

CYBER FACTSHEET EUROPE

CyberRisk Coverage Highlights



Why you need the protection

It takes only one cyber event or data security breach to impair your company's financial results, or even potentially put you out of business. One resourceful hacker, virus, or system glitch can shut down your entire network within minutes, paralysing operations and your ability to earn income. One successful hack, lost laptop, or lost paper record can cause a data breach impacting the privacy of customers, employees, and others. Travelers has you protected from every angle... pre-breach, post-breach and always.

Coverage highlights

CyberRisk coverage is specifically designed to help in the event of a cyber breach. It's available for businesses of all sizes as a stand-alone policy or as part of a management liability suite of coverages. CyberRisk provides more solutions with options that include coverage for forensic investigations, litigation expenses associated with the breach, regulatory defence expenses/fines, crisis management expenses, business interruption and cyber extortion. And now, CyberRisk protection doesn't end after a breach occurs. New to CyberRisk is Betterment – an insuring

clause that provides coverage for costs to improve a computer system after a security breach, when the improvements are recommended to eliminate vulnerabilities that could lead to a similar breach. In addition to coverage, Travelers provides policyholders innovative value-added pre-breach and post-breach risk management services at no additional cost.

HCL Technologies pre-breach services

- **Cyber Resilience Readiness Assessment and Cyber Security Professional Consultation**
An online assessment designed for an organisation to quickly understand their current cybersecurity posture while receiving an official report and up to 1 hour consultation with a HCL Technologies security professional to help in improving areas of weakness or vulnerability.
- **HCL Technologies™ Cyber Security Awareness Training**
Gain access to security awareness training as a method of defence against cybersecurity threats by promoting proactive employee behaviour. These courses can be accessed on a cloud-based learning management system hosted by HCL Technologies or on your existing SCORM-compliant LMS platform.
- **Risk Management Expertise**
Topical insights and expertise on current cyber related trends, risks and threats that face organisations in today's business environment. These resources will help with your organisation's preparedness when it comes to cyber related events.

Travelers Breach Coach®:

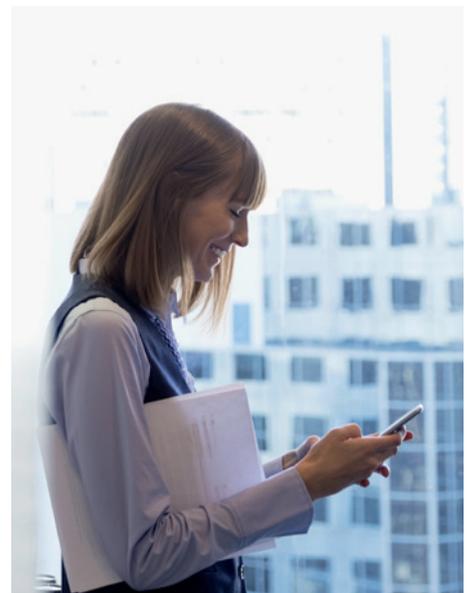
Should you experience a data breach event, you may choose to call the Breach Coach listed in the Travelers eRisk Hub portal for immediate triage assistance.

Your initial 30-minute consultation is at no additional charge.

Please be aware that the Breach Coach service is provided by a third-party law firm. Therefore, contacting the Breach Coach does NOT satisfy the claim or notification requirements of your policy

Risk Management Whitepapers:

Topical insights and expertise on current cyber related trends, risks and threats that face organisations in today's business environment. These resource guides will help with your organisation's preparedness when it comes to cyber related events.



Travelers CyberRisk coverage includes the following insuring clauses:

 **Liability Insuring Clauses:**

Privacy and security

Coverage for claims arising from unauthorised access to data, failure to provide notification of a data breach where required by law, failure to destroy confidential information, failure to comply with a privacy policy, wrongful collection of private or confidential information, failure to prevent a security breach that results in the inability of authorised users to gain system access, the participation in a DDoS attack, or the transmission of a computer virus.

 **Media**

Coverage for claims arising from copyright infringement, plagiarism, defamation, libel, slander, and violation of an individual's right of privacy or publicity in electronic and printed content.

 **Regulatory**

Coverage for administrative and regulatory proceedings, civil and investigative demands brought by domestic or foreign governmental entities or claims made as a result of privacy and security acts or media acts.

Breach Reponse Insuring Clauses:

 **Privacy Breach Notification**

Coverage for costs to notify and provide services to individuals or entities who have been affected by a data breach. Examples include call centre services, notification, credit monitoring and the cost to purchase identity fraud insurance.

 **Computer And Legal Experts**

Coverage for costs associated with analysing, containing, or stopping privacy or security breaches; determining whose confidential information was lost, stolen, accessed, or disclosed; and providing legal services to respond to such breaches.

 **Betterment**

Coverage for costs to improve a computer system after a security breach, when the improvements are recommended to eliminate vulnerabilities that could lead to a similar breach.

 **Cyber Extortion**

Coverage for ransom and related costs associated with responding to threats made to attack a system or to access or disclose confidential information.

 **Data Restoration**

Coverage for costs to restore or recover electronic data, computer programmes, or software lost from system damage due to computer virus, denial-of-service attack or unauthorised access.

 **Public Relations**

Coverage for public relations services to mitigate negative publicity resulting from an actual or suspected privacy breach, security breach, or media act.

 **Rewards**

Coverage for rewards paid for information that directly leads to the conviction of any person for committing or attempting to commit an illegal act related to the cover provided under the policy.

 **Cyber Crime Insuring Clauses:**

Funds Transfer Fraud

- Coverage for loss of money or securities due to fraudulent transfer instructions to the Insured's financial institution.
- Coverage for loss of money or securities due to a person impersonating another and fraudulently providing instructions to transfer funds.
- Coverage where due to a security breach the insured's client or vendor is duped into sending money or products to a fraudster rather than the rightful recipient.

 **Computer Fraud**

Coverage for loss of money, securities, or other property due to unauthorised system access.

 **Telecom Fraud**

Coverage for amounts charged by a telephone service provider resulting from an unauthorised person accessing or using an insured's telephone system.

Business Loss Insuring Clauses:

 **Business Interruption**

Coverage for loss of income and expenses to restore operations as a result of a computer system disruption caused by a virus, computer attack or system failure, including the voluntary shutdown of systems to minimise the business impact of the event.

 **Dependent Business Interruption**

Multiple coverage options for loss of income and expenses to restore operations as a result of an interruption to the computer system of a third party that the insured relies on to run their business.

 **System Failure**

Coverage for loss of income and expenses to restore operations as a result of an accidental, unintentional, and unplanned interruption of an insured's computer system.

 **Reputation Harm**

Coverage for lost business income that occurs as a result of damage to a business' reputation when an actual or potential cyber event becomes public.

Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.