LRS IT SOLUTIONS

CASE STUDY

LRS performs
Cyber Risk Analysis

Manufacturer looked to improve network security posture by testing for vulnerabilities

THE COMPANY

Founded in 1945, MEC (Mayville Engineering Company) is a manufacturer that provides a broad range of prototyping, metal fabrication, tube bending, machining, welding, coating, and value-added assembly services to a variety of markets including commercial vehicle, power sports and recreational vehicles, agriculture, construction and forestry, military, mining, automotive, and power generation companies.

MEC maintains an extensive manufacturing infrastructure in 20 facilities across seven states. An employee-owned company, MEC excels at turnkey manufacturing and works closely with customers to design products and implement solutions so that the manufacturing process features maximum consistency at the lowest total cost.

The company has a small team of IT and Security employees who are responsible for the full spectrum of IT obligations.

THE NEED: Security services partner

MEC was looking for ways to advance its cybersecurity preparedness and proactively identify vulnerabilities with potential of exploitation. MEC's IT and Security staff wears many hats and is responsible for a broad range of operational and strategic service delivery responsibilities for the business.

Realizing that today's cybersecurity threats come in many forms and implementing defensive controls can be extremely difficult, MEC recognized the need to partner with a security services firm. The firm that MEC had partnered with previously had done an adequate job, but the company saw the need for an expertise and hands-on approach that they wanted.

MEC reached out to LRS.

THE SOLUTION: LRS Cyber Risk Analysis.

LRS performed its Cyber Risk Analysis (CRA) with a goal of reducing bad actors' ability to steal data if the environment was compromised. This was done by evaluating Active Directory and firewalls for misconfiguration and security weaknesses. Additionally, all network-connected devices were scanned for known security vulnerabilities.

LRS also performed network pene¬tration testing services that included an internal and external vulnerabil¬ity assessments, wireless penetra¬tion testing, email phishing campaigns, and social engineering tests at various MEC locations. The scope of the testing was established by planning meet¬ings and input from MEC to decide what targets to include, the level of brute force attempts to be executed, and other forms of testing that could be executed without compromising business operations.

THE RESULT: Corrective Action Plan for mitigating weaknesses.

The LRS cybersecurity testing team presented MEC with a Corrective Action Plan (CAP) with prescriptive measures to remediate or mitigate identified vulnerabilities. MEC also received a comprehensive analysis and risk scoring profile containing quantifiable metrics that could be used to establish ongoing Key Performance Indicator and Key Risk Indicator targets.

MEC's team appreciated the level of focus and creative effort that went into creating a set of security assessments that aligned with their security strategy and recognized that the delivered results were useful in their quest for improving the security posture. They appreciated the regular updates and interaction with LRS on the status of the testing

"The detailed manner in which the LRS Team was able to assess our information systems allowed to us better understand our cyber risks."

— Corporate Manager, IT Risk & Compliance

milestones and the fact that LRS offered enough flexibility to accommodate a change in scope in the midst of the engagement.

As MEC's Corporate Manager for It Risk & Compliance said, "The detailed manner in which the LRS Team was able to assess our information systems allowed to us better understand our cyber risks."

MEC found LRS security services to be of higher value, lower cost, and overall superior to what they were receiving from their previous provider. Their management team has indicated that they plan to continue the LRS services on a regular basis in the future.

ACCOMPLISHED CYBERSECURITY GOALS

- Identified weaknesses in MEC's network defenses
- Created a plan for remediation and or mitigating vulnerabilities

SOLUTIONS

- Cyber Risk Analysis
- Network Penetration Test

LRS IT SOLUTIONS

Learn more, visit LRSitsolutions.com or call 217.793.3800