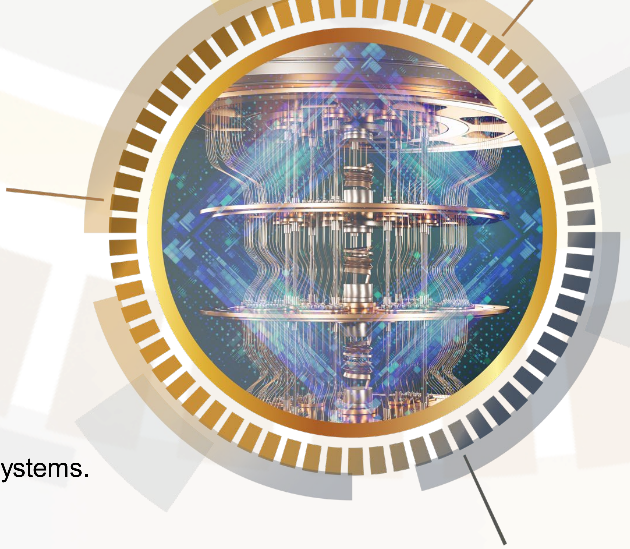
Deloitte.



5x5 series: Insights and Actions

OT Security in the Energy and Chemicals Sector

Cybersecurity is not just an IT issue. These days, Energy and Chemicals companies are increasingly becoming targets of cyberattacks that target their Operational Technology (OT) systems.

5 things you should know

1 **Protecting mission-critical operations from cyber criminals and nation-states is urgent.** Energy and Chemicals organizations realize they could be targets and should deploy cybersecurity and risk management systems addressing the evolving threat landscape. Also, **increased regulatory oversight** in the wake of high-profile cyberattacks should be addressed. Effectively responding to and recovering from a breach is imperative to avoid impacts to the broader economy.

2 Many Energy and Chemicals organizations have **increasingly complex ecosystems** and **supply chain integrity** is a significant concern. Organizations are looking to improve **supply chain resilience** and reliability in order to **limit third-party risk and potential disruptions**.

3 Companies face the challenge of **securing an ever-expanding attack surface** because of the convergence of IT and OT technologies such as Internet of Things (IoT), Industrial Internet of Things (IIoT), and Industrial Control Systems (ICS) that control their operations.

4 Many Energy and Chemicals organizations are embracing cloud computing, artificial intelligence (AI), and machine learning (ML) to **pave the way for greater operational efficiency and infrastructure modernization**.

5 Energy and Chemicals companies are working to **establish commitments and strategies to meet environmental, social, and governance (ESG) goals, as well as alternative and clean energy goals**, which can drive the need to evolve risk management and risk insight capabilities.

5 actions you can take

1 **Take a fresh look at your OT cybersecurity programs,** starting with a high-level risk assessment to help the organization understand their operational cybersecurity risks, risk tolerance, and target profile(s). Establish roadmaps and governance materials to enable the organization to continuously improve (e.g., policies, standards, procedures, job aids, and employee/supplier training).

2 Conduct a **consequence-based risk assessment for OT**. Deloitte professionals have pioneered the development of the Cyber Process Hazards Analysis (PHA) methodology of performing industrial automation and control systems (IACS) cybersecurity risk assessments that align to international standards. The Cyber PHA methodology evaluates multiple combinations of threats, vulnerabilities, and consequences to provide leadership with a broad view and ranking of the operational risks and potential regulatory concerns (e.g., health, safety, environment, business interruption, equipment damage, off-spec product) associated with a cyber incident.

3 Improve management of the ever-growing number of vulnerabilities in your OT systems with Deloitte's risk-based approach to **rationalize cybersecurity vulnerabilities**. The methodology extends the established framework of Common Vulnerability Scoring System (CVSS) to consider safety, environmental, and business consequences, helping clients prioritize what vulnerabilities to treat, terminate, transfer, or tolerate within their OT systems

4 **Conduct OT security acceptance testing on new or recently updated OT systems** to determine if the implementation addresses security requirements and follows industry standards and leading practices. Deloitte offers cybersecurity acceptance testing before the system is shipped. Acceptance testing incorporates numerous test steps to analyze items such as passwords, user accounts, port security, device hardening, network management, switch/firewall security, controller write protection, and network segmentation.

5 **Establish product security collateral and third-party security assurances and certifications** to share with customers during the purchasing process to demonstrate the programmatic capabilities that are in place, the security safeguards of the product, that regulatory requirements are met, and proof from third parties that the product is safe and secure.

Learn more from these additional resources

Cyber-physical security (CPS) insights for Internet of Things (IoT) and Operational Technology (OT) products, systems, and ecosystems (deloitte.com)

Connect with us

John Cusimano
Managing Director
Deloitte & Touche LLP
jcusimano@deloitte.com

Kieran Norton
Principal, Emerging Technology Leader
Deloitte & Touche LLP
kinorton@deloitte.com

Mike Kosonog
Advisory Partner
Deloitte & Touche LLP
mkosonog@deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com /us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.