Cyber Respond
Summary of Cover

This is a summary of our Cyber Respond 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 Respond insurance?

Aviva Cyber Respond is our alternative Cyber offering which provides you with a simpler product designed with the needs of smaller businesses in mind, offering cover limits of £25,000, £50,000 and £100,000 with the option to add External Cyber Crime up to a cover limit of £10,000. Cyber Respond is suitable where you don't need the extended covers or higher limits of Cyber Complete.

Significant benefits and features:

- **Incident Response:** 24/7 access to our team of experts.
- **Data Security Breach:** cover for costs to manage a breach including IT forensic experts, legal advice, notifying affected individuals and offering credit or identity fraud monitoring services.
- **Data Recovery:** cover for costs of restoring data lost as a result of virus, hacking or denial of service attack. If your computer equipment is damaged, we will repair or replace it.
- **Reputation Management:** cover for costs of public relations consultants to minimise adverse publicity following a loss.
- **Increased Cost of Working:** cover for additional expenses incurred as a result of a cyber incident, helping you continue trading.
- **External Cyber Crime (optional cover):** cover for 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: cover for loss of directors' or employees' money from their personal bank account due to unauthorised access to your IT network.
- **No compulsory excess as standard**

Significant exclusions and limitations:

- External cyber crime does not include losses deliberately carried out by an employee or which result from them working in collusion with a third party.
- We will not cover any loss arising from pre-existing faults in or the unsuitability of programs or computer systems or software unless caused by Virus or Similar Mechanism, Hack or Denial of Service Attack.
- We will not cover any payment made to a Cyber Extortionist following a Cyber Extortion.
- Loss resulting from failure of the internet, utilities, telecommunications, domain name service, certificate authority or content delivery network.

How does our Cyber Respond product differ from our Cyber Complete product?

You'll find below an 'at a glance' comparison of the covers provided under both products. This does not contain the full terms and conditions of the cover, which can be found in the policy document.

Cover	Cyber Respond	Cyber Complete
Breach response		
24/7/365 Incident response	✓	✓
Cover for costs of an incident manager	✓	✓
Cover for costs of specialist IT forensics	✓	✓
Cover for costs of specialists to resolve the event	✓	✓
Legal support	✓	✓
Support with any regulatory reporting required	✓	✓
Notification costs following a data security breach	✓	✓
Reputation management	✓	✓
Resilience improvements	✗	✓
Criminal reward fund	✗	✓
First-party: business loss		
IT systems and data	✓	✓
Cyber terrorism	✓	✓
Increased cost of working	✓	✓
Business interruption	✗	✓
Outsourced service providers interruption	✗	✓
System failure	✗	✓
Optional customer and supplier extensions for certain risks	✗	✓
Cyber extortion ransom payment	✗	✓
Manufacturing and other industrial processes	✗	✓
Regulatory fines and penalties (where insurable by law)	✗	✓
External cyber crime (optional)		
Unauthorised use of computer equipment	✓	✓
Social engineering fraud	✓	✓
Funds transfer fraud	✓	✓
Telecommunications fraud	✗	✓
Corporate identity fraud	✗	✓
Theft of personal money	✓	✓
Virtual currency	✓	✓
Third-party: liabilities		
Network security	✗	✓
Data privacy	✗	✓
Multimedia	✗	✓
Media removal costs	✗	✓
Payment card industry	✗	✓

Cover	Cyber Respond	Cyber Complete
Additional benefits		
Minimum excess	£0	£1,000
Excess not applicable if advice provided by incident response is able to resolve the·issue	✓	✓
Cover applies to both electronic and physical data	✓	✓
Legal helpline and support available at no additional cost	✓	✓
Counselling service for employees affected by a cyber event	✓	✓
Free cyber and data risk management materials and resources	✓	✓
Access to cyber specialist partners at preferential rates	✓	✓
Free 2-hour cyber risk management consultancy session with an Aviva Risk Management Consultant (for policyholders paying £5,000 premium)	✗	✓

Added-value services:

DAS Businesslaw

https://avivabusinesslaw.farill.io/

This is a complimentary website, provided by Aviva, offering many tools and resources to help you manage your business effectively. Once insurance is in place with us, you will have access to:

- Unlimited legal advice via the legal advice helpline.
- Email alerts on changes in law, legislation and regulation.
- A range of regularly updated business and legal guides, document builders, interactive checklists and videos that can help with the day-to-day running of the business, as well as helping to manage exposure to legal risk.
- Topics ranging from branding, crowdfunding and financial and tax planning to marketing strategy can help to build and grow your business.

Things you need to do

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

- Access to Computer Equipment must be authenticated by the use of individual identification and passwords.
- 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 anti-virus software that's updated at least once a month.
- 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.

Your obligations

This is a summary of the main 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 notify us promptly of any event which might lead to a claim and follow the claims procedure set out in 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 document.
- 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.

How long does my Aviva Business Insurance last for?

Your policy will remain in force for 12 months from the date of commencement (or as otherwise shown on your Schedule) and for any period for which you renew the policy, as long as you continue to pay your premium.

Making a Claim

If you need to make a claim please call our claims line using the appropriate telephone number shown below. Our line operates 24 hours a day, 365 days a year. Please have your policy number to hand when calling.

Telephone: 0800 051 4473

Calls to 0800 numbers from UK landlines and mobiles are free. For our joint protection telephone calls may be recorded and/or monitored.

How do I make a complaint?

If for any reason you are unhappy with the product or service, please get in touch as soon as possible. For contact details and more information about the complaints procedure please refer to your policy documents.

Where a complaint cannot be resolved to your satisfaction you may be able to ask the Financial Ombudsman Service (FOS) to carry out an independent review. Whilst firms are bound by their decision you are not. Contacting them will not affect your legal rights. You can contact the FOS on **0800 023 4567** or 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**

BCOAG16626 10.2023

AVIVA