Cybersecurity Incident Analysis: Chemical Sector Case Study
Team: James & Lubna

Companies Analyzed:

- BASF: Chemical producer specializing in solvents, resins, glues, and industrial gases.
- Hexion: Producer of adhesives and thermoset resins.
- Momentive: Manufacturer of quartz/silicone products and various plastics.

Incident Overview:

- On March 12, two companies—Hexion and Momentive (both subsidiaries of the same parent organization)—were targeted in a ransomware attack by the LockerGoga threat group. The attack resulted in a complete shutdown of IT systems and critical data, with reported costs reaching approximately $33 million USD.

Key Details & Outcomes:

- System Disruption:
  - IT systems were completely shut down, halting digital operations.
  - Despite the IT outage, manufacturing continued due to effective network segmentation between IT and production systems.
- Operational Response:
  - Rather than paying the ransom, the companies restored systems using backups, underlining the importance of robust data recovery protocols.
  - The incident led to a global IT outage, prompting the organization to deploy hundreds of new computers and issue new email accounts for employees.
- Risk & Impact Analysis:
  - Network Segmentation: The separation between manufacturing and IT networks minimized production downtime.
  - Backup Strategy: Reliance on backups prevented financial losses associated with ransom payments.
  - Critical Infrastructure: By targeting a key segment of the chemical sector, the attack underscored vulnerabilities that can have wide-ranging impacts on everyday products and processes.

Strategic Insights:

- This case study highlights the necessity of integrating proactive security measures such as network segmentation, regular system backups, and rapid incident response protocols. The decision not to pay the ransom, while resource-intensive, helped safeguard long-term operational integrity and served as a model for handling similar incidents in critical infrastructure sectors.

Reference:

- SecurityWeek Article