Putting risk in its place

BusinessRisk PARTNERS

Business Risk Partners Cyber Application

☐Please answer all questions within this application as fully as possible. If you would like to include any additional information, please provide by means of a separate attachment.

A. General Information	
Name of Applicant	
Address	
Date of Establishment	
Website	
Number of employees	
Please list subsidiaries	
Are there any plans to be involved in mergers and acquisitions in the next 12 months?	

B. Financial Information							
Currency							
Gross Annual Revenue							
Last completed financial year							
Current year (estimated)							
Next year (estimated)							
Revenue split by territory (%)	United States	EU	LATAM	Asia Pacific	Middle East	Australia	Other (please specify)
What percentage of revenue is derived from an ecommerce platform/online sales?							

C. Data Assessment		
1. Please confirm the total unique number of personally identifiable information you store, process or access		
2. Please identify the types of information you store, process or access and estimate the number of personally identifiable information for each:	Social security numbers:	
	Credit card information:	
	Driver's License numbers:	

Business Risk Partners Cyber Application

	Healthcare Information:		
	Financial information:		
	Other (please specify):		
3. Please confirm data is encrypted when:	At rest in the network	Yes ☐	No ☐
	In transit within and from your organization?	Yes ☐	No ☐
	On portable devices such as laptops, USB and mobile phones	Yes ☐	No ☐
4. Do you purge data in line with applicable regulations?		Yes ☐	No ☐
D. Network Security			
1. Do you employ a Chief Information/Security Officer who is responsible for network security and privacy?		Yes ☐	No ☐
2. a) Do you use MFA for any remote access to your systems (including Citrix desktop, or Remote Desktop Protocol "RDP?		Yes ☐	No ☐
b) If no, please comment on any mitigating controls:			
3. Do you use multi factor authentication to protect privileged user accounts?		Yes ☐	No ☐
4. a) Does your organization utilize Microsoft Office 365?		Yes ☐	No ☐
b) If so is the Advanced Threat Protection add-on utilized and MFA enforced for all users?		Yes ☐	No ☐
5. Have you implemented an Intrusion detection/prevention system which is updated and monitored regularly?		Yes ☐	No ☐
6. How often are intrusion logs reviewed?		Yes ☐	No ☐
7. a) Can your users access e-mail through a web app on a non-corporate device?		Yes ☐	No ☐
b) If Yes: do you enforce Multi-Factor Authentication (MFA)?		Yes ☐	No ☐

Putting risk in its place

BusinessRisk PARTNERS

Business Risk Partners Cyber Application

8. a) Is an e-mail filtering system (e.g. MailChimp, MimeCast or equivalent) in place that is activated for all email accounts?	Yes ☐	No ☐
b) If yes, please specify tools used:		
9. Do you employ any of the following solutions?		
SPF ☐	DKIM ☐	DMARC ☐
10. Do you have firewalls and automatically updating anti-virus software in force across your network?	Yes ☐	No ☐
11. In what time frame do you install critical and high severity patches across your enterprise?		
<1 day ☐	<1 week ☐	<1 month ☐	Other ☐
12. a) Are you using any unsupported software or operating systems?	Yes ☐	No ☐
b) If so how do you mitigate the risk of malware or ransomware infecting the network via unpatched vulnerabilities and please comment on timeframes for removing the legacy systems?		
13. a) Are all employees required to complete training on network security?	Yes ☐	No ☐
b) If so please confirm employee training is carried out at least annually and include social engineering/phishing	Yes ☐	No ☐
14. Do you have access control procedures and hard drive encryption to prevent unauthorized exposure of data on all laptops, PDAs, smartphones (e.g. BlackBerry), and home-based PCs?	Yes ☐	No ☐
15. Do you use a protective DNS service (e.g. Quad9, OpenDNS or the public sector PDNS)?	Yes ☐	No ☐
16. Do you use an endpoint protection product across your enterprise?	Yes ☐	No ☐
17. Do you use an endpoint application isolation and containment technology?	Yes ☐	No ☐
18. Do you utilize a SIEM monitored 24 x 7 by a SOC?	Yes ☐	No ☐

Business Risk Partners Cyber Application

19. Is the network physically or virtually segregated? Both ☐ Physically ☐ Virtually ☐ Neither ☐				
Please add any further comments applicable to this section here:				
E. Network Interruption				
1. Please provide details of the impact on your business should your networks be disrupted?				
2. Please describe any manual workarounds/continuity plans to mitigate any possible business interruption due to a cyber event				
3. Do you have a Business continuity plan that is tested at least annually?			Yes ☐	No ☐
4. Have you carried out a penetration test on your network?	Internal ☐		External ☐	Neither ☐
5. If so, have any critical recommendations yet to be implemented?			Yes ☐	No ☐
6. Do you have a hot site/alternative site for failover?			Yes ☐	No ☐
7. How often do you backup your data and systems?				
Real time ☐	Hourly ☐	Daily ☐	Weekly ☐	Other ☐
8. Are your backups encrypted?			Yes ☐	No ☐
9. Where are backups stored? Select all that apply				
Cloud ☐	On premises ☐	Offline storage ☐	Online storage ☐	Secondary data centre ☐
10. Do you use credentials unique to backups that are stored separately from user credentials?			Yes ☐	No ☐
11. What is your Recovery Time Objective (RTO) for critical systems?				
<4hrs ☐	<12hrs ☐	<24hrs ☐	<48hrs ☐	other ☐
12. Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware?			Yes ☐	No ☐
Please add any further comments to this section here:				

Business Risk Partners Cyber Application

F. Vendor Management

1. Please identify all critical vendors and the service they provide

Managed Security Services:		
Cloud / back up / Website hosting:		
Internet Service Providers:		
Business Critical Software Providers:		
Data Processors:		
POS hardware providers:		
Colocation Services:		

2. Do you audit vendors to ensure they meet your security standards?		
3. Are vendors contractually required to indemnify you if they contribute to a data breach or network disruption?		

4. How often are their contracts reviewed

Monthly ☐	Quarterly ☐	Annually ☐	Other ☐

5. Do you restrict vendors access to relevant data, systems and applications only to the role they are performing?	Yes ☐	No ☐

E. Multimedia (please skip to section G is coverage not required)

1. Do you have established procedures for editing, reviewing and removing content on your website prior to release?	Yes ☐	No ☐
1. Do you obtain legal reviews of all media and advertising prior to release?	Yes ☐	No ☐

2. Does the review include screening the content for the following:
   a. ☐disparagement issues?
   b. ☐copywriting infringement?
   c. ☐trademark infringement?
   d. ☐invasion of privacy?

3. Do you obtain content from third parties?	Yes ☐	No ☐
a. If so do you use legally reviewed contracts which include clauses to ensure that you are held harmless?	Yes ☐	No ☐

Please add any further applicable comments on this section here:

Business Risk Partners Cyber Application

G. Operational Technology (please skip to section H if not applicable)		
1. What percentage of the applicant's revenue derives from manufacturing or processing equipment controlled by operational technology?		
1. Is OT separated from IT in such a way that there is no direct connection from IT to OT such as RDP (used for remote administration) without additional (separate) authentication?	Yes ☐	No ☐
2. Is the OT at manufacturing sites separate from each other such that lateral movement between sites is not possible?	Yes ☐	No ☐
3. Are remote maintenance accesses restricted in rights and only opened when needed?	Yes ☐	No ☐
4. Is there malware protection / whitelisting on OT endpoints	Yes ☐	No ☐
5. Is critical data on OT backed up at least monthly?	Yes ☐	No ☐
6. Are default passwords in IoT devices changed?	Yes ☐	No ☐
7. Can the applicant's operational technology systems be controlled remotely via the internet, VPN, Bluetooth and/or a third party connection?	Yes ☐	No ☐
8. In event of an outage, please comment on the possibility to shift production to another factory:		
9. Are all factories able to operate independently? E.g. do any of the factories rely on one another or if there is an outage at one factory, would all other factories be able to operate?		
10. Are all products available for manufacture at multiple factories?		
11. Is there any scope for capacity to be increased to make up for lost production following an outage?		
12. If the corporate network suffers an outage, can factories continue to operate to the same level?		

Business Risk Partners Cyber Application

Please add any further applicable comments to this section here:						
H. Point of Sale systems (please skip to section I if not applicable)						
1. What is your revenue from sales using POS systems?						
2. What level of PCI merchant are you?	1☐	2☐	3☐	4☐	Not compliant ☐	
3. Are your systems EMV compliant?				Yes ☐	No ☐	
4. Is credit card data encrypted and tokenized at all times?				Yes ☐	No ☐	
5. If not, at what points are data unencrypted and how is this protected in its absence?						
6. Are POS terminals designed to be tamper-proof?				Yes ☐	No ☐	
7. Are vulnerability scans and penetration tests carried out on POS systems?				Yes ☐	No ☐	
8. If so, how often are these performed?						
9. If multi factor authentication used to access your POS network?				Yes ☐	No ☐	
10. Do you allow vendors to directly access your POS network?				Yes ☐	No ☐	
11. If so, what specific security controls are in place for vendor access?						
12. Are alerts from IDS/IPS or DLP for your POS network monitored 27/4?				Yes ☐	No ☐	
13. Is the POS network built on legacy or unsupported operating system?				Yes ☐	No ☐	
14. Is the network segregated to the extent that is one location suffered an outage, the others could continue to operate?				Yes ☐	No ☐	
Please add any further applicable comments to this section here:						
I. Claims						

Putting risk in its place

BusinessRisk PARTNERS

Business Risk Partners Cyber Application

1. Have any of the Applicant's owner, principals, directors, officers or employees ever been the subject of disciplinary or criminal actions as a result of their professional activities?	Yes ☐	No ☐
1. Have you had any claims or circumstances relating to your technology solutions, media, intellectual property rights or network security and privacy, which have or may have given rise to a claim under a previous policy, whether insured or otherwise, within the last 5 years?	Yes ☐	No ☐
2. Do you or any other person or organization proposed for this insurance have knowledge of any wrongful act, error, omission, security breach, privacy breach, privacy-related event or incident or allegations of breach of privacy that may give rise to a claim?	Yes ☐	No ☐
If Yes, please provide full details below including total costs and remedial actions have been carried out since the breach:		

C. 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.

Signed:	
Title:	
Date:	