Cybersecurity Transformation for Industry 4.0: A Case Study of an Indian Paper & Pulp Company

PAPER & PULP

BACKGROUND

In pursuit of Industry 4.0 transformation, a prominent Indian conglomerate embarked on a journey to integrate cutting-edge technology into its various business units. The conglomerate selected its Paper & Pulp Strategic Business Unit (SBU) as the pioneering entity to demonstrate rapid advancements. To facilitate this transformation, the conglomerate initiated the deployment of an Inter Plant Historian system across multiple factories. This move necessitated a robust integration between Operational Technology (OT) systems on the shop floor and the corporate network. However, this convergence introduced new vulnerabilities, significantly expanding the risk surface area of the core OT network. Any cyberattack could potentially result in severe financial, environmental, and human losses.

CHALLENGES

The company encountered several challenges as it ventured into the realm of digital transformation and cybersecurity:

Where to Begin: Like many brownfield companies, the company grappled with where to start its cybersecurity journey amid the complex landscape of Industry 4.0.

Scope of Work: Defining the right scope of work for cybersecurity initiatives was a critical concern.

Lack of Security Controls: The company sought to integrate automation systems with Plant Historian but had not deployed any security controls such as firewalls, deep packet inspection, patch management, or updated antivirus software in the OT network.

Reluctance to Deploy Security Inspections: OEMs and shop floor teams were hesitant to implement security inspections on data flowing through the OT network.

Point Product vs. Comprehensive Solution: The company debated whether to purchase point products incrementally or wait for a comprehensive solution.

Inability to Patch Critical Systems: Due to OEM constraints, essential Microsoft systems (e.g., HMI, OPC, Engineering Workstations) are running older version of OS (e.g. Windows 7, etc.) and couldn't be patched.

Lack of In-House Skills: The company lacked the skills to manage cybersecurity on a day-to-day basis, and the remote site locations were critical concerns

SOLUTIONS

To address these challenges, the company partnered with Quality OT Solutions (QOS), leveraging their experience as a trusted cybersecurity partner from previous IT security projects. QOS adopted a strategic approach:

Think Big, Act Swift, Start Small: QOS recommended a phased approach, commencing with an 5-prong OT Security Assessment at one of the paper mills. This assessment helped determine the necessary components for an effective IT-OT security solution, including the

required number of sensors along with additional passive and active network components.

Demonstrate Quick Wins: Starting small allowed the company to achieve early successes, gaining the confidence of shop floor and engineering teams, which accelerated the rollout of IT-OT security.

Expansion: The project that began in 2018 with an single plant OT security assessment was expanded across all plants in early 2019 with a culmination into the deployment of IEC62443 proposed IT-OT Security Architecture with security enforcers and SOPs.

Handing Ops Skills Concerns: The consoles of security enforcers were extended to a QOS shared SOC in Bengaluru, providing critical daily operational support. By Q1 2023, the project evolved into 24x7 Network Situational Awareness with Real-Time Security Event and Alert management from the shared SOC. QOS's Managed Security Services played a pivotal role in the project's success.

Virtual Patch Management: The implementation of Virtual Patch Management on IT-OT security enforcers proved highly valuable, offering compensatory controls for systems, unable to be patched.

BENEFITS

The company reaped several benefits from this approach to cybersecurity in its OT networks during its Industry 4.0 journey:

Risk Mitigation through Phased Approach: Adopting a phased approach mitigated the risk of vendor lock-in when dealing with limited scope clarity.

Quick Start with OT Security Assessments: Initiating the project with OT security assessments provided a rapid start, while Managed Security Services ensured confidence among stakeholders for whom in-house cybersecurity operations seemed unattainable.

Virtual Patch Management: Virtual patching addressed constraints related to older versions of critical OT systems, ensuring a higher level of security.

Becoming a Reference Site: The Paper & Pulp division became the reference site for IT-OT security within the conglomerate's other manufacturing divisions, underlining the success of the project.

This case study highlights how a well-thought-out cybersecurity strategy, when aligned with digital transformation goals, can not only secure critical infrastructure but also serve as a reference point for similar initiatives across an organization.

