Cyber Incident Response Service
Cyber Incident Response Services

AXA XL is committed to being a trusted partner in helping our clients improve their cybersecurity. We’ve partnered with Accenture to offer our clients end-to-end cybersecurity services, from bespoke cyber risk reports through to risk mitigation and post breach services.

Through AXA XL’s Cyber insurance policy, clients will have access to Accenture’s Cyber Incident Response Service. Working with AXA XL Claims handlers, this service guides insured clients through each stage of a cyber incident from initial notification, to investigation and containment, to restoration and closure of the incident.

What Services are Included?

- Global hotline – 24/7/365 service for first notification of loss
- Rapid triage & assessment – rapid triage of incidents to support containment
- Dedicated incident manager – for high-severity cyber incidents
- Specialised incident response teams – providing support on a global scale
- Specialist support – access to relevant service providers

How will this help me?

- Clearly signposted cyber claims process throughout the whole incident, from First Notification of Loss to Incident Resolution
- Access to technology expertise, combining cyber resilience insight as well as industry experience to provide relevant, timely information
- Rapid incident response capability that supports clients in responding to, containing and resolving incidents in a cost-effective manner
- A wider panel of cyber law firms, PR firms and other technology providers, to provide a comprehensive incident response service

Who will we work with?

Our partnership, with Accenture, provides you with access to a panel of market-leading vendors ready to respond to any type of cyber incident. Post breach providers include:

- Legal & regulatory
- Crisis comms & PR
- Identity fraud & credit monitoring
- Incident response & IT forensics
- Forensic accounting & e-discovery

Accenture Security

“At Accenture Security, we are committed to helping our customers respond and recover from cyber security incidents and to combat the evolving threat landscape to help organizations build cyber resilience”.

Justin Harvey
Global Incident Response Lead

Global Panel

The below firms are part of the Cyber Incident Response Panel as global vendors, able to provide support in a range of International markets*

Legal & Regulatory

- Clyde & Co
- CMS
- DLA Piper

Crisis Comms & PR

- BCW

Identity Fraud & Credit Monitoring

- Experian
- CyberScout

Incident Response & IT Forensics

- Accenture Security
- CrowdStrike
- CyberScout
- S-RM

Forensics Accounting & E-Discovery

- Epiq
- Baker Tilly

axaxl.com

Accenture may decide in its discretion to refuse to act or withdraw from providing certain services, including (but not limited to) for reasons owing to conflicts of interest, capacity constraints or specialist work outside of Accenture’s area of expertise. The first notification of incident activities provides a facility for you to make an initial report of an actual or potential cyber security incident. Accenture will endeavour to meet these estimated timeframes but we are not responsible if we fail to do so. This is because these timeframes are dependent on a number of factors including (but not limited to) the acceptance of the Terms for notification of incident activities and (if applicable) the Arrangement Letter, clearing our conflict of interest and other processes, the availability of the relevant service providers (and the clearance of their relevant processes), validation from you that the incident questionnaire is correct and the provision of any other information we may request. Panel availability and applicability may vary and is dependent on both incident severity as well as geography. Decisions on the engagement of panel providers is responsibility of end client, and will require approval from AXA XL prior to commencing work with panel provider.

* Panel availability and applicability to each incident may vary and dependent on both incident severity as well as geography. Panel members may decide in their discretion to refuse to act or withdraw from providing certain services, including (but not limited to) for reasons owing to conflicts of interest, capacity constraints or specialist work outside of their area of expertise.