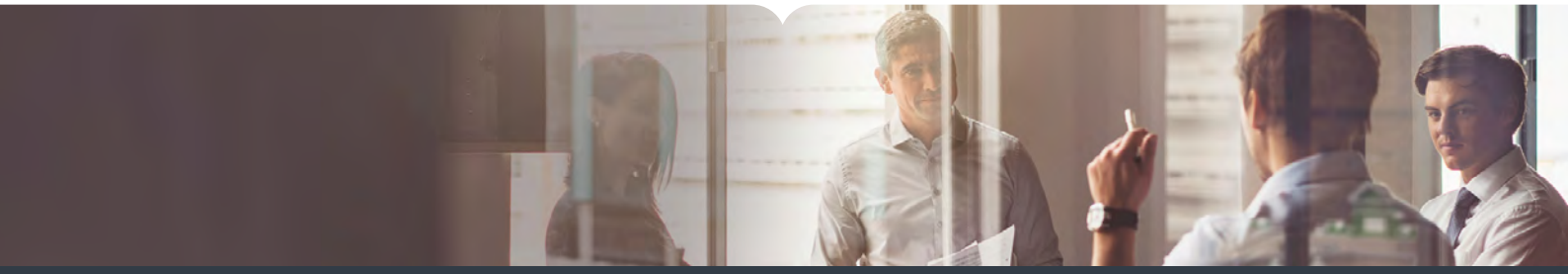
TRAVELERS



PRODUCT INFORMATION

Cyber protection for technology customers

In today's data-driven world where sensitive information is stored and transferred both on paper and electronically, organisations of all sizes are vulnerable to costly claims including claims made against you by others, arising from data security breaches and extortion demands that are occurring at alarming and growing rates.

Network Security – designed to help you protect your business

Whether data is compromised by a hacker, virus, cyber thief, or because of lost or stolen computers, laptops, flash drives, smart phones or dumpster diving, the breaches can have serious ramifications. There are substantial financial costs involved in finding the cause of and remedying a breach, including the cost of notifying customers. Your company can also suffer damage to its reputation and from the interruption to business activities.

Our Network Security coverage is effective as soon as you discover that you have suffered a breach or an extortion demand, and offers ten optional first-party cyber modules designed to help you protect your business.

Cover	What is covered?	Claim scenario
1. Security Breach Notification and Remediation Expenses	Data Breach Notification Expenses can arise from contractual agreements, regulatory requirements or voluntary agreements. In the event that you suffer an actual or alleged security breach we will cover the costs and expenses you incur: • including forensic fees, to determine the cause of the security breach and the persons whose identity information was accessed or acquired without their authorisation; • to develop materials and to notify those individuals whose identity information was accessed or acquired; • to provide credit or identity monitoring for two years or longer as may be required by relevant breach notification law; • to provide identity fraud insurance to affected persons; and to provide a call centre to handle inquiries.	A skilled cyber-criminal hacks into your company network and captures names, addresses, and credit card information for over 50,000 of your customers. Expenses will likely include the hiring of a breach response firm to find the cause of the breach, assisting with notice requirements and expenses, providing credit monitoring and a call centre for impacted individuals.
2. Crisis Management Service Expenses	Reimburses you for costs you incur to help off-set negative publicity generated from a cyber event.	Your Marketing Director has their laptop stolen. The laptop contains over 100,000 customer records, including personal contact information. Expenses will likely include hiring a public relations firm to restore customer confidence or mitigate negative publicity generated from the incident.
3. Extortion Expenses	Reimburses you for money or securities you pay to a person or organisation that seeks to extort money from you.	Your computer system is hacked and ransomware is installed. The hackers demand payment of £10,000 in Bitcoins to release your systems.
4. Business Interruption	Covers your loss of profit or revenue resulting from the interruption or interference with your business following the introduction of a computer virus or other unauthorised cyber-attack. In addition, contingent business interruption extensions are available to cover your dependency on IT providers and other outsource providers.	Your organisation's server is infected by a severe virus, and as a result, your e-commerce website is not available for an extended period, during which time you are unable to trade.

Cover	What is covered?	Claim scenario
5. Computer Programme or Electronic Data Restoration	Reimburses you for costs incurred to restore, replace or reproduce computer programmes, software or other data which is stored within your network, damaged or destroyed by a cyber-attack.	A hacker installs a virus on your network which causes damage to the system and wipes all of the data on the servers. You need to restore all the data that you have lost.
6. Computer Fraud	Covers your loss of money or securities due to an unauthorised instruction to your computer network to transfer money to a third party account.	An organised crime ring hacks into the accounts payable data in your computer system and alters the bank routing information on outgoing payments. This results in £500,000 being transferred to the crime ring's account.
7. Funds Transfer Fraud	Covers your loss of money or securities due to the fraudulent electronic instruction by a third party to a financial institution.	You receive an email that appears to be from your bank but is not. Your employee opens the email, which activates a computer virus called a Trojan Horse that reads keystrokes. The perpetrator uses this means to obtain banking and password information and initiate a fraudulent electronic wire transfer from your bank account.
8. Telecommunications Theft	Reimburses you for charges you incur as a result of long distance calls being made following a hack into your telephone system by a non-employee.	A criminal gang gains access to your long distance telephone systems, and makes multiple calls to a number chargeable at a premium rate, costing the company thousands of pounds in call charges.
9. Damage to Computer Equipment	Covers the costs to repair or replace your computer equipment that is damaged or is no longer operable following the introduction of a computer virus or other unauthorised cyber-attack.	After a suspected cyber breach, your firms systems are not functioning as they should. Following an investigation by an IT professional, it appears there is damage to the computer equipment which has led to it running considerably slower than it should.
10. Rewards Expenses	Reimburses you for money you pay for information which leads to the arrest and conviction of an individual committing an act which leads to loss under any of the modules (1-9) above.	Following a cyber breach, you receive a call from an unknown third party who offers you information which will give you the details of the persons who launched this attack, in exchange for a monetary reward. Travelers will reimburse you for the payment of this reward on the proviso that it leads to the arrest and conviction of the perpetrator.
11. Defamation	Covers you for claims and the associated costs and expenses brought against you for unintentional libel or any other unintentional defamation.	A client posts some feedback onto the chat room area of your website that explains why they choose to use your company over one of your major competitors. Their reasons include the statement that the competitor did not create a good working environment and that an employee, a personal friend of theirs, had been harassed by the directors in the course of their work. The post has been seen by the competitor who seeks damages.
12. Personal rights	Covers you for claims and the associated costs and expenses brought against you for your unintentional breach of confidence or failure to protect private or confidential information of others.	Your employee's company laptop is stolen from his home. The laptop contains private financial information of your clients and is not encrypted. Your clients sue you for damages caused by your failure to protect their private financial information.
13. Computer virus	Covers you for claims and the associated costs and expenses brought against you as a result of your unintentional transmission of a computer virus, whether or not created by you, to a third party's computer system.	Your employee inadvertently downloads a destructive computer virus that spreads to other files housed on your computer network. Your client downloads information from your website, allowing the virus to spread to the client's computer system and resulting in widespread loss of data and a computer network shutdown. Your client sues you, contending you should have prevented transmission of the virus. The client seeks damages for the lost data and economic loss caused by the network shutdown.
14. Data Protection	Covers you for your unintentional failure to comply with the requirements of data protection legislation.	Your server has been hacked and the personal information of your clients and past clients have been stolen. It has emerged that personal data of past clients was kept for longer than was necessary and was not appropriately secured and a claim is brought under the Data Protection Act.
15. Cyber computer misuse	Covers you for claims, and the associated costs and expenses, brought against you as a result of the corruption and modification of software programmes and data. Cover includes the modification or theft by your employee of data entrusted to you by your clients.	An employee corrupts your client's data that has been entrusted to you, which means your client incurs additional costs when trying to use this data. This results in a demand for compensation from your client.

Cover	What is covered?	Claim scenario
16. Denial of access	Covers you for claims and the associated costs and expenses brought against you as a result of an authorised third party being unable to gain access to your computer systems.	Your system has been the target of a Distributed Denial of Service (DDoS) attack, which slows and ultimately crashes your system. You have failed to install the appropriate patches and computer updates. Many of your clients are reliant on your online services to trade effectively and are seeking damages for loss of income suffered as a result of being unable to access your network.
17. Cybermedia Intellectual Property Rights	Covers you for claims and the associated costs and expenses brought against you in respect of your unintentional infringement of intellectual property rights or laws. Cover includes infringement of patent or trade secrets (except where claims are brought in North America).	You inadvertently include a picture taken by a third party on your website without permission and you are subsequently sued for breach of copyright.

Data Breach Response Service

A data breach response service is available 24/7 to assist you in the event that you suffer an actual or alleged data breach. This service is in partnership with a leading law firm who are experts in handling data breach events. Customers will also have the benefit of access to a wide range of specialist partners in areas such as IT forensics, public relations and denial of service attack response.

An initial complimentary 30 minute consultation with a Data Breach Coach is provided for each cyber event giving you access to the relevant expertise and knowledge to help mitigate against potential losses.

Cybermedia Liability – designed to protect your business from third party cyber exposures arising through the use of the internet, e-mail or website

The internet makes it easier to see and be seen, which has implications for increasing the likelihood of accidentally infringing the intellectual property rights of others, or for unintentional defamation by failing to remove libellous statements on your website bulletin board.

The internet and other electronic communications also provide an access point into your business which can impact your liability for protecting confidential information of others, or complying with data protection legislation.

In the course of your everyday business, the introduction of a virus to your computer system that you inadvertently pass on to your customers' systems, or the impact of a computer hack which could prevent your authorised customers from accessing your computer system, can be costly.

Our Cybermedia Liability covers can provide insurance protection for claims made against you by others. Cover is provided for civil liability for compensation, claimants costs and expenses, and your own defence costs and expenses.