Deloitte.

Powering the future of the energy industry series: Insights and actions

Protecting factories of the future

While it may be tempting for organizations to leverage IT cybersecurity controls out of the box to protect their manufacturing environments, it is not normally advisable (or, at times, even possible) to do this. Cybersecurity for manufacturing environments requires a tailored, programmatic approach and focused attention from multiple stakeholder groups across the organization. This is increasingly important as more connected technologies are introduced to these environments to enable smart manufacturing programs.

***5** things you should know*		***5** actions you can take*
Secure network architecture and segmentation should be top of mind as organizations add connectivity to aging manufacturing environments to enable smart factory programs.	1	IT and operational technology (OT) networks that enable manufacturing should be segmented from one another **to help prevent attackers from moving freely throughout a manufacturing environment**. Deploying a pair of firewalls between IT and OT networks helps to achieve this segmentation and allows **a "de-militarized zone" (DMZ) to be created, which is a vital element in enabling the secure data flow required to protect factories of the future.**
Cybersecurity monitoring and asset visibility within OT networks is becoming a fundamental control for manufacturing organizations looking to more efficiently identify indicators of compromise.	2	OT network monitoring capabilities should **passively collect information**, and active scanning should be enabled only when these networks (and their components) are well understood. OT network monitoring and asset visibility capabilities also enable organizations to **identify vulnerabilities and risks at the device level** and better prioritize their mitigation. **Monitoring should also be centralized** through a Security Operations Center (SOC) that can act as a quarterback to guide the sites during the response processes.
OT-specific response and recovery planning should be a focus of a cybersecurity program. This should include periodic exercises to test response and recovery plans.	3	Personnel at the sites and centralized personnel, such as those in the SOC, **should know who to call and when**. Plans should be **documented and tested** at set intervals to confirm that personnel understand their roles and responsibilities. **Backups** of critical systems should also be available to enable recovery in the event that those systems need to be restored.
Identity management with a focus on privileged access should be a cornerstone of OT cybersecurity programs.	4	Organizations should look closely at how access to systems is being managed across their OT environments. Organizations often assign privileges to employees and vendors that go beyond what is required to perform their business responsibilities. **Identity management solutions and corresponding access review processes** should be extended to OT, when possible.
Operating models, as well as regular training and communication, enable an effective OT cybersecurity program.	5	**Clearly defining roles and responsibilities (and mapping when coordination is required)** is a vital element to making OT cybersecurity programs effective, particularly when enabling smart factory capabilities. Additionally, **training and tailored communications** help stakeholders understand their responsibilities from the corner office to the shop floor.

Explore our *cyber-physical systems (CPS) security* services or contact us to learn more:

Connect with us:

Brian Clark
Partner
Deloitte & Touche LLP
bclark@deloitte.com
+1 816 802 7751

Jason Hunt
Principal
Deloitte & Touche LLP
jashunt@deloitte.com
+1 901 322 6804

Adam Mack
Senior Manager
Deloitte & Touche LLP
admack@deloitte.com
+1 202 220 2608