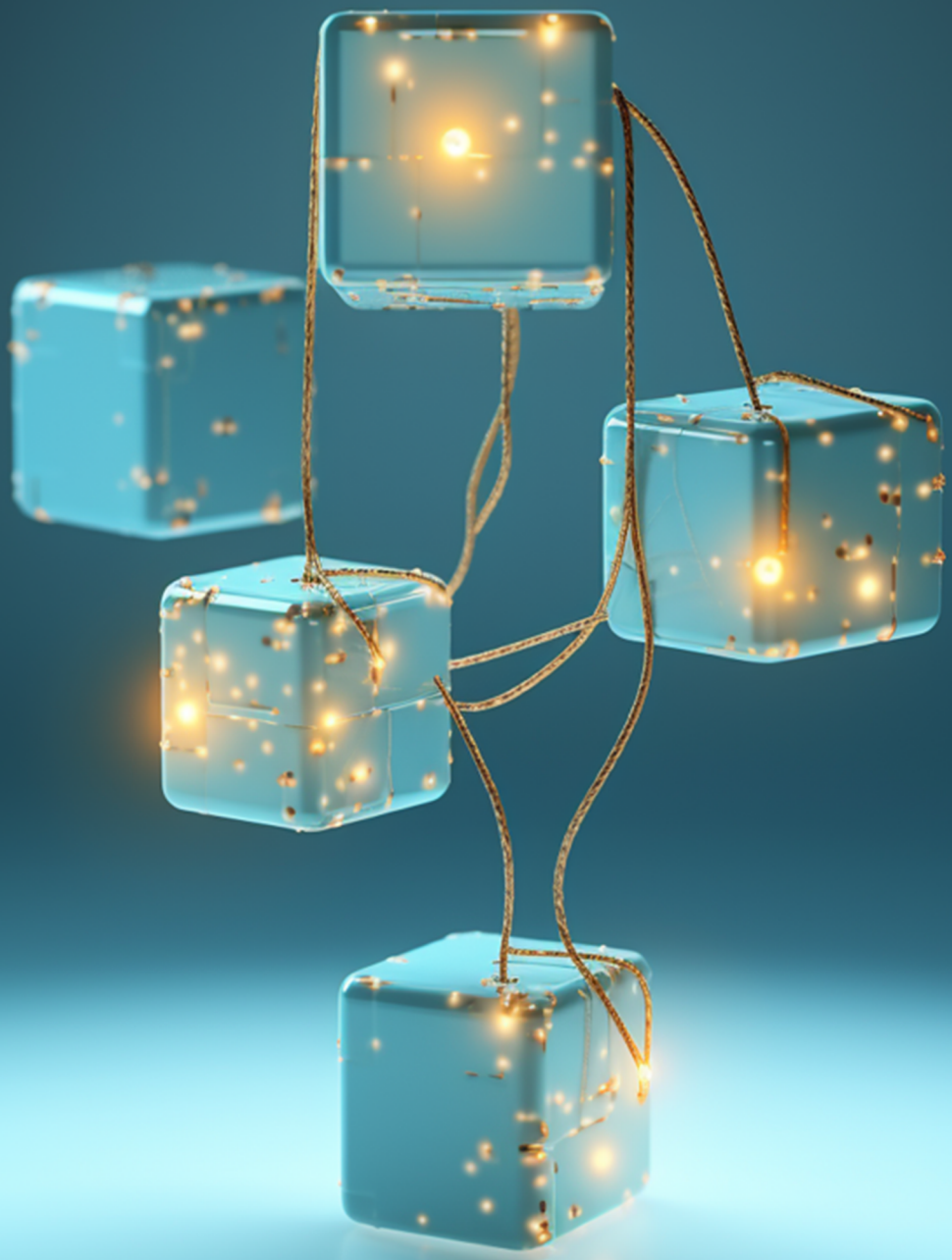
WORLD ECONOMIC FORUM

Unlocking Cyber Resilience in Industrial Environments: Five Principles

WHITE PAPER

NOVEMBER 2023



Images: Midjourney, Getty Images

Contents

Executive summary

The digitalization and connectedness of industrial environments is opening up business opportunities and enhancing operational efficiency. At the same time, it exposes organizations to cyberattacks that can offset these gains.

Today's industrial environment consists of operational technologies (OT) which, according to some sources, are largely outdated.[1] They have interoperability and connectivity limitations, and weak or no security management capabilities and procedures.[2]

The increased convergence of OT with the traditional IT environment is leading to an increase in inherent vulnerabilities, which are doubling every year.[3]

The OT environment is fundamental for ensuring the continuation of industrial operations that keep global economies and infrastructures running. To improve OT environment security, the World Economic Forum in collaboration with partners from the electricity, manufacturing, and oil and gas industries, has developed a list of guiding principles. Combined with a set of best practices, these aim to help cyber leaders ensure a cyber resilient OT environment for uninterrupted and efficient business operations.

Principle 1: Perform comprehensive risk management of the OT environment.

Principle 2: Ensure OT engineers and operators of installations have responsibility for OT cybersecurity.

Principle 3: Align with top organizational leadership, strategic planning teams and third parties to make security-by-design a reality.

Principle 4: Make cybersecurity standards and best practices contractually enforceable on partners and vendors to build a cybersecure OT environment.

Principle 5: Run joint tabletop exercises to ensure preparedness in case of an actual incident.

These principles and best practices can help organizations safeguard, maintain and monitor their industrial OT environment as well as ensure business continuity. While many organizations may already have some measures in place to ensure a cyber resilient OT environment, shared guidance can help manage cyber risks at the ecosystem level to increase systemic resilience.

Introduction

Why does OT cybersecurity matter?

The industrial infrastructure and operations landscapes are undergoing a profound transformation due to technological innovation. A growing convergence of information technology (IT) and operational technology (OT) is driven by the rapid adoption of cutting-edge technologies like big data, digital twins and the industrial internet of things (IIoT). These two domains are expected to become increasingly intricate and interconnected over time. This inexorable shift is exemplified, in part, by the projected IIoT market growth,[4] which is expected to surge from approximately $85.5 billion in 2023 to nearly $169.6 billion by 2028.

What is the difference between IT and OT?

Information technology refers to technologies including computers and networks that store, process and transmit information, while operational technology encompasses industrial control systems (ICS) that operate, control and monitor industrial equipment and processes.

The growing synergy between IT and OT, commonly referred to as IT/OT convergence, presents numerous opportunities for industrial organizations. These include remote control; real-time monitoring; enhanced visibility of machinery, plants and assets; simplification of anomaly detection; improved operational efficiency and productivity; and faster decision-making processes.

However, this newfound connectivity between OT devices and IT networks also expands the cyber risk landscape, introducing both intentional and unintentional cybersecurity threats. Traditionally, the OT environment remained "air-gapped," meaning it was not connected to the internet, and external hardware and removable media (e.g. USB drives) were the primary cybersecurity concerns. As these two environments merge, cybersecurity breaches can infiltrate from IT to OT through means such as internet malware infection and unauthorized access via mobile devices.

Today, OT environments, in large part, rely on legacy technologies built to perform specific tasks and operating on specialized software and proprietary protocols. Often designed without cybersecurity in mind, many of these legacy systems have been produced by now-defunct manufacturers whose software updates are infrequent and difficult to implement, ultimately leaving them exposed to security threats. In fact, a recent study by Microsoft found that 75% of industrial control devices are unpatched and feature high-severity vulnerabilities.[5] Other threat factors include improper network segmentation – which, according to Dragos, happens to be the case for 50% of organizations[6] – or poor remote-access practices.

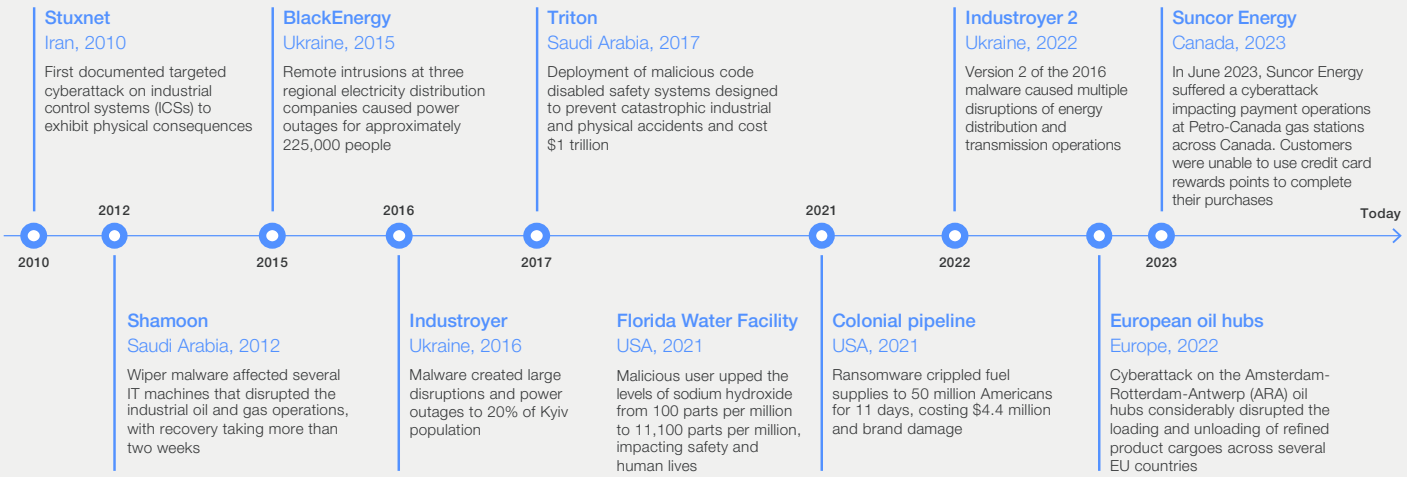
Malicious actors do not shy away from exploiting such vulnerabilities. A report by McKinsey shows that OT cyber events have increased by 140% from 2020 to 2021.[7] Of those events, 35% sustained physical damage with an estimated impact of $140 million per incident.[8] That said, it is important to note that not all industries are equally impacted by OT attacks. For instance, since 2021,[9] the manufacturing sector has been the most targeted, experiencing 61% of cyberattacks. The oil and gas (11%), transportation (10%) and utilities (10%) sectors have been next.

> Since 2021, the manufacturing sector has been the most targeted, experiencing 61% of cyberattacks. The oil and gas (11%), transportation (10%) and utilities (10%) sectors have been next.

Organizations in the manufacturing, oil and gas, and electricity industries bore damages amounting to $2.8 million on average in 2021.[10] In addition to financial losses (directly from the damage and from related downtime), data and intellectual property theft, and reputation damage, cybersecurity breaches in OT environments can have consequences such as:

- Damage to the environment.
- Exposure of people and personnel to dangerous conditions. Gartner predicts that by 2025, malicious actors will be able to weaponize the OT environment to cause harm or loss of life.[11]
- Reduced availability and quality of essential goods and services including energy, healthcare and transportation; this can trigger behaviours such as panic-buying and stockpiling by consumers.
- Legal and regulatory violations resulting in fines, lawsuits and regulatory scrutiny.
- Implications for national security and public safety, given that OT is a significant component of critical infrastructure, and any level of cybersecurity risk can be considered critical.

FIGURE 1 | **Cyber incidents in the oil and gas industry**



What are the sources of risks?

Cybersecurity risks in the OT environment are amplified by several overarching issues that are not always technical in nature but depend on factors such as corporate culture and governance. These include:

Lack of emphasis on cyber issues in operations and shortage of personnel for OT cybersecurity.

Human error – research shows that 79% of OT experts consider human error to be the greatest risk for OT systems.[12] Moreover, the current onboarding and training of OT personnel do not sufficiently ensure that they adopt appropriate policies and measures for OT cybersecurity.

Unclear delineation of process ownership and prioritization of risks.

The IT/OT convergence has blurred process ownership, allowing for no clear delineation of responsibilities and obligations between the IT and OT teams. In addition, the two view their priorities differently. From the IT perspective, procedures for data security and privacy are crucial, whereas the OT team places primary focus on physical performance and safety of facilities and equipment.

Poor device/asset visibility and rapid introduction of new assets.

While the creation and maintenance of an asset inventory in the OT environment is regarded as one of the top security controls, according to Dragos,[13] as many as 80% of organizations lacked visibility of the OT environment in 2022. Organizations need to have an overview of the devices in their networks – for instance, whether these devices are obsolete or supported, their vulnerabilities and what they are connecting to – both in the IT and OT environments. Organizations should be able to investigate the systems and processes in each zone and provide recommended security controls.

Supply chain and third-party risk.

A study found that 40% of OT cybersecurity practitioners consider supply chain/third party access to the OT environment to be one of the top three cybersecurity risks.[14] Whereas such concerns may be motivated by the weaker cybersecurity practices of third parties, OT cybersecurity can also be compromised by deliberate tampering of third-party hardware, software or firmware. This can happen during the manufacturing, distribution or maintenance processes.

To ensure a strong cybersecurity posture across organizations and industries, robust cybersecurity measures must be developed and implemented to protect both IT and OT environments.

What are the existing cybersecurity frameworks for the OT environment?

Organizations are not starting from scratch when it comes to OT cybersecurity. In fact, a number of cybersecurity frameworks have already been developed for the OT environment.

The International Electrotechnical Commission (IEC) 62443[15] is an international series of standards that tackle cybersecurity for industrial automation and control systems. The National Institute of Standards

and Technology (NIST) has released SP 800-82[16] – a guide on how to improve the security of OT systems; while the European Joint Research Centre has proposed a framework on Industrial Automation and Controls Systems (IACS) to share practices on IACS products' cybersecurity certifications.[17]

Other examples of cybersecurity frameworks applicable to the OT environment and beyond include the NIST Cybersecurity Framework[18] as well as the Cybersecurity Capability Maturity Model (C2M2).[19] Efforts have also been made at the local level to enhance OT cybersecurity. For instance, Saudi Arabia has developed the Operational Technology Cybersecurity Controls. Similarly, oil and gas companies on the Norwegian continental shelf follow guidelines such as NOG 104, NOG 110 and NOG 123, while in the US, the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) and the American Petroleum Industry Pipeline Security standards are of relevance.

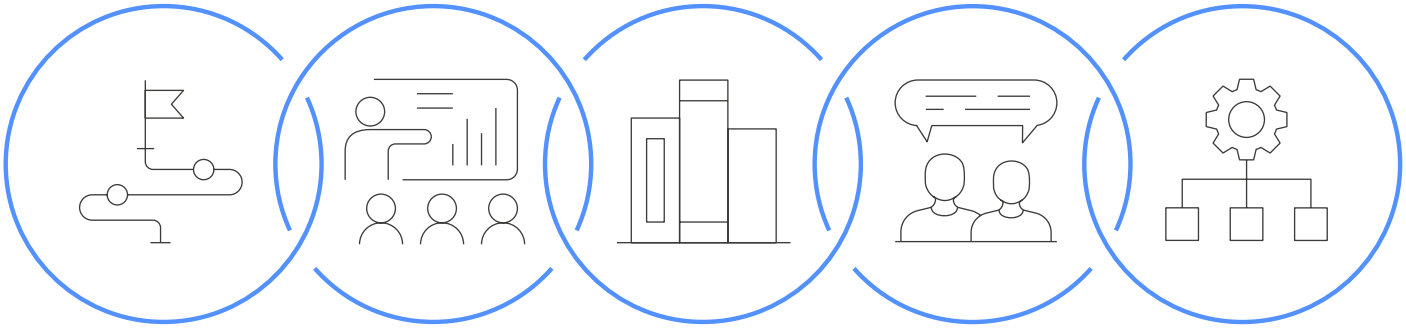
While numerous OT cybersecurity frameworks are available, many of those referenced here are extremely complicated and require a lot of effort to ensure effective implementation, particularly for third-party suppliers and vendors that may struggle to comply due to resource limitations – human or financial. This obligates industrial organizations to ensure that third parties are capable of applying and adhering to these frameworks and standards.

No silver bullet exists for successful implementation of OT cybersecurity frameworks and standards. Most of the time, industry players must apply a wide range of frameworks and standards to cover distinct parts of their infrastructure, such as water pumps and utilities.

A lot of the above-mentioned frameworks are very focused on technical controls. Yet, OT governance, i.e. who is responsible for cybersecurity in OT and how it interlocks with IT, remains a challenge for many organizations.

1 Guiding principles for cyber resilient OT environments

The action group “Securing the OT environment” convening cyber leaders from the electricity, manufacturing and oil and gas industries around the topic of OT cybersecurity, has developed a set of five guiding principles to help industrial organizations address cyber risks and build resilience as the IT/OT convergence continues.



Principle 1

Perform comprehensive risk management of the OT environment

Principle 2

Ensure OT engineers and operators of installations have responsibility for OT cybersecurity

Principle 3

Align with top organizational leadership, strategic planning teams and third parties to make security-by-design a reality

Principle 4

Make cybersecurity standards and best practices contractually enforceable on partners and vendors to build a cybersecure OT environment

Principle 5

Run joint tabletop exercises to ensure preparedness in case of an actual incident

2

Actionable approaches to implementing OT cybersecurity principles

To ensure the successful implementation of the identified OT cybersecurity principles, organizations must undertake a number of actions to translate theory into tangible institutional practice.

Principle 1

Perform comprehensive risk management of the OT environment

To increase overall cybersecurity preparedness and reduce the potential and impact of cyberattacks, industrial organizations must take a comprehensive approach to risk management. This comprises risk assessment – identification of vulnerabilities and gaps that expose an organization to an attack, and of risks that could impede recovery and resilience – as well as mitigation and monitoring strategies. For risk management to be robust and complete, it is important that organizations:

- Identify and classify assets on the basis on their criticality, value and sensitivity to the organization's operations.
- Create an inventory of the "crown jewels" – the highest-value assets in their OT environment which, if compromised, could have a major impact. Once the "crown jewels" have been identified, organizations should identify how they connect to the network, data flows, etc.
- Detect security vulnerabilities and threats across the mapped assets and OT environment; identify the consequences that could result if the vulnerabilities are exploited (e.g. in case of unauthorized access, data theft, equipment damage, injury and loss of life, harm to national security, etc.); and prioritize mitigation accordingly.
- Identify potential threats (including threat events, threat actors, etc.) that could target their OT environment.
- Establish an OT cybersecurity strategy aligned with the overall cybersecurity strategy, outlining the prevention, detection and response capabilities. It should be reviewed, evaluated and updated regularly. Organizations should also consider developing guidelines to ensure effective adoption and implementation of the OT cybersecurity strategy.

Principle 2

Ensure OT engineers and installation operators have responsibility for OT cybersecurity

Research shows that 95% of organizations[20] will place the responsibility for OT cybersecurity under the Chief Information Security Officer (CISO) in the next 12 months. However, considering that cybersecurity is a shared responsibility, the IT team alone cannot have full control of OT cybersecurity; all stakeholders, at all levels of organizational management, need to do their part.

This makes it imperative that roles and responsibilities be clearly defined and properly communicated with IT/OT personnel. That said, OT teams do not necessarily have the awareness or knowhow to properly inspect and secure OT networks. In order to share responsibility for OT cybersecurity, OT personnel across industrial organizations need to understand:

- When, how and why a security breach might occur in the OT environment. Communications on security awareness should be carried out continuously for all OT personnel.
- Who to contact in case of a security breach or suspicious activity, that is, who to get help from and who to collaborate with for support.

Different threat detection technologies used by IT and OT could detect threats in the OT environment. Therefore, cooperation and communication between the IT and OT departments is essential to ensure that all staff have clearly and precisely defined roles and responsibilities for working together on incident response in OT.

- The vulnerabilities and risks (including inherited risks) that each connected device in the OT environment brings.
- The role of the Security Operations Centre (SOC), CISO team, etc. OT personnel should also build a relationship with the SOC and CISO teams to ensure transfer of knowledge on security architecture and policies, including on the prevention, detection, analysis and response to cybersecurity incidents. Among the OT personnel, a "Cyber Champion" should be appointed in each facility who can help with cyber issues during crises.

Principle 3

Align with top organizational leadership, strategic planning teams and third parties to make security-by-design a reality

Most of the existing OT was not designed with cybersecurity in mind. Security-by-design is a process rather than a one-time "bolt-on" effort and as such should go beyond integration of security during the design and development phase of a product/service. To enforce a security-by-design approach in the OT environment, organizations should:

- Raise cybersecurity issues and risks to corporate management to ensure that critical OT systems are safeguarded from potential risks and vulnerabilities from the outset by:
  - Organizing executive briefings to highlight the impact of OT cyber risks on business operations, finances and reputation.
  - Developing and presenting risk assessments to communicate the interplay between OT cybersecurity breaches, operational downtime and compliance penalties.
  - Sharing case studies illustrating real-world examples of cybersecurity incidents in the OT environment and the consequences experienced by organizations that were caught off-guard.
- Encouraging the integration of OT cybersecurity into the overall business strategy to ensure competitive advantage by demonstrating commitment to protecting critical OT infrastructure. It can ultimately help foster overall resilience across industry ecosystems.

Principle 4

Contractually bind and enforce security standards on partners and vendors to build a secure OT environment

Third-party suppliers and vendors differ in the way they approach cybersecurity. Nevertheless, they have to guarantee the security of their product or service and take responsibility for what is delivered. To build a secure OT environment and ensure successful collaboration with and enforcement of security standards by partners and vendors, industrial organizations should:

- Conduct thorough due diligence of both IT and OT cybersecurity posture before collaborating with any third-party vendors and suppliers. The assessment should cover how a cyberattack against a third-party vendor or supplier could impact operations.
- Classify and categorize third parties according to their level and type of risk (compliance, financial, reputation, etc.) before they can access facilities, network and confidential information.
- Incorporate a list of baseline security requirements for third-party vendors and suppliers with access to facilities, network and confidential information within the security framework mentioned in principle 1. These security requirements should be met before formalization of collaboration. Examples of security requirements include:
  - Implementation of security levels (SL) 3 and 4 of IEC 62443.
  - Application of advanced cybersecurity standards for OT software development.
  - Demonstration of proven hands-on expertise in handling cybersecurity events.
- Include OT cybersecurity requirements in contracts. OT cybersecurity requirements should cover areas such as secure remote access, use of removable media devices to transfer files, terms and conditions for data protection and processing of sensitive information shared between the organization and the third party, accident/incident notification and reporting, etc.
- Continuously audit vendor and supplier security performance to ensure they are adhering to previously agreed security controls.
- In case the security controls are not observed, organizations should develop an exit strategy that includes proper oversight over the termination of collaboration with the vendor, return of assets, etc.

Principle 5

Run joint tabletop exercises to ensure preparedness in case of an actual incident

A tabletop exercise cannot always perfectly replicate every aspect of a real-life scenario or incident response situation. To ensure maximum preparedness and amplify its benefits, the tabletop exercise should include key personnel and should have clearly defined and achievable objectives. Organizations should therefore:

- Use security scenarios based on real events, and leverage and adapt existing crisis management procedures to the cyber context.
- Engage the correct stakeholders that go beyond IT and OT personnel. Exercises should include the emergency preparedness group, executive leadership and management, technical staff, third parties, legal counsel as well as psychologists who can evaluate the responses and actions taken by the security incident response team (SIRT).
- Clarify the representation of OT cyber competence in incident response to ensure preparedness when a threat event occurs and explore whether operations can be run in the OT environment without the IT.
- Include OT sites across multiple geographies and consider the legal aspects that may arise.
- Identify weaknesses/gaps in the incident response and include lessons learned in the post-drill analysis reports.
- Produce and continuously update the executives' playbook with lessons learned from such exercises.

3 Monitoring the implementation of OT cybersecurity principles

Implementation of OT cybersecurity principles alone is not enough. Tracking their progress and continuous assessment of impact is key in order to ensure effectiveness of the principles and that organizations are adapting to the new processes. To successfully monitor the implementation of OT cybersecurity principles, organizations should:

- Perform regular audits to monitor compliance with the OT cybersecurity principles, including assessments of critical third parties with access to the OT environment.
- Conduct real-time monitoring to discover, identify and assess devices and vulnerabilities within the OT environment. The “now, next and never” approach can help organizations assess vulnerabilities. Gathered information should be kept in a register and reviewed periodically.
- Develop a strategic roadmap and process for reporting to the corporate board about progress on OT cybersecurity.
- Send data (e.g. IDS data) regularly to the security operations centre (SOC) to ensure timely detection, investigation and response to security incidents.

Additional measures:

- Conduct physical walk-throughs and inspections of OT sites.
- Review and define job and role descriptions to ensure cybersecurity roles and responsibilities for OT personnel.
- Perform periodic benchmarking to assess maturity on OT cybersecurity principles.
- Ensure tabletop exercises are a recurrent activity to monitor progress on incident response.
- Carry out threat hunting in OT and proactively seek indicators of potential compromise.

4 Enabling innovation in OT

Discussions on cybersecurity in OT would not be complete without acknowledging the role of innovation across industries. Research from 2023 shows that 45% of industrial manufacturing organizations have started pilots on generative AI.[21] Strides towards the employment of new technologies are also being made in the automotive and energy sectors where 68% and 64% of organizations, respectively, have started exploring the potential of generative AI.[22]

In addition to AI and machine learning, industry players are also using several emerging technologies including:

- Cloud computing
- Edge computing
- Internet of things (IoT)
- Secure remote-access software
- 5G

While selecting the technology may be simple, implementing it seamlessly in existing operational environments while ensuring minimal disruption and maximum cybersecurity is a complex task that requires careful planning and rigorous risk assessment.

In broad terms, new technologies allow for:

- Automation of decision-making processes.
- Enhanced secure access practices, including for third parties.
- Increased situational awareness fostered by improved visibility of assets, vulnerabilities and threats.
- Improved threat hunting, threat intelligence and incident response.
- Better compliance with regulatory measures.
- Greater access to production data.

However, the deployment and use of new technologies in OT environments also comes at a cybersecurity cost. Often, new devices incorporate cybersecurity vulnerabilities that are not necessarily managed prior to their launch on the market. By introducing additional entry points for cyber threats, these new technologies expand the attack surface. Other cybersecurity challenges can arise from the use of inaccurate or flawed datasets to train algorithms and machine learning models.

To address these cybersecurity challenges, companies must review and adopt proper governance measures considering that existing cybersecurity controls and standards may not be applicable to the use of new technologies in OT.

Finally, the introduction of new technologies needs a skilled talent pool that possesses an understanding of both traditional OT systems and sophisticated new digital solutions.

Other measures that can help organizations address some of the cybersecurity issues arising from the adoption of new technologies in OT include:

- Developing a clear change management programme.
- Introducing network segmentation.
- Implementing layered security controls to mitigate vulnerabilities.
- Having accessible and updated documentation featuring cybersecurity best practices.

The introduction of new security models such as zero trust is becoming increasingly relevant in the context of both old and new cybersecurity threats in OT. Research from 2022 shows that 88% of OT cybersecurity leaders in the US have already taken some steps to adopt zero trust.[23] While the intent to deploy zero trust in OT may exist, successful implementation remains somewhat of a challenge due to a lack of internal knowledge, conflicting direction from leadership and lack of resources.

In certain instances, implementation of zero trust in OT may require organizations to replace legacy technologies. Such an approach can prove expensive and disruptive. However, organizations can also deploy zero trust in such a way that no upgrades to existing technologies are needed.

To allow for effective application of zero trust across OT environments, organizations need to:

- Have good awareness of the overall security model and define zero trust practices in OT environments.
- Secure top management approval and sponsorship.
- Establish a clearly defined zero trust strategy and roadmap.
- Decide on reasonable zones of zero trust deployment as opposed to total zero trust deployment.
- Be careful about vendor selection and question the “silver bullet” of the product offering.

Conclusion

Digitalization is transforming industrial environments in this era of IT/OT convergence. While the new business opportunities are clear, the threat of cyber risk expanding from connected environments and products is growing. Cyber incidents in the industrial ecosystem can have catastrophic economic, safety and environmental consequences.

With the industrial environment representing the bulk of operations in critical infrastructure organizations, ensuring a secure and cyber resilient OT environment is of paramount importance. Cyber leaders must adapt to the transforming industry as environments become more interconnected, digital and automated.

To improve OT environment security, the World Economic Forum in collaboration with partners from the electricity, manufacturing, and oil and gas industries, has developed a list of guiding principles. The adoption of these principles in the OT environment is imperative to cope with cybersecurity risks and enable the longer-term benefits of the digitalization of the OT environment.

This should not be a plug-and-play exercise. It must be complemented with work in areas already embedded into the industry culture such as safety, and with significant investment in skills and in the workforce. Given the complex ecosystem, close collaboration and commitment from all public and private stakeholders across the industry is essential to ensure cyber resilience in the OT environment.

Contributors

World Economic Forum

Filipe Beato
Lead, Centre for Cybersecurity

Natasa Perucica
Research and Analysis Specialist,
Centre for Cybersecurity

Community

The World Economic Forum would like to extend its sincere thanks to the cyber leaders from the electricity, manufacturing and oil and gas industries who contributed their valuable insights and perspectives to this white paper. The following individuals led in-depth discussions as part of the "Securing the OT Environment" action group to address some of the most pressing questions around OT cybersecurity.

Salem Al-Elwi
Saudi Aramco, Saudi Arabia

Norah Alkhathlan
Saudi Aramco, Saudi Arabia

Qusai Alrabei
Schneider Electric, France

Edgardo Alfonso Arrieta Arteta
Ecopetrol, Colombia

Hossain Alshedoki
KPMG, Saudi Arabia

Nik Bartholomew
Occidental Petroleum Corporation, US

Jalal Bouhdada
DNV, Norway

Stefan Braun
Henkel, Germany

Carlos Buenano
Armis, US

Dawn Cappelli
Dragos, US

Piotr Ciepiela
EY, Poland

Giovanni Cock
Ecopetrol, Colombia

David Corral Morgadez
Repsol, Spain

Dharminder Debisarun
Palo Alto Networks, US

Stefan Deutscher
Boston Consulting Group, Germany

Younes Dragoni
Global Shaper, Lugano Hub, Switzerland

Janne Merete Hagen
Norwegian Water Resources and Energy Directorate, Norway

Eram Hasan
Engro, Pakistan

Ronald Heil
KPMG, Netherlands

Gabriel Hengel
Cybersecurity and Infrastructure Security Agency, US

Octavio Herrera
Occidental Petroleum Corporation, US

Roger Hill
Kudelski Group, US

David Andres Hurtado
Naturgy, Spain

Lars Idland
Equinor, Norway

Rayan Kashghari
Saudi Aramco, Saudi Arabia

Sigmund Kristiansen
Aker BP, Norway

Srinidhi Mallur
Saudi Aramco, Saudi Arabia

Suwat Meemook
Bangchak Corporation, Thailand

Giorgio Medina
Eni, Italy

Rishi Muchalla
Check Point Software Technologies, US

Michael Ng
Petronas, Malaysia

Sebastian Nikelski
Volkswagen, Germany

Goran Novkovic
Neom, Saudi Arabia

Ranjan Pal
Massachusetts Institute of Technology, US

Barbara Pereira
Galp, Portugal

Christina-Dorothea Schlichting
Volkswagen, Germany

Arno Sevinga
Royal Vopak, Netherlands

Nicholas Shah
Procter & Gamble, US

Joanna Swiatkowska
European Cyber Security Organisation, Belgium

Annika Wägenbauer
Institute for Security and Safety, Germany

Keith Walsh
Claroty, US

Swantje Westpfahl
Institute for Security and Safety, Germany

Olivera Zatezalo
Suncor Energy, Canada

Production

Bianca Gay-Fulconis
Designer, 1-Pact Edition

Madhur Singh
Editor

Endnotes

1. Microsoft, "Secure your OT and IoT devices with Microsoft Defender for IoT and QuZara CyberTorch." *Microsoft Security Blog*, 3 March 2022, https://www.microsoft.com/en-us/security/blog/2022/03/03/secure-your-ot-and-iot-devices-with-microsoft-defender-for-iot-and-quzara-cybertorch/.
2. Ribeiro, Anna, "CISA, DOE warn that hackers are gaining access to various internet-connected UPS devices." *Industrial Cyber*, 30 March 2022, https://industrialcyber.co/threats-attacks/cisa-doe-warn-that-hackers-are-gaining-access-to-various-internet-connected-ups-devices/.
3. Microsoft, "Secure your OT and IoT devices with Microsoft Defender for IoT and QuZara CyberTorch." *Microsoft Security Blog*, 3 March 2022, https://www.microsoft.com/en-us/security/blog/2022/03/03/secure-your-ot-and-iot-devices-with-microsoft-defender-for-iot-and-quzara-cybertorch/.
4. Wood, Laura, "Global Industrial IoT (IIoT) Market Report 2023: Growing Demand for Connected Supply Chains and Operational Efficacy Flexibility Bolsters Sector." *GlobeNewswire*, 27 March 2023, https://www.globenewswire.com/en/news-release/2023/03/27/2634574/28124/en/Global-Industrial-IoT-IIoT-Market-Report-2023-Growing-Demand-for-Connected-Supply-Chains-and-Operational-Efficacy-Flexibility-Bolsters-Sector.html.
5. Microsoft, "Microsoft Releases Its Third Edition of Cyber Signals: Analyzing the Rise in Risks to Critical Infrastructure." *Microsoft News Center*, 15 December 2022, https://news.microsoft.com/apac/2022/12/15/microsoft-releases-its-third-edition-of-cyber-signals-analyzing-the-rise-in-risks-to-critical-infrastructure/.
6. "Everything You Need to Know to Defend Against ICS/OT Cyber Threats in 2023." *Dragos*, 2022, https://www.dragos.com/resource/everything-you-need-to-know-to-defend-against-ics-ot-cyber-threats-in-2023/.
7. Ayman, Alissa; Bacelar, Duarte; Braga, Duarte; Espirito Santo, Hugo; Boehm, Jim; Candina, Joana; Vieira, Benjamim and Richter, Wolf, "How to Enhance the Cybersecurity of Operational Technology Environments." *McKinsey & Company*, 23 March 2023, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/how-to-enhance-the-cybersecurity-of-operational-technology-environments.
8. Ibid.
9. Alvarez, Michelle; Carruthers, Stephanie; Chung, Joshua; Craig, Scott; Dwayer, John; Eitan, Ari; Emerson, Richard, et al., "X-Force Threat Intelligence Index 2022." *IBM*, 2022, https://www.ibm.com/downloads/cas/ADLMYLAZ.
10. "The State of Industrial Cybersecurity." *Trend Micro*, 2022, https://resources.trendmicro.com/rs/945-CXD-062/images/TR00_ICS_OT_Security_Survey_Report_220525US_web.pdf?mkt_tok=OTQ1LUNYRC0wNjlAAAGGekNqBDAktPQrDV926OlhJmPQxl2MkpwSxgbzWTff_DQ5VrXKkTemgAFHrdNq9afwHbrYOrq6gsk8AY3w9mV1O6l882ppcgOseLezWlvC2wotTPV_OVNC.
11. Gartner, "Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans." 21 July 2021, https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we.
12. SCADAfence, "SCADAfence Releases Results of Global Survey of IT and OT Cyber Security Professionals." *CISION PR Newswire*, 14 July 2022, https://www.prnewswire.com/news-releases/scadafence-releases-results-of-global-survey-of-it-and-ot-cyber-security-professionals-301586516.html.
13. "Everything You Need to Know to Defend Against ICS/OT Cyber Threats in 2023." *Dragos*, 2022, https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Infographic-2022.pdf?hsLang=en.
14. Guha, Debjyoti, "Operational Technology Security Is Compromised by Third-party Risk." Skybox Security, 31 January 2022, https://www.skyboxsecurity.com/blog/operational-technology-security-compromised-third-party-risk/#:~:text=Research%20discovers%20that%20third%2Dparty,of%20OT%20security%20decision%2-0makers.&text=A%20research%20study%20by%20Skybox,top%20three%20highest%20security%20risks.
15. "Understanding IEC 62443." *IEC*, 24 February 2021, https://www.iec.ch/blog/understanding-iec-62443.
16. Stouffer, Keith; Suzanne, Lightman; Victoria, Pillitteri; Marshal, Abrams and Adam, Hahn, "Guide to Industrial Control Systems (ICS) Security." *National Institute of Standards and Technology*, 6 May 2015, https://csrc.nist.gov/pubs/sp/800/82/r2/final.
17. P. Theron and A. Lazari, "The IACS Cybersecurity Certification Framework (ICCF)." *Joint Research Centre (JRC)*, April 2018, https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC111611_The_IACS_Cybersecurity_Certification_Framework.pdf.
18. "NIST Cybersecurity Framework." *National Institute of Standards and Technology*, 20 September 2022, https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework.
19. "Cybersecurity Capability Maturity Model (C2M2)." *Carnegie Mellon University*, June 2022, https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf.
20. "Fortinet Global OT and Cybersecurity Survey: 75 percent of organizations experienced at least one unauthorized access to their OT environments in the last year." *Fortinet*, 6 June 2023, https://www.fortinet.com/de/corporate/about-us/newsroom/press-releases/2023/fortinet-global-report-finds-75-percent-ot-organizations-experienced-intrusion-last-year.

21. "Harnessing the Value of Generative AI." *Capgemini Research Institute*, July 2023, https://prod.ucwe.capgemini.com/wp-content/uploads/2023/07/Final-Web-Version-Report-Harnessing-the-Value-of-Gen-AI.1.pdf.

22. Ibid.

23. "Securing Critical Infrastructure: The Journey to Zero Trust." *Xage*, July 2022, https://xage.com/wp-content/uploads/2022/07/Xage-ZeroTrustReport-July-2022.pdf.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org