Cyber
Summary of cover

This is a summary of our cyber insurance cover and does not contain the full terms and conditions of the cover, which can be found in the policy document. It is important that you read the policy document carefully when you receive it.

What is cyber insurance?

Aviva cyber insurance protects you against loss of, or damage to, information from IT systems and networks. It covers such things as hackers and cyber criminals causing damage or disruption to data, the subsequent loss of revenue and funds as well as your liability arising from an event. It gives you 24/7 access to an incident manager and the specialist support required to recover from a cyber related event.

Significant benefits and features

- **Incident Response:** 24/7 access to our team of experts.
- **Data Security Breach:** costs to manage a breach including IT forensic experts, legal advice, notifying affected individuals and offering credit or identity fraud monitoring services.
- **Data recovery:** costs due to a virus, hacking or denial of service attack. If your computer equipment is damaged, we will repair or replace it.
- **Data Regulation Breach:** protection against a breach of Data Regulation. This includes cover for your defence costs and regulatory fines (where insurable by law).
- **Business Interruption:** loss of revenue as a result of a malicious attack, extortion or a data breach directly affecting your IT systems or those of your outsourced IT or data provider.

  Additional Expenses: to reduce the reduction in revenue.

  This could be the cost to hire extra staff or equipment.
- **Extortion*:** recovery costs or ransom payment (where insurable by law) if a hacker holds your business to ransom or threatens to reveal sensitive data until a ransom is paid.
- **External cyber Crime (optional cover):** financial loss due to unauthorised access to your IT network or if a third party deceives an employee into paying or transferring money by impersonating another person.

  Theft of Personal Money: loss of directors' or employees' money from their personal bank account due to unauthorised access to your IT network.
- **Telecommunications Services (optional cover):** cost of unauthorised telephone calls and charges made by an external hacker.
- **Reputation Management Expenses:** costs of PR consultants to minimise adverse publicity following an incident.
- **Resilience Improvements:** costs to improve the resilience of your computer system following a claim.
- **Network Security:** negligent transmission of a virus to a third party or failure to prevent unauthorised access to your systems leading to a denial of service attack e.g. a supplier is unable to access your website and their business suffers a financial loss.
- **Data Privacy and Confidentiality:** damage or distress suffered by your customers or employees due to a data breach whether it was accidental or hacking of personal data. Loss, disclosure or destruction of third party confidential commercial information held under an agreement that results in a financial loss.
- **Payment Card Liability:** costs resulting from non-compliance with payment card industry data security standards. This includes fees, charges and recertification costs.
- **Multimedia Liability*:** costs if you mistakenly infringe the copyright or trademark of a third party due to your use of on line media. Cover for defamatory comments made on line. This could be in an email or social media.

  Media Removal: we'll cover the costs to remove on-line content if it helps avoid a claim being made against your business.

* Optional cover on our Digital Cyber product

Significant exclusions and limitations

The most significant exclusions and limitations are listed below. Please refer to the policy wording for the full list of exclusions and limitations.

- External cyber crime does not include losses deliberately carried out by an employee or if they work in collusion with a third party.
- We will not cover You for more than one claim arising from the same extortionist.
- Failure of infrastructure including the internet, utilities, telecommunications ,domain name service, certificate authority or content delivery network.
- Errors or omissions in any professional advice or services.
- Any proceedings or claims brought by a subsidiary, parent or associate company.
- Infringement of patents or misappropriation of trade secrets, or licence fee or royalties in respect of intellectual property.
- Unlawful surveillance or any unsolicited communications or unauthorised collection of data.

Certain limitations apply to the policy. This will be shown on your schedule, for example:

- The excess (the amount you have to pay on any claim).
- Any loss of revenue claim that lasts less than 8 hours.
- We will not cover prior claims or circumstances that you were aware of, or ought to have known of, prior to the cover start date.
- You must not disclose that you have Extortion cover unless disclosure is required by law.

Things you need to do

This is a summary of the actions you must take in relation to our cyber insurance cover to make sure you are protected and that your policy cover operates fully.

- Any default or manufacturers' passwords or access codes must be changed and kept secure.
- Data must be backed up no less frequently than every 7 days. You must check backup routine is working, and backups must be stored securely and separately from the original data or programs.
- All personal data and other sensitive, protected or confidential data must be stored and disposed of in a secure manner.
- Updates to software must be carried out within 14 days of an update being released, where the product vendor describes the issue as 'critical' or 'high risk', or the update addresses a vulnerability with a Common Vulnerability Scoring System (CVSS) v3 score of 7 or above.
- Computer equipment connected to the internet or an external network must be protected against unauthorised access by an active firewall.
- Computer equipment and any personal devices used for accessing your computer systems must have effective and up to date software protecting against virus and malicious code that's updated at least once a month.
- On receiving a cyber extortion demand you must immediately notify and comply with the requirements of our Claims Service Provider. You will also need to report the crime to Action Fraud, the UK's national fraud cybercrime reporting centre.
- You, your partners, directors and employees must be trained in the dangers of social engineering fraud and how to spot these attempts and you must keep a record of such training.
- You must have a documented policy in place, which states that details of any new payee requests or amended payment instructions are always checked verbally by using details held on file or a published website and do not solely rely on the new instruction. This policy must be accepted by all Partners, directors and Employees, with such acceptance recorded.

Cyber incident response service

Speed is of the essence when there's a cyber security breach. Our cyber incident response team provides immediate support 24/7, providing access to all the specialist support required to:

- identify, contain and repair a breach and restore data
- provide legal and PR consultancy to help safeguard your reputation
- notify those individuals affected by a breach and co-ordinate credit or identity theft monitoring for your customers
- provide consultancy to prepare for any regulatory investigation.

Your obligations

This is a summary of the actions you must take to make sure your policy cover operates fully.

- You must make a fair presentation of the risk to us, which includes telling us of any circumstances which we would take into account in our assessment or acceptance of this insurance. If you fail to make a fair presentation of risk this could affect the extent of cover provided or invalidate your policy.
- You must also make a fair presentation to us in connection with any variations, e.g. changes you wish to make to your policy.
- You must take all reasonable precautions to prevent loss or damage, and comply with any security or other loss prevention conditions in your policy documents.
- You must notify us promptly of any event which might lead to a claim and follow the claims procedure set out in your policy.
- For further details and any specific obligations relating to your trade or business activities following our assessment of your risk, please refer to your policy documents.

Making a claim

Claims can be reported via our cyber claims team on **0800 051 4473**.

How do I make a complaint?

If for any reason you are unhappy with our service, we would like to hear from you. In the first instance, please contact your insurance adviser. Where a complaint cannot be resolved to your satisfaction, you may be able to ask the Financial Ombudsman Service to carry out an independent review. Whilst we are bound by their decision you are not. Contacting them will not affect your legal rights. You can contact the Financial Ombudsman Service by telephone on **0800 023 4567**. You can also visit their website at **www.financial-ombudsman.org.uk** where you will find further information.

Where am I covered?

This will depend on the product and choices you have made. Please refer to the policy booklet for details of where you are covered.

When and how do I pay?

Payment options should be discussed with your insurance adviser.

How do I cancel the contract?

You can cancel your policy at any time during your period of cover, subject to the notice period shown in your policy. To cancel, contact your insurance adviser.

Would I receive compensation if Aviva were unable to meet its liabilities?

Depending on the circumstances of your claim you may be entitled to compensation from the Financial Services Compensation Scheme (FSCS) if we cannot meet our obligations. **See fscs.org.uk**

| Retirement | Investments | Insurance | Health |

BCOAG14424 10.2023

AVIVA