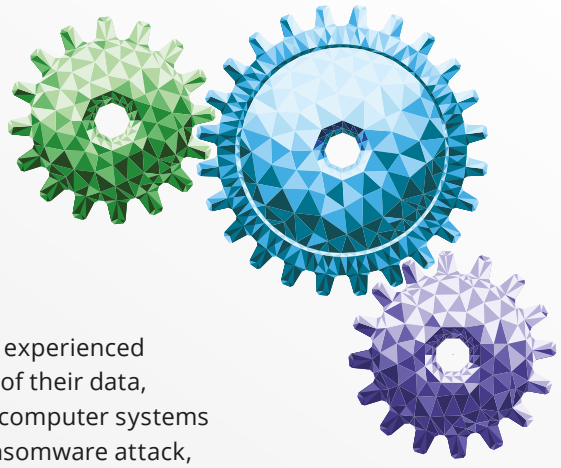
CASE STUDY

AUTOMOBILE DEALERSHIP



INCIDENT – RANSOMWARE

During one of their busiest times of the year, the client, a car dealership, experienced a large-scale ransomware attack that impacted multiple locations. Most of their data, including their back-up data, was encrypted by the threat actor, so their computer systems had to be taken offline to prevent further infection. As a result of the ransomware attack, all locations were rendered inoperable and remained closed until their systems were restored.

AXIS RESPONSE

The AXIS Incident Response Manager immediately put the client in contact with a panel of experts including:

- Forensic investigators, to investigate the scope of the intrusion, determine whether recovery of data was available on back-up systems, and begin negotiations with the threat actors to determine the amount of the ransom
- Privacy counsel, to provide legal advice and counselling to minimize the impact of any unauthorized access to legally protected data
- A forensic accountant, to calculate financial impact of business interruption

Upon notice to AXIS of this incident, the panel of cyber experts was mobilized within hours to assess the incident itself and advise the client with all the information they needed to determine the best course of action.

OUTCOME

Working together with the client, the ransomware was ultimately removed, data restored, and network fully operational within a short period of time to minimize further impact on the client's business. Once the client's business was restored, we provided compensation for the company's business income loss and additional expenses incurred during the period of restoration.

KEY CYBER COVERAGES TO CONSIDER

- Forensic and legal expense
- Data recovery expense
- Business interruption loss

PREPARE

- Provide cyber security and awareness training to all staff
- Segment networks to hinder the spread of malicious software
- Keep software and applications on servers and computers patched and updated
- Take steps to protect back-ups from ransomware