Guidepost

EFFECTIVELY INTEGRATING PHYSICAL SECURITY TECHNOLOGY INTO THE OPERATIONAL TECHNOLOGY (OT) DOMAIN

Effectively Integrating Physical Security Technology into the OT Domain CSJ Fall 2020

The Operational Technology (OT) domain has historically been an area of sensitivity primarily within the industrial (manufacturing, petrochemical and utility) markets. Recent compromises of OT have expanded the exposure to loss from this domain into more core corporate markets including pharmaceutical, finance and technology spaces. In order to effectively mitigate threats to this domain, a holistic countermeasure implementation program must be put in place and be managed as a core competency within the overall cybersecurity posture of an organization. Physical security controls must be a priority within this posture to effectively control access to the on-site assets that manage OT.

The article, Effectively Integrating Physical Security Technology into the Operational Technology (OT) Domain, written by Matthew Wharton, was recently published in Cyber Security – A Peer Reviewed Journal.

This compelling article introduces two key initiatives. The first is to apply physical security controls to protect OT, which may require an expansion of the locations at a site where these controls are deployed. The second is to treat physical security assets as OT so they fall under the same level of network segmentation, threat management, version control and access management as core OT assets.

MATTHEW WHARTON SR.

President, Strategic Accounts

Matthew Wharton serves as president for strategic accounts. Mr. Wharton is a career security professional with more than 35 years of experience leading security consulting and integration firms. He designs solutions from “The Owner’s Perspective” with improved recommendations that meet regulatory and fiscal requirements and transform internal functions from cost centers to sources for corporate investment that deliver increased integrity to the enterprise and enhance shareholder value.