
AXA
XL Insurance
Cyber Incident Response Service
accenturesecurity

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

Your company discovers a cyber security breach... now what?

Use this roadmap as a quick reference for what to do if you're the victim of a cyber incident.

Step 1:

Call the Cyber Response hotlines (details on next page) or email us at cyberclaims.axa@accenture.com

First notification of the incident

Provide policy information (e.g. policy number) and details of the incident to register a potential cyber incident and begin the incident response process. When emailing, leave contact details for a call-back from a Claims Manager.

A Claims Manager will walk you through the incident questionnaire to gain an understanding of the incident. English and French language support is available 24/7. Spanish and Portuguese language support during business hours, via call back for certain local languages, typically within 1 hour.

Step 2:

Accenture will set up a scoping call to determine next steps

2 Hours – 24 Hours

You will receive the questionnaire to validate the information captured is correct, along with our terms and conditions relating to the first notification of incident activities. These terms must be accepted and returned to us prior to the scoping call.

For more serious incidents you'll be assigned a dedicated Cyber Incident Manager to help you navigate through the incident.

The scoping call will outline the extent of the incident and conditions, review incident details and discuss next steps. Following the call, we will also send you our terms and conditions for Incident Management and Cyber Incident Response Services ("Arrangement Letter").

The Arrangement Letter must be accepted and returned to us prior to the provision of any Incident Management and Cyber Incident Response Services.

Step 3:

Initial Investigations commence

24 Hours – 48+ Hours

Where assistance is required, incident response teams will engage with you to support you in managing the incident.

You will have access to the following panel of cyber-focused vendors (if applicable).

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

* Panel availability and applicability to each incident may vary and is 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.

To access the Terms and Conditions for Incident Response, please visit https://cyberriskconnect.com/. Please note that these may vary depending on jurisdiction.

Important contact information

How you manage the first hours and days of a live incident or security threat is critical – not only for protecting your information, but also for safeguarding your business and reputation.

Please use the below contact information to engage with our Cyber Incident Response Service. Please also ensure you notify your insurance broker of the potential incident.

English and French language support is available 24/7. Spanish and Portuguese language assistance can also be provided by call-back within business hours.

Global email

cyberclaims.axa@accenture.com

Global phone number

+44 1895519407

Australia

1800324920

Singapore

18004075131

Brazil

08000474303

Spain

900816669

France

0805543012

Sweden

0201604304

Germany

08007243546

UK

0800 0859483

Italy

800949953

USA

8332579403

Netherlands

0800 2288005

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.