

Business Risk Partners Ransomware Supplemental

A. Back-up and Recovery Capabilities

1. How often do you backup your data and systems?

Real time Hourly Daily Weekly Other

2. Are your backups encrypted? Yes No

3. Is backup data kept fully isolated (offline) from the enterprise network so that it is inaccessible from endpoints and servers that are joined to the corporate domain? Yes No

i. If not, please identify any mitigating controls in place:

4. Do you use credentials unique to backups that are stored separately from user credentials? Yes No

5. What is your lowest Recovery Time Objective (RTO)?

<4hrs <12hrs <24hrs <48hrs other

6. Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware? Yes No

B. Email Security

1. Can your users access e-mail through a web app on a non-corporate device? Yes No

i. If Yes: do you enforce Multi-Factor Authentication (MFA)? Yes No N/A

2. Does all email traffic get routed through an email gateway manager? Yes No

i. If Yes, what tool is employed?

3. Do you use Office 365 in your organization? Yes No

i. If Yes: Do you use the o365 Advanced Threat Protection add-on? Yes No N/A

4. Is phishing training conducted to all staff on at least an annual basis? Yes No

C. Network Security

1. Do you use MFA to protect privileged user accounts? Yes No

Business Risk Partners Ransomware Supplemental

| | | |
|---|---|--|
| 2. Do you use MFA for all remote access to the network? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 3. Do you manage privileged accounts using tooling (e.g., CyberArk)? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 4. Is the network physically or virtually segregated? | Both <input type="checkbox"/> Physically <input type="checkbox"/> Virtually <input type="checkbox"/> Neither <input type="checkbox"/> | |
| 5. Have you configured host-based and network firewalls to disallow inbound connections by default? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 6. In what time frame do you install critical and high severity patches across your enterprise? | <1 day <input type="checkbox"/> <1 week <input type="checkbox"/> <1 month <input type="checkbox"/> Other <input type="checkbox"/> | |
| 7. Do you use an endpoint protection product across your enterprise? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 8. Do you use an endpoint application isolation and containment technology? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 9. Do you have any end of life or end of support software? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| i. If Yes, is it segregated from the rest of your network? | Yes <input type="checkbox"/> | No <input type="checkbox"/> N/A <input type="checkbox"/> |
| 10. Please use this section to provide any clarifying or additional detail related to your answers above. | | |
| 11. Please detail any additional measures to mitigate the risk of ransomware: | | |

D. Declaration

I accept that completion of this proposal form does not bind the Applicant or the Insurer(s) to bind a contract of insurance. I agree that, if an insurance policy or policies are issued, this application and any other information supplied prior to inception of the insurance policy shall form the basis of any contract of insurance effective hereon and shall be incorporated therein. I hereby declare that I am authorized to complete this proposal on behalf of the Applicant and that the above statements and particulars are true and that full enquiry has been made to ensure their accuracy. I have not omitted, suppressed or misstated any material facts which may be relevant to underwriters' consideration of this proposal. I undertake to inform Insurer(s) of any material change to any fact contained herein that occurs prior to inception of the contract of insurance.

Business Risk Partners Ransomware Supplemental



| | |
|---------|--|
| Signed: | |
| Title: | |
| Date: | |