



## CLAIM EXAMPLES

# How CyberRisk responds to assist and protect our Insureds

## Liability Insuring Agreements



### Privacy and Security

#### What is covered

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.

#### Claim Scenario

A hacker obtains sensitive personal information from the insured's computer system. As a result, a number of customers bring a claim against the insured for allowing access to their personal information.

#### Coverage Response

Damages and defence costs for covered lawsuits.



### Media

#### What is covered

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

#### Claim Scenario

A third party brings a lawsuit against the insured alleging that the insured plagiarised

the third party's online content and organisational branding as well as infringed upon its trademarks.

#### Coverage Response

Damages and defence costs for covered lawsuits.



### Regulatory

#### What is covered

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.

#### Claim Scenario

A hacker obtains sensitive personal information from the insured's computer system. As a result, the Information Commissioner's Office bring a regulatory action against the insured.

#### Coverage Response

Costs for responding to regulatory claims stemming from the data breach, including any resulting fines or penalties (where insurable by law)

## Breach Response Insuring Agreements



### Privacy Breach Notification

#### Definition

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.

#### Claim Scenario

A fraudster hacks into the insured's internal processing system. Names, addresses and National Insurance numbers for more than 50,000 of the insured's customers are captured from the system, requiring notification to all 50,000 customers.

#### Coverage Response

Costs to deliver notice to impacted customers, and to provide credit monitoring, a call center, and an ID fraud policy for impacted individuals.



### Computer and Legal Experts

#### Definition

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.

#### Claim Scenario

An insured suspects that a fraudster hacked into its internal processing system when the police notifies them of identity theft impacting a number of the insured's customers.

#### Coverage Response

Costs to engage a forensics provider to contain the breach and determine its scope and legal costs to determine the insured's notification obligations under relevant privacy laws and provide other services to assist the insured in responding to and managing the breach.



## Betterment

### Definition

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.

### Claim Scenario

The insured's computer system is compromised by ransomware. Forensic providers contain the virus and determine that the source of the infiltration is a vulnerability in the insured's computer system. Upon recommendation from the forensic provider, the insured purchases new software to improve its system security.

### Coverage Response

Costs to purchase new software to address the system vulnerability.



## Cyber Extortion

### Definition

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

### Claim Scenario

The insured's system is infected with a virus that encrypts the insured's data. A ransom payment is demanded to unlock the system.

### Coverage Response

Costs to manage and mitigate the incident, and if necessary, payment of the ransom demand.



## Data Restoration

### Definition

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

### Claim Scenario

A computer virus corrupts the insured's software and data.

### Coverage Response

Costs for recovery and restoration of the insured's electronic data and computer programs.



## Public Relations

### Definition

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

### Claim Scenario

The insured's chief financial officer has his laptop stolen. The laptop contains more than 100,000 customer records, including National Insurance numbers.

### Coverage Response

Costs for hiring a public relations firm to mitigate negative publicity generated from the incident.



## Rewards

### Definition

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.

### Claim Scenario

The insured offers a £10,000 reward for information following a break in where customers' personal data was stolen. Information received leads to the conviction of the burglar.

### Coverage Response

Reimbursement of the reward paid.

## Cyber Crime Insuring Agreements



## Computer Fraud

### Definition

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

### Claim Scenario

An organised crime ring gains unauthorised access to the insured's accounts payable in their computer system and alters the bank routing information on outgoing payments resulting in a £100,000 transfer to the crime ring's account.

### Coverage Response

Reimbursement of the insured's funds



## Funds Transfer Fraud

### Definition

Coverage for loss of money or securities due to fraudulent transfer instructions to a financial institution.

### Claim Scenario

A fraudster obtains the insured's information and uses the information to impersonate the insured to its financial institution. The fraudster requests a £100,000 transfer from the insured's bank account.

### Coverage Response

Reimbursement of the insured's funds.



## Social Engineering Fraud

### Definition

Coverage for loss of money or securities due to a person impersonating another and fraudulently providing instructions to transfer funds.

### Claim Scenario

An employee in the insured's accounts payable department receives an email purportedly from an established vendor changing the vendor's banking instructions. The employee relies upon the fraudulent email instruction and transfers £50,000 from the insured's bank account to the fraudster. The insured discovers the fraud when the real vendor contacts the insured requesting payment.

### Coverage Response

Reimbursement of the insured's funds.



## Vendor or Client Payment Fraud

### Definition

Coverage for loss of money or securities due to fraudulent delivery instructions

### Claim Scenario

A company contracts to provide a product to a customer, however the company's computer system is hacked and bogus delivery details are provided, thus diverting the dispatched product to the fraudster rather than the customer

### Coverage Response

Reimbursement of the additional cost of supplying the product to the original customer



## Telecom Fraud

### Definition

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

### Claim Scenario

An unknown third party gains unauthorised access to the insured's telephone system and uses the system to incur £50,000 in international charges. The insured discovers the loss when it receives its monthly statement from its telephone provider containing the fraudulent charges.

### Coverage Response

Reimbursement of the fraudulent charges the insured is required to pay to its telephone provider.

## Business Loss

## Insuring Agreements



## Business Interruption

### Definition

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

### Claim Scenario

An insured's computer system is infected by a virus and as a result, the insured's internal computer network is not available for an extended period of time.

### Coverage Response

Payment to the insured for its lost income as a result of the disruption and expenses incurred to restore operations.



## System Failure

### Definition

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.

### Claim Scenario

An organisation's computer system is rendered inoperable through employee negligence and as a result, the insured's business operations are shut down for an extended period.

### Coverage Response

Payment to the insured for its lost income as a result of the disruption and expenses incurred to restore operations.



## Dependent Business Interruption

### Definition

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.

### Claim Scenario

A cloud services provider's system is infiltrated by malware and rendered inoperable. As a result, the insured is unable to access its data and its business operations are shut down for an extended period.

### Coverage Response

Payment to the insured for its lost income as a result of the disruption and expenses incurred to restore operations.



## Reputation Harm

### Definition

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.

### Claim Scenario

The insured's system is compromised by malware that permits an unknown third party to gain access to 100,000 customer records containing personally identifiable information. Following the insured's investigation, and notification to affected individuals, the local media runs an article about the event damaging the insured's business reputation.

### Coverage Response

Payment to the insured for its lost income resulting from disclosure of the event.

Get  
cyber  
ready

Visit

[www.travelers.co.uk/cyber](http://www.travelers.co.uk/cyber)

for more cyber security  
tips for your business.



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.

[travelers.co.uk](http://travelers.co.uk) [travelers.ie](http://travelers.ie)