CASE STUDY

FOOD PROCESSING & DISTRIBUTION

INCIDENT – RANSOMWARE

The client, a food processor and distributor, had become a victim of a sophisticated ransomware attack. Taking matters into their own hands, the client wiped their system and restored it from back-up, hoping this would solve the issue. However, a month later, the threat actor began to threaten the owner with further ransomware attacks as they were still in the system.

They had gained access to extremely sensitive information, including social security numbers and the full contents of emails, from the first attack. Since that attack, the threat actor had already used the information to open credit cards and even divert supplier payments. They demanded a ransom to stop the threats and release the information they had taken.

AXIS RESPONSE

As soon as AXIS was informed of the situation, the Incident Response Manager assembled a panel of cyber experts, including:

- Forensic investigators, to secure the client's system as the threat actor still had access
- Privacy counsel, to notify the hundreds of people whose information had been compromised or were otherwise affected by the incident
- A negotiator specializing in ransomware cases, to begin a dialogue with the threat actor as the situation escalated

OUTCOME

The negotiator's dialogue with the threat actor ensured the client regained access to their systems and all the data held for ransom. As the attack affected so many people, the privacy counsel advised the client to take all the necessary legal steps to report the incident and inform those whose data had been at risk. Finally, to prevent future attacks of this nature, the forensic investigators secured the client's system.

KEY CYBER COVERAGES TO CONSIDER

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

PREPARE

- Prepare an Incident Response Plan and practice it regularly
- Provide cyber security and awareness training to all staff to ensure they are educated, but also empowered to flag a problem when it arises
- Apply multi-factor authentication passwords across the business
- Take steps to protect your back-ups from ransomware
- Annual cyber security hygiene/health check