

CASE STUDY:

Cybersecurity Assessment for a Global Biopharmaceutical Company

OVERVIEW: One of the world's leading biopharmaceutical companies, initiated an Enterprise Cyber Resiliency initiative to protect and isolate its manufacturing sites from cyber-attack and have the ability to sustain operations in light of a corporate-level attack. A key facet of the customer's cyber resiliency approach was segmentation to establish limited, controlled sharing across operations and infrastructure.

Due to Astrix Technology Group's (Astrix) expertise with enterprise-wide laboratory information systems, experience working with other biotech and pharmaceutical companies, and track record of eliminating risk and delivering on similar projects for other life science organizations, the customer chose Astrix to conduct an assessment of its laboratory systems across five global manufacturing sites.



BUSINESS CHALLENGE: The customer had cybersecurity concerns in two main areas: quality control (QC) laboratory instrumentation and their associated data acquisition systems. Specifically, the customer sought input from Astrix in the following areas:

- **Assess and advise on the upgrade and hardening of three key laboratory systems during the course of cyber-resiliency segmentation efforts. The three systems include:**
 - ▶ Chromatography Data System (CDS)
 - ▶ Laboratory Method Execution System (LMES)
 - ▶ Consumables Inventory Management System (CIMS)
- **Assess and advise on the migration approach and deployment plan for instrumentation associated with CDS, LMES and CIMS for each site.**

"A key facet of the customer's cyber resiliency approach was segmentation to establish limited, controlled sharing across operations and infrastructure."

SERVICES PROVIDED: In order to effectively accomplish the project objectives, the Astrix Team engaged with the customer on 5 critical tasks, each of which is outlined below:

TASK #1: Project Initiation and Kickoff Meeting

Initially, the Astrix Team reviewed information provided by the customer offsite to become familiar with the current state of laboratory operations, as well as review the plans for laboratory system segmentation and instrument migration. This was followed by a Kickoff Meeting that served to introduce the Astrix Team and the customer's core project team members, review and confirm the project scope, and finalize the project approach with input from the customer to establish a shared project vision and focus.

TASK #2: QC Lab Applications On-site Assessment

The Astrix Team went onsite to one of the manufacturing sites to review the customer's plans for the QC lab application hardening effort. The proposed changes included technical upgrades for the three key laboratory systems:

1. LMES

- ▶ Technical upgrade of the Application Server's Windows Operating System
- ▶ Application upgrade to LES 2019
- ▶ Technical upgrade of Citrix Server
- ▶ Technical upgrade of Oracle database server
- ▶ Technical upgrade of Accelrys Enterprise Platform's Windows Operating Server
- ▶ Application upgrade to Pipeline Pilot 2018
- ▶ Technical upgrade of LMES Configuration Manager server's Windows Operating System

2. CIMS

- ▶ Technical upgrade of Application Server's Windows Operating System
- ▶ Application Upgrade of CIMS application server to LIMS 2019
- ▶ Technical upgrade of Oracle database server

3. CDS

- ▶ Technical upgrade of the Application Server's Windows Operating System
- ▶ Application upgrade to Empower 3 SR3 (including application server, Citrix server, and LAC/E boxes)
- ▶ Technical upgrade of the Citrix Server
- ▶ Technical upgrade of the Oracle database server (including operating system)
- ▶ Technical upgrade of the LAC/E boxes' Windows Operating System



The Astrix Team reviewed plans for these upgrades in detail leveraging its deep domain knowledge while meeting with key stakeholders and gathering additional documentation.

TASK #3: QC Lab Applications Assessment Report

Using the knowledge gained during the site visit about the customer's QC lab application segmentation approach, the Astrix Team produced an assessment report that included:

- ▶ Key findings and observations from site visit
- ▶ Evaluation of architecture and proposal of alternate candidate architectures
- ▶ Analysis of performance considerations, risks, and opportunities for each system in scope: LMES, CIMS, CDS
- ▶ Suggested order and/or prioritization of proposed upgrades
- ▶ Evaluation of project timeline and compression options
- ▶ Resource assessment including number of resources for each phase and experience evaluation
- ▶ Overall risk assessment including the potential for organizational disruption from the project
- ▶ Recommendations for project success

TASK #4: OCR Instrument Migration On-site Assessment

The Astrix Team performed an onsite assessment at one of the manufacturing sites in order to evaluate all factors which could accelerate the transition of instruments at each site to secure OCR infrastructure, while also reducing complications in the process. Items considered during this migration assessment included:

- ▶ Opportunities to standardize migration process across laboratory sections, sites, and instrument types
- ▶ Confirmation of existing instrument inventory list
- ▶ Evaluation of facilities for considerations that may affect migration plans due to access restrictions, geographic diversity, etc.
- ▶ Evaluation of OCR infrastructure as it relates to instrument and related QC application interconnectivity
- ▶ Exceptions and special considerations that complicate or violate the standard strategy
- ▶ Site resource capacity

TASK #5: Instrument Migration Assessment Report

Leveraging information gained during the OCR instrument migration assessment, the Astrix Team produced a report which included:

- ▶ Key findings and observations from site visits, including key risk factors and potential complications
- ▶ Recommended process by instrument type for migration or suggested modifications to existing migration plans
- ▶ Suggested order and/or prioritization of migrations across sites and instrument types
- ▶ Evaluation of project timeline
- ▶ Options for compressing project timeline
- ▶ Assessment of resources required to perform system upgrades, testing, validation and user training
- ▶ Overall risk assessment including the potential for organizational disruption from the project
- ▶ Opportunities to scale resources in a cost-aware manner to ensure team expansion coincides with readiness
- ▶ Additional recommendations for project success

RESULTS DELIVERED:

The Astrix team provided a detailed assessment of the strategic approach necessary to achieve cyber resiliency of the informatics platforms throughout all of the global sites by establishing limited controlled sharing across their operations and infrastructure, thereby minimizing or eliminating risk from potential cyber-attack. The risk assessment provided recommendations surrounding hardening of the CDS, LMES and CIMS systems and the technical upgrades required to support cyber resiliency measures.

As a longer-term effort, a migration assessment was conducted in preparation for the accelerated transition of the site wide instrumentation to the new secure OCR infrastructure to achieve minimal disruption to the ongoing operations of the organization. With over 25 years of experience and expertise with enterprise-wide laboratory informatics systems, the Astrix team was able to provide an industry proven strategic approach to mitigate risk and achieve cyber resiliency across a multi-site global biopharmaceutical company.

ABOUT US:

Astrix Technology Group Astrix Technology Group has over 25 years’ experience helping scientific organizations architect, select, implement, integrate and validate laboratory informatics technologies. Our experienced professionals have the skills necessary to help your laboratory turn data into knowledge, increase workflow efficiency, improve quality and facilitate regulatory compliance.
Visit astrixinc.com for more information.



astrix
TECHNOLOGY GROUP
CORPORATE HEADQUARTERS
125 Half Mile Rd, Suite 200
Red Bank, NJ 0770
732-661-0400