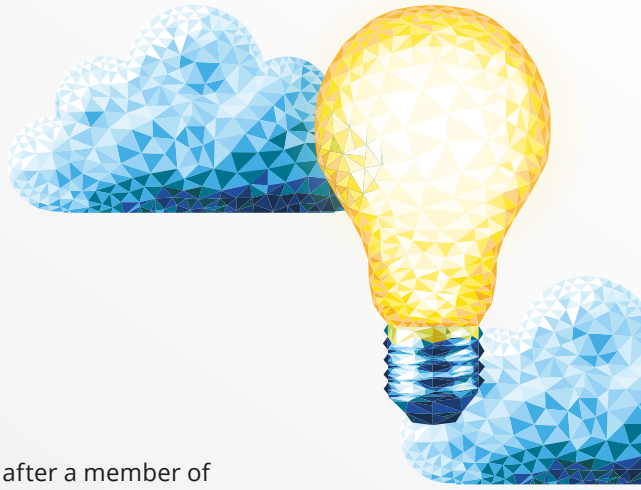
CASE STUDY

EDUCATION



INCIDENT – PHISHING

The client, a school, found their IT systems had been compromised after a member of staff clicked on a malicious link in an email. The school's IT department discovered that a threat actor had gained access to the entire email system, and were monitoring and redirecting emails, launching further phishing campaigns on the school's contacts.

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 around third-party liability and how to handle such campaigns efficiently
- Forensic investigators, to quickly restore the network before any additional harm could be done

The AXIS Incident Response Manager worked closely with the client's security team, coordinating initial calls and overseeing all activities.

OUTCOME

Thanks to the quick deployment of the panel, and their intervention in mitigating additional harm to the network, the school's systems were brought back under control before students and faculty returned to class.

KEY CYBER COVERAGES TO CONSIDER

- Forensic and legal expenses
- Incident response costs
- Security event liability

PREPARE

- Prepare an Incident Response Plan and practice it regularly
- Clearly articulate and enforce the password policy, ensuring all passwords are complex
- 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