

DUAL Cyber

# Security and privacy protection

Ransomware questionnaire

**DUAL**



# Security and privacy protection ransomware questionnaire

- 
01. Please confirm which of the following email filtering systems are used and that the system is activated for all email accounts:
- |           |          |                                    |  |  |
|-----------|----------|------------------------------------|--|--|
| MailChimp | MimeCast | Other not listed (please specify): |  |  |
|-----------|----------|------------------------------------|--|--|
- 
02. Do you use Office 365 in your organisation? If **yes**, please also answer below:
- |   |     |    |
|---|-----|----|
| Do you use the Office 365 Advanced Threat Protection add-on?            | Yes | No |
| Do you enforce multi-factor authentication for all users of Office 365? | Yes | No |
- 
03. Do you use endpoint detection and response (EDR) tools for malware protection?
- |     |    |
|-----|----|
| Yes | No |
|-----|----|
- 
04. Please confirm you secure all remote access to your network and any cloud-based application where sensitive data may reside (including, but not limited to; webmail, Citrix desktop, or Remote Desktop Protocol "RDP") by requiring access using multi-factor authentication:
- |     |    |
|-----|----|
| Yes | No |
|-----|----|
- 
05. Do you use multi-factor authentication to protect privileged user accounts?
- |     |    |
|-----|----|
| Yes | No |
|-----|----|
- 
06. Are access controls based upon the principle of least privilege?
- |     |    |
|-----|----|
| Yes | No |
|-----|----|
- 
07. 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?
- |     |    |
|-----|----|
| Yes | No |
|-----|----|
- 
08. Are your back-ups disconnected from and inaccessible through the organisation's network?
- |     |    |
|-----|----|
| Yes | No |
|-----|----|
- 
09. Do you test the successful restoration and recovery of key server configurations and data from back-ups?
- |     |    |
|-----|----|
| Yes | No |
|-----|----|
- 
10. Confirmation that processes are in place to identify and apply patches within 30 days of release:
- |     |    |
|-----|----|
| Yes | No |
|-----|----|
- 
11. Please describe any additional steps your organisation takes to detect and prevent ransomware attacks (network segmentation, software tools, external security services etc.):

# Declaration

I/We declare that the statements made and particulars given in the proposal are true and I/we have not mis-stated or suppressed any material fact.

I/We undertake to inform insurers of any material alteration to these facts occurring before completion of the contract of insurance.

Signature of partner/director:

Name of partner/director:

Date:

DD      MM      YYYY

## Helping you do more

One Creechurch Place, London EC3A 5AF

+44 (0)20 7337 9888

[enquiries@dualgroup.com](mailto:enquiries@dualgroup.com)

[dualinsurance.com](http://dualinsurance.com)

DUAL Corporate Risks Limited is authorised and regulated by the Financial Conduct Authority under firm reference number 312593. DUAL Corporate Risks Limited is registered in England and Wales No. 4160680, with its registered offices at: One Creechurch Place, London EC3A 5AF. UK0075.

