COMMERCIAL INSURANCE

Mid-Market Cyber Insurance

RISKCAN
Underwriting Managers

Section A. CLIENT INFORMATION

Name: ____________________ Date Established: (DD/MM/YYYY): ____________________

Address: ____________________

Email address: ____________________ Website: ____________________

Phone: ____________________ Fax: ____________________

Section B. REVENUE

1. Please give the revenue generated from sales to the following:

   Canada: ____________ US: ____________ UK/EU: ____________

   Australia / New Zealand: ____________ Rest of World: ____________

2. What percentage of your revenue is delivered from on-line sales? ____________

3. If in excess of 25% please complete questions below.

   a. Do you (or your cloud provider) provide high availability for your transactional website and applications? ○ YES ○ NO

      If yes, please provide brief details.

      ____

   b. Do you deploy a Web Application Firewall? ○ YES ○ NO

      ‣ *Additional comments:*

      ____

      If yes, does the Web Application Firewall sit in front of the database, or network gateway, if more than one database is being protected? ○ YES ○ NO

      ‣ *Additional comments:*

      ____

   c. Total Number of employees including directors? ____________

Section C. RECORDS

1. Please give the total number of records for which you are legally liable:

   Payment Card Industry (credit or debit cards): ____________ Driving license, Tax or Social Security numbers: ____________

   Other Personal Data: ____________ Healthcare: ____________ Financial (not credit or debit cards): ____________

2. Do you adhere to the current legislation governing the handling of Personal Data in those territories in which you trade? ○ YES ○ NO

   ‣ *Additional comments:*

   ____

Section D. NETWORK SECURITY

1. Do you secure all remote access to your network and data with a minimum of two-factor authentication? ○ YES ○ NO

    ▸ *Additional comments:*

2. Do you run commercial grade antivirus and firewall protection across your entire network, including servers and all end points? ○ YES ○ NO

    ▸ *Additional comments:*

3. How often are virus signatures updated?

    ○ Automatically ○ Daily ○ Weekly ○ Other: ____________________

    ▸ *Additional comments:*

4. Do you run a Security Information and Event Management Application? ○ YES ○ NO

    If yes, is this monitored by a Security Operations Centre on a 24/7 basis? ○ YES ○ NO

    ▸ *Additional comments:*

5. Please provide details of all other network security applications running on your network and endpoints.

6. Have you disabled Remote Desktop Protocol on all of your endpoints, where applicable? ○ YES ○ NO

    ▸ *Additional comments:*

7. Do you allow remote access to your corporate network? ○ YES ○ NO

    If yes, is this protected by a minimum of two-factor authentication? ○ YES ○ NO

    ▸ *Additional comments:*

8. Do you encrypt all sensitive data (as defined in Section C above) whilst:

    □ In transit □ Stored on servers □ Stored on portable media

    ▸ *Additional comments:*

9. How often do you undertake an external security audit? ○ Annual ○ Never ○ Other: ____________________

    ▸ *Additional comments:*

10. Who has overall responsibility for network security? ____________________

11. How often do you apply critical patches?

○ Automatically ○ Daily ○ Weekly ○ Other: ______________________

▸ *Additional comments:*

12. Do you enforce a policy of auditing and managing computer and user accounts? ○ YES ○ NO

▸ *Additional comments:*

13. Do you enforce password changes at least every three months? ○ YES ○ NO

▸ *Additional comments:*

14. Is access to sensitive data restricted according to the employee's user requirements? ○ YES ○ NO

▸ *Additional comments:*

15. Do you automatically revoke all IT access for staff on leaving your employment? ○ YES ○ NO

▸ *Additional comments:*

16. How often is your information security policy reviewed? ○ Annual ○ Other: ______________________

▸ *Additional comments:*

Section E. PAYMENT CARD INDUSTRY COMPLIANCE

[**Note**: even if you completely outsource your entire card data processing to a validated third party, you may still need to be compliant with Payment Card Industry Data Security Standards (PCI DSS) rules and complete a Self-Assessment Questionnaire].

1. Are you in Compliance with the Payment Card Industry Data Security Standards? ○ YES ○ NO ○ N/A

▸ *Additional comments:*

2. What level of merchant? ○ 1 ○ 2 ○ 3 ○ 4

3. If you are a level 1 merchant, please advise below.

   a. Date of last PCI audit? (DD/MM/YYYY): ______________

   b. Were there any major non-compliance issues? ○ YES ○ NO ○ N/A

   ▸ *Additional comments:*

   If so, have these been rectified? ○ YES ○ NO ○ N/A

   ▸ *Additional comments:*

4. Are you EMV[1] (chip and pin) compliant? ○ YES ○ NO

▸ *Additional comments:*

5. Are you running Microsoft XP PoS Ready or any other unsupported application? ○ YES ○ NO

▸ *Additional comments:*

Section F. BUSINESS CONTINUITY

1. Are you ISO22301 certified? ○ YES ○ NO

▸ *Additional comments:*

2. Do you have a written business continuity plan that is reviewed annually? ○ YES ○ NO

▸ *Additional comments:*

3. Does your business continuity plan assess the risk from cyber perils? ○ YES ○ NO

▸ *Additional comments:*

4. Network Dependency - after how long will your business be impacted by an interruption to, or loss of, your network?

○ 6 hrs ○ 12 hrs ○ 24 hrs ○ 48 hrs

▸ *Additional comments:*

5. How long will it take to fully restore your critical systems? (Recovery Time Objective)

○ 6 hrs ○ 12 hrs ○ 24 hrs ○ 48 hrs

▸ *Additional comments:*

6. Do you test the Disaster Recovery Plan/ Business Continuity Plan annually? ○ YES ○ NO

▸ *Additional comments:*

7. Do you (or your cloud/outsource partner) configure your network to provide high availability or failover for your website and other critical applications and data? ○ YES ○ NO

▸ *Additional comments:*

8. Do you back up data that is necessary to run your business at least every 5 days? ○ YES ○ NO

▸ *Additional comments:*

9. Is your backed up data stored offline such that it is not accessible from your network? ○ YES ○ NO

Additional comments:

10. How often is back up data tested for integrity? ○ Weekly ○ Monthly ○ Other: __________

Additional comments:

Section G. EMAIL SECURITY

1. Do you use any of the following to authenticate your email:

□ SPF[2] □ DKIM[3]

If so, do you also use DMARC[4]? ○ YES ○ NO

Additional comments:

2. Do you use Office 365? ○ YES ○ NO

If so, have you deployed Advanced Threat Protection / Defender? ○ YES ○ NO

Additional comments:

3. Do you scan incoming email for malicious attachments or links? ○ YES ○ NO

Additional comments:

4. Do you provide training to assist employees in spotting phishing and other social engineering attacks? ○ YES ○ NO

If yes, how frequently? ○ Weekly ○ Monthly ○ Other: __________

Additional comments:

5. Do you undertake any phishing campaigns or training to advise employees of the risk of social engineering attacks? ○ YES ○ NO

If yes, how frequently? ○ Weekly ○ Monthly ○ Other: __________

Additional comments:

Section H. MANUFACTURING

(Please complete this section if you manufacture or assemble any products).

1. Do you run your CNC machinery on a Direct (or Distributed) Numerical Control basis (instructions are sent to machinery from a separate server)? ○ YES ○ NO

If yes, please provide details of the logical connections between your manufacturing environment and other applications (logistics/stock purchasing etc.):

2. Do you allow remote access to your manufacturing network? ○ YES ○ NO

   If yes, is this protected by a minimum of two-factor authentication? ○ YES ○ NO

   ▸ *Additional comments:*

3. Does your manufacturing network run within any unsupported operating systems (e.g. Windows XP, Windows 7, Windows Server 2008)? ○ YES ○ NO

   ▸ *Additional comments:*

4. What are the logical (network) connections between the manufacturing environment(s) and the corporate network? Please explain.

5. How quickly are critical patches applied within your manufacturing environment? Please explain.

6. Are any of your servers running manufacturing processes internet facing? ○ YES ○ NO

   ▸ *Additional comments:*

7. Do you employ application white-listing? ○ YES ○ NO

   ▸ *Additional comments:*

Section I. CLAIMS

1. Have you suffered any unplanned outage, not caused by a power failure, of more than 4 hours in the last 24 months that may have resulted in a claim under a cyber policy if one was in force? ○ YES ○ NO

   If yes, please provide details.

2. During the last 36 months has any sensitive or personal data for which you are legally liable been compromised or lost? ○ YES ○ NO

   If yes, please provide details.

Section J. DECLARATION

I declare that the statements and particulars in this application are true and that no material facts have been misstated or suppressed after enquiry. I agree that this application, together with any other information supplied shall form the basis of any contract of insurance affected thereon. I undertake to inform the Insurers of any material alteration to those facts occurring before completion of the contract of insurance. A material fact is one which would influence the acceptance or assessment of the risk.

The answers to these questions form part of an application for insurance only.

Nothing in this application shall be deemed an agreement to provide insurance and underwriters may decline to offer coverage or offer coverage on terms that differ from the coverage sought by the applicant.

The answers given in this application are correct to the best of my knowledge. I understand that these answers will form part of a policy that is subsequently offered. I also understand that any false statement may void the insurance in its entirety or result in a claim being denied.

Please confirm that you are prepared to receive electronic execution and delivery of the policy.

Please send the completed and signed form to your broker.

Print Name	Title/Position
Signature of Applicant	Date

Signing of this form does not bind the Applicant to complete the insurance.

ENDNOTES

1. Europay, MasterCard, and Visa; 2. Sender Policy Framework; 3. DomainKeys Identified Mail; 4. Domain-based Message Authentication, Reporting, and Conformance