



## Case Study 5: AI System Breach in Combination Product Supply Chain

A combination product manufacturer implemented an AI-driven supply chain platform to streamline operations and integrate real-time supplier data. However, shortly after deployment, a cybersecurity breach compromised proprietary formulations and sensitive patient data.

This breach led to internal chaos, potential regulatory violations, and serious reputational damage. The company had to act fast to contain the incident.

The manufacturer's internal IT team took the lead in resolving the breach. Compliance Insight supported their response by reviewing quality and validation documentation and advising on appropriate corrective and preventive action (CAPA). We ensured that the corrections were effective and that the regulatory file reflected a clear and timely response to the incident.

While remediation took time, these actions restored system integrity and preserved their regulatory standing.

**Key Takeaway:** AI-driven operations require layered cybersecurity protections. Compliance Insight can support quality system readiness and documentation during crisis response.