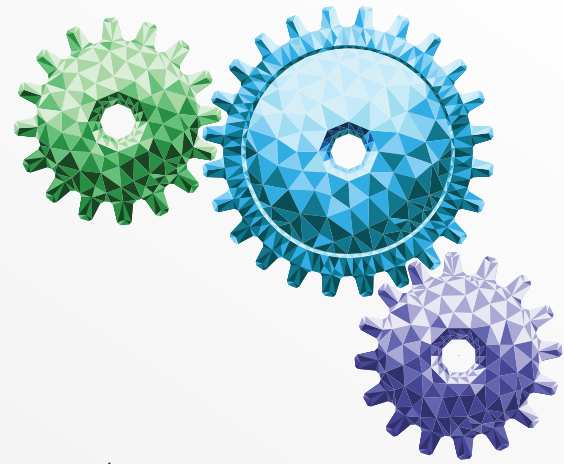# MANUFACTURING

— INCIDENT – RANSOMWARE

The client, a global manufacturer, experienced a sophisticated ransomware attack that crippled their systems. Many of the client's computers and servers were affected and spread throughout multiple systems, rendering their business inoperable.

— AXIS RESPONSE

Immediately after the client alerted AXIS to the incident, a panel of cyber experts was assembled which included:

- Privacy counsel, to offer guidance on the firm's regulatory obligations

- Forensic investigators, to minimize operational disruption and recover encrypted systems quickly

The AXIS Incident Response Manager then convened an initial planning call with the client to begin the planning and get the response activity underway.

— OUTCOME

Fortunately, the forensic investigators were able to recover some systems while analysing the ransomware, allowing the business to function on a limited basis. Due to the ransomware being a common variant, the investigators were able to reverse engineer it and identify the necessary decryption keys. This resulted in a full recovery of the client's systems with only minor disruption.

KEY CYBER COVERAGES TO CONSIDER

- Incident response costs
- Ransomware and extortion services
- Business interruption

PREPARE

- Prepare an Incident Response Plan and practice it regularly
- Keep software and applications patched and updated
- Provide cyber security and awareness training to all staff
- Apply multi-factor authentication (e.g. one-time token)
- Take steps to protect back-ups from ransomware
- Segment networks to hinder the spread of malicious software

AXIS | CYBER INSURANCE

axiscapital.com

ACCS1 1220