COMMERCIAL INSURANCE

Small to Medium Enterprise Cyber Insurance

RISKCAN
Underwriting Managers

Cybercrime is real and it can impact your business. We're here to help you manage the risk of cyber attacks and completing this application form can help to ensure your business has the right insurance coverage in place.

This application form is ideal for small to medium enterprises with:

- Maximum revenues of $60M.
- 25% maximum US sales.
- Maximum $2M limit of insurance.
- Maximum 100,000 records of personal data on individuals.

For additional eligibility information, please speak to your broker.

Section A.

Name: ____________________

Address: ____________________

Website: ____________________ Date Established (DD/MM/YYYY): __________

Description of Operations:

____

If the following items are applicable to your operations AND your revenues exceed $30 Million ($10 million for technology, legal professionals, and manufacturing), please complete Section E - SUPPLEMENTAL INFORMATION:

- Education
- Legal Professionals
- Financial Institutions
- Healthcare Centres and Professions
- Manufacturing
- Power Generation and Utilities
- Wholesaling, Online Retail Seller, Transportation and Logistics
- T.V., Broadcasting, Publishing, Music, Creative Arts and Advertising
- Technology and Telecommunications

1. Total Annual Revenues ($): __________

   % derived from USA: ________ % derived from other countries: ________

   Additional comments: ____________________

2. Limit of Insurance required: □ $60,000 □ $100,000 □ $250,000 □ $500,000 □ $1,000,000
   □ $2,000,000 □ $5,000,000

   Bricking and Telephone Hacking ($50,000 is included): □ $100,000

Section B.

1. Do you deploy a business grade firewall at all external gateways of your network, as well as a business grade antivirus application across your entire network, including servers or endpoints? ○ YES ○ NO

   Additional comments: ____________________

2. Do you (or your cloud service provider) back up data that is necessary to run your business at least every 7 days? ○ YES ○ NO

   Additional comments: ____________________

3. Is this backed up data stored offline in an environment that is separate to your network and tested at least every 180 days for integrity? ○ YES ○ NO

   Additional comments: ____________________

If you answered 'no' to any of the questions above: All Risk-Can Cyber Insurance Policies includes access to *Avast Business CloudCare*, a Proactive Security Management tool available free of charge. Please talk to your broker for more information.

4. Do you install critical patches within 30 days of release? ○ YES ○ NO

   ▸ *Additional comments:* ____________________

5. Are you compliant with the Payment Card Industry (PCI) Data Security Standards, if applicable? ○ YES ○ NO

   ▸ *Additional comments:* ____________________

6. Have you suffered any loss or has any claim been made against you; or are you aware of any matter that is likely to give rise to any loss or claim where you would seek an indemnity from our cyber insurance policy? ○ YES ○ NO

   If yes, please provide the following details for each incident:

   a. What occurred? ____________________

   b. How long was the downtime? ____________________

   c. How much did it cost you? ____________________

   d. How has network security been improved since the attack? ____________________

7. Do you have secure remote access to your applications that are necessary to run your business with a minimum of multi-factor authentication? ○ YES ○ NO

   If no, please provide details of the critical applications that are remotely accessible that do not have secure connections and what you are doing to mitigate this exposure.

   ____

If total revenues exceed $30 million ($10 million for technology, legal professionals, and manufacturing), answer questions 8 to 12:

8. Have you disabled Remote Desktop Protocol (RDP) on all your network's endpoints, including servers, where RDP is not required? ○ YES ○ NO

   ▸ *Additional comments:* ____________________

9. Is all personal data encrypted while on, and in transmission from, your network? ○ YES ○ NO

   If no, please provide details of the personal data that is not encrypted and what you are doing to mitigate exposure.

   ____

10. Do you secure remote access to your network and personal data with a minimum of multi-factor authentication? ○ YES ○ NO

    If no, please provide details of your network's environments and personal data that is remotely accessible and without a secure connection. What are you doing to mitigate this exposure?

    ____

11. Have you deployed the following security protocols:

    a. Sender Policy Framework (SPF) ○ YES ○ NO

    b. Domain Keys Identified Mail (DKIM) across all your IT network devices? ○ YES ○ NO

    If yes, to either or both SPF and DKIM being deployed, have you also deployed the Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol across all your IT network devices? ○ YES ○ NO

    ▸ *Additional comments:*

    ____

12. Have you successfully tested the restoration of your business' critical applications (i.e. free from malware, and no delay / unexpected downtime) and recovery of key server configurations in the last 12 months? ○ YES ○ NO

    ▸ *Additional comments:*

    ____

Section C. FUNDS TRANSFER FRAUD (FTF) Coverage

FTF coverage provides protection in the event that a fraudulent change has been made to your bank account so that an e-transfer is redirected to a cyber criminal.

Please note that FTF coverage is not available for the following business operations:

- Accountant
- Fund Administrator
- Payroll Services
- Bank
- Gambling Establishments
- Stockbrokers
- Data Aggregator
- Hedge fund managers
- Trust Administration
- Data Analytics
- Investment Managers
- Venture Capitalists
- Finance Brokers
- Investment Trading Platforms
- Venture Capital Vehicles
- Foreign Exchange
- Mortgage Brokers
- Wealth Managers

If your business is not listed above and you would like to purchase FTF coverage, please complete the following questions.

1. Do you have a written procedure for validating all changes to vendor/client/customer contact details and bank account details in writing before the changes are actioned, including oral confirmation over the telephone? ○ YES ○ NO

   If yes, is that written procedure always followed? ○ YES ○ NO

   ▸ *Additional comments:*

2. Limit of insurance required[1]: □ $25,000 □ $50,000 □ $100,000

Section D. 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.

Signature of Applicant

Print Name

Date (dd/mm/yyyy)

Where applicable, please complete the supplemental information in Section E, then return this form to your broker.

Section E. SUPPLEMENTAL INFORMATION

Please complete the appropriate section applicable to your operations.

- Education **Pg. 4 →**
- Legal Professionals **Pg. 4 →**
- Financial Institutions **Pg. 5 →**
- Healthcare Centres and Professions **Pg. 5 →**
- Manufacturing **Pg. 6 →**
- Power Generation and Utilities **Pg. 7 →**
- Wholesaling, Online Retail Seller, Transportation and Logistics **Pg. 8 →**
- T.V., Broadcasting, Publishing, Music, Creative Arts and Advertising **Pg. 8 →**
- Technology and Telecommunications **Pg. 9 →**

Education

1. How many records of personal data on individuals (PCI, PII, PFI and / or PHI)[1] do you collect, store and process? ______________________

2. Is there a single policy governing all individual departments, run by one department / provider that controls network and data security? ○ YES ○ NO

   ▸ *Additional comments:* ______________________

3. Do you have contractual (indemnity) arrangements with any outsource or cloud providers (data controller) storing the personal data you store, collect and process in the event of a breach of privacy legislation by the data controller? ○ YES ○ NO

   If no, advise the number of records.

   ____

4. Is all personal data encrypted while in transit, backed up and at rest on your network? ○ YES ○ NO

   If no, provide details of type of data, number of records and where they are unencrypted.

   ____

5. Is your critical data backed up, stored offline in an environment which is separate to your network, and tested at least every 30 days for integrity? ○ YES ○ NO

   ▸ *Additional comments:* ______________________

6. Do you comply with the current national and international legislation governing the handling of personal data (e.g. GDPR, APP, HIPAA) applicable to your business? ○ YES ○ NO

Legal Professionals

1. How many records of personal data on individuals (PCI, PII, PFI and / or PHI)[1] do you collect, store and process? ______________________

2. Do you have contractual (indemnity) arrangements with any outsource or cloud providers (data controller) storing the personal data you store, collect and process in the event of a breach of privacy legislation by the data controller? ○ YES ○ NO

   If no, advise the number and type of records.

   ____

3. Is your critical data backed up, stored offline in an environment that is separate to your network, and tested at least every 30 days for integrity? ○ YES ○ NO

   ▸ *Additional comments:* ______________________

4. Is all personal data encrypted while in transit, backed up and at rest on the network? ○ YES ○ NO

   If no, provide details of type of data, number of records and where they are unencrypted.

   ____

5. Do you comply with the current national and international legislation governing the handling of personal data (e.g. GDPR, APP, HIPAA) applicable to your business? ○ YES ○ NO

   ▸ *Additional comments:* ______________________

Financial Institutions

1. How many records of personal data on individuals (PCI, PII, PFI and / or PHI)[1] do you collect, store and process? __________
2. Do you have contractual (indemnity) arrangements with any outsource or cloud providers (data controller) storing the personal data you store, collect and process in the event of a breach of privacy legislation by the data controller? ○ YES ○ NO

   If no, advise the number and type of records.

   ____
3. Is all personal data encrypted while in transit, backed up and at rest on the network? ○ YES ○ NO

   If no, provide details of type of data, number of records and where they are unencrypted.

   ____
4. Do you comply with the current national and international legislation governing the handling of personal data (e.g. GDPR, APP) applicable to your business? ○ YES ○ NO

   ▸ *Additional comments:* __________
5. Is your critical data backed up, stored offline in an environment that is separate to your network, and tested at least every 30 days for integrity? ○ YES ○ NO

   ▸ *Additional comments:* __________
6. Do you configure your network to provide high availability or failover for your website, critical applications and data you access / rely on to reduce any potential business interruption / downtime? ○ YES ○ NO

   ▸ *Additional comments:* __________

Healthcare Centres and Professions

1. How many records of personal data on individuals (PCI, PII, PFI and / or PHI)[1] do you collect, store and process? __________
2. Do you have contractual (indemnity) arrangements with any outsource or cloud providers (data controller) storing the personal data you store, collect and process in the event of a breach of privacy legislation by the data controller? ○ YES ○ NO

   If no, advise the number and type of records.

   ____
3. Is all personal data encrypted while in transit, backed up and at rest on the network? ○ YES ○ NO

   If no, provide details of type of data, number of records and where they are unencrypted.

   ____
4. Is your critical data backed up, stored offline in an environment that is separate to your network, and tested at least every 30 days for integrity? ○ YES ○ NO

   ▸ *Additional comments:* __________
5. Do you comply with the current national and international legislation governing the handling of personal data (e.g. GDPR, APP, HIPAA) applicable to your business? ○ YES ○ NO

   ▸ *Additional comments:* __________

Manufacturing

1. Network Dependency – after how long will your business suffer financial impact by a loss to your network?

   □ 6 hours □ 12 hours □ 24 hours □ 48 hours □ More than 48 hours

   ▸ *Additional comments:*

2. How long will it take to fully restore your critical systems?

   □ 6 hours □ 12 hours □ 24 hours □ 48 hours □ More than 48 hours

   ▸ *Additional comments:*

3. What are your recovery time objectives for fully restoring your critical systems?

   □ 6 hours □ 12 hours □ 24 hours □ 48 hours □ More than 48 hours

   ▸ *Additional comments:*

4. Do you run your CNC machinery on a Direct Numerical Control basis? ○ YES ○ NO

   If yes, please answer the questions below.

   a. Are the logical connections between your manufacturing environment and other applications (logistics/stock purchasing etc.) fully separated? ○ YES ○ NO

   Please provide details of the logical connections between your manufacturing environment and other applications (logistics/stock purchasing etc.).

   b. Does your manufacturing network run within any unsupported operating systems (e.g. Windows XP)? ○ YES ○ NO

   ▸ *Additional comments:*

   c. If you are operating on unsupported platforms, are these applications completely isolated from other platforms (e.g. air-gapped)? ○ YES ○ NO

   ▸ *Additional comments:*

   d. Are critical patches applied within 30 days in your manufacturing environment? ○ YES ○ NO

   ▸ *Additional comments:*

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

   ▸ *Additional comments:*

   f. Are any of these servers managed by a supplier? ○ YES ○ NO

   Does any supplier have a direct access to any of these servers? ○ YES ○ NO

   If yes, does that supplier have a direct access to any of these servers? ○ YES ○ NO

   If yes, have you deployed secure remote access with multi-factor authentication that times out the connection in no less than 24 hours? ○ YES ○ NO

   ▸ *Additional comments:*

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

   ▸ *Additional comments:*

   h. Do you allow remote access to your manufacturing network only via multi-factor authentication? ○ YES ○ NO

   ▸ *Additional comments:*

Power Generation and Utilities

1. Are the logical connections between your manufacturing environment and other applications (logistics/stock purchasing etc.) fully separated? ○ YES ○ NO

   Please provide details of the logical connections between your manufacturing environment and other applications (logistics/stock purchasing etc.)

2. Does your manufacturing network run within any unsupported operating systems (e.g. Windows XP)? ○ YES ○ NO

   a. If you are operating on unsupported platforms, are these applications completely isolated from other platforms (e.g. air-gapped)? ○ YES ○ NO

   ▸ Additional comments:

3. Are critical patches applied within 30 days in your manufacturing environment? ○ YES ○ NO

   ▸ *Additional comments:*

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

   ▸ *Additional comments:*

5. Are any of these servers managed by a supplier? ○ YES ○ NO

   If yes, does that supplier have a direct access to any of these servers? ○ YES ○ NO

   If yes, have you deployed secure remote access with multi-factor authentication that times out the connection no less than 24 hours? ○ YES ○ NO

   ▸ *Additional comments:*

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

   ▸ *Additional comments:*

7. Do you allow remote access to your manufacturing network only via multi-factor authentication? ○ YES ○ NO

   ▸ *Additional comments:*

8. Network Dependency – after how long will your business suffer financial impact by a loss to your network?

   □ 6 hours □ 12 hours □ 24 hours □ 48 hours □ More than 48 hours

   ▸ *Additional comments:*

9. How long will it take to fully restore your critical systems?

   □ 6 hours □ 12 hours □ 24 hours □ 48 hours □ More than 48 hours

   ▸ *Additional comments:*

10. What are your recovery time objectives for fully restoring your critical systems?

   □ 6 hours □ 12 hours □ 24 hours □ 48 hours □ More than 48 hours

   ▸ *Additional comments:*

Wholesaling, Online Retail Seller, Transportation and Logistics

1. What percentage of your revenue is delivered from online sales? (if +25%, complete the Mid-Market Application)

2. Do you have a business continuity plan that has a cyber-attack response procedure? ○ YES ○ NO

   ▸ *Additional comments:*

3. Do you test this business continuity plan annually? ○ YES ○ NO

   ▸ *Additional comments:*

4. Network Dependency – after how long will your business suffer financial impact by a loss to your network?

   □ 6 hours □ 12 hours □ 24 hours □ 48 hours □ More than 48 hours

   ▸ *Additional comments:*

5. How long will it take to fully restore your critical systems?

   □ 6 hours □ 12 hours □ 24 hours □ 48 hours □ More than 48 hours

   ▸ *Additional comments:*

6. What are your recovery time objectives for fully restoring your critical systems?

   □ 6 hours □ 12 hours □ 24 hours □ 48 hours □ More than 48 hours

   ▸ *Additional comments:*

7. Do you (or your cloud service provider) configure your network to provide high availability or failover for your website and other critical applications? ○ 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:*

T.V., Broadcasting, Publishing, Music, Creative Arts and Advertising

1. How many records of personal data on individuals (PCI, PII, PFI and / or PHI)[1] do you collect, store and process?

2. Do you have contractual (indemnity) arrangements with any outsource or cloud providers (data controller) storing the personal data you store, collect and process in the event of a breach of privacy legislation by the data controller? ○ YES ○ NO

   If no, advise the number and type of records.

3. Is all personal data encrypted while in transit, backed up and at rest on the network? ○ YES ○ NO

   If no, provide details of type of data, number of records and where they are unencrypted.

4. Is your critical data backed up, stored offline in an environment that is separate to your network, and tested at least every 30 days for integrity? ○ YES ○ NO

   ▸ *Additional comments:*

5. Do you comply with the current national and international legislation governing the handling of personal data (e.g. GDPR, APP, HIPAA) applicable to your business? ○ YES ○ NO

   ▸ *Additional comments:*

6. Do you configure your network to provide high availability or failover for your website, critical applications, and data you access / rely on to reduce any potential business interruption / downtime? ○ YES ○ NO

   ▸ *Additional comments:*

Technology and Telecommunications

1. How many records of personal data on individuals (PCI, PII, PFI and / or PHI)[2] do you collect, store and process? ____________

2. Is all personal data encrypted while in transit, backed up and at rest on the network? ○ YES ○ NO

   If no, provide details of type of data, number of records and where they are unencrypted.

   ____

3. Is your critical data backed up, stored offline in an environment that is separate to your network, and tested at least every 30 days for integrity? ○ YES ○ NO

   ▸ *Additional comments:* ____________

4. Do you comply with the current national and international legislation governing the handling of personal data (e.g. GDPR, APP, HIPAA) applicable to your business? ○ YES ○ NO

   ▸ *Additional comments:* ____________

5. Do you configure your network to provide high availability or failover for your website, critical applications, and data you access / rely on to reduce any potential business interruption / downtime? ○ YES ○ NO

   ▸ *Additional comments:* ____________

6. Are administrative privileges restricted to specific users on your computer network and only accessed by multi-factor authentication? ○ YES ○ NO

   ▸ *Additional comments:* ____________

7. Have you successfully tested the restoration of your business' critical applications (i.e. free from malware, and no delay / unexpected downtime) and recovery of key server configurations in the last 6 months? ○ YES ○ NO

8. Do you have contractual (indemnity) arrangements as an outsource / cloud provider / data processor with your customers for storing their personal data in the event of a breach of privacy legislation by you? ○ YES ○ NO

   If yes:

   a. How much is the value range of the indemnity offered per client? ____________

   b. How many clients have an indemnity been issued to? ____________

   c. What is the average indemnity issued to a client? ____________

   ▸ *Additional comments:* ____________

ENDNOTES

[1] FTF limit cannot be more than 1/5 of the selected limit of liability, with exception for limit of liability of $100,000 or less. Max FTF limit available is $25,000.

[2] PCI: Payment Card Industry; PII: Personally-Identifying Information; PFI: Personal Financial Identity; PHI: Protected Health Information