Security & Privacy Protection Insurance

Ransomware Form

DUAL

	Yes	No
1. Please confirm that an email filtering system is used and that the system is activated for all email accounts?	☐	☐

2. Does the email filter provide the following protections? Please tick all that apply:

- ☐ screenings for malicious attachments/links
- ☐ quarantine service
- ☐ reputation checks
- ☐ email fraud defence (DMARC)

3. Do you use Office 365 in your organisation?	☐	☐

If 'Yes', tick all that apply:

- ☐ Office 365 Advanced Threat Protection add-on
- ☐ multi-factor authentication for all users of Office 365

4. Do you use endpoint detection and response (EDR) tools for malware protection?	☐	☐
5. Do you have a Security Operations Centre (SOC) in place?	☐	☐

If 'Yes', tick all that apply:

- ☐ 24/7
- ☐ MSSP
- ☐ SIEM

6. Please confirm you secure any and ALL remote access to their corporate network or any cloud-based services by requiring multi-factor authentication. This relates to access by any party, including third party vendors granted authorised access, via any means other than a wired connection to the company network when at a physical location owned or operated by the insured.	☐	☐
7. Do you use multi-factor authentication to protect privileged user accounts?	☐	☐
8. Are access controls based upon the principle of least privilege?	☐	☐
9. Do you back up critical data regularly (minimum once per week)?	☐	☐
10. Are your back-ups disconnected from and inaccessible through the organisation's network and/or do you use a dedicated cloud storage provider, designed for this purpose?	☐	☐
11. Do you test the successful restoration and recovery of key server configurations and data from back-ups?	☐	☐
12. Do you have a secure/hardened baseline configuration which is regularly reviewed and updated by someone with the security expertise and/or in line with industry standards?	☐	☐
13. Have you undertaken a Network scan regarding unauthorised access/malware etc. within the past 60 days?	☐	☐
14. Confirmation that processes are in place to identify and apply patches within 30 days of release	☐	☐

15. If you answered 'No' to any of the above, please provide additional details.

16. Please describe any additional steps your organisation takes to detect and prevent ransomware attacks (network segmentation, software tools, external security services, penetration tests, vulnerability testing etc.)

Declaration

Duty to make a fair presentation of the risk/disclose material information

From 12 August 2016, the duty of disclosure for commercial insurance contracts changed with the implementation of the Insurance Act 2015 ("The Act"). For risks incepting or renewing on or after 12 August 2016, you have a duty to make "a fair presentation of the risk". To meet this duty, you need to disclose all material information to Insurers which is known to you (or which ought to be known to you). Information is material if it would influence the judgement of a prudent insurer in establishing the premium or determining whether to underwrite the risk and, if so, on what terms. Material information does not necessarily have to actually increase the risk of the insurance under consideration.

I/We declare that the answers to the questions in this proposal form are true and accurate having consulted with all partners or directors and other persons involved in the management of the applicant firm.

This application must be signed by a corporate officer with authority to sign on the applicant's behalf.

I/we understand that the information provided will be used in deciding whether the insurer will accept the application, the terms of any policy provided and the price charged by the insurer for the risk

Title ..... Name of Partner/ Director .....

Signature of Partner/ Director .....

Date .....

A copy of this proposal should be retained by you for your own records.

dualgroup.com/cover-cyber

Helping you do more