Background and Financial Information

5. Nature of business _____

6. Year Business Started _____

7. Total Number of Employees *(please include all full, part, time seasonal, leased, etc.)* _____

8. Please provide the following financial information:

Total Assets as of Most Recent Fiscal Year End	Total Gross Revenues Last Fiscal Year	Anticipated Revenues This Fiscal Year	Anticipated Revenues Next Fiscal Year
$	$	$	$

9. Percentage of Annual Revenues Estimated to be attributable to E-Commerce/Online Sales _____ %

[5] What does the insured do (see product guide for classifications)

[8] Estimated figures are acceptable

[9] This includes any products that can be purchased online (e.g. items purchased through the Insured's website or online storefronts such as amazon, etsy, ebay

Supplemental Questions

	Yes	No
13. Do you provide any kind of professional data hosting or processing and/or any kind of IT hardware or software support to others?	☐	☐

14. Indicate which of the following controls you have implemented with respect to electronic funds transfers:
- ☐ Callback procedures to verify funds transfer requests or changes to banking information
- ☐ Dual authorization for funds transfers greater than $2,500
- ☐ Other *(please describe)* _____

15. What percent of your employees handle Company business from their personal devices *(select one)*?
- ☐ We prohibit it
- ☐ I don't know
- ☐ Less than 25%
- ☐ 25 – 75%
- ☐ More than 75%

[13] Includes website hosting/creation, tech support, software development, web content, etc.

[14] Call back procedure requires the business to verify transfer requests or changes to payment information with the vendor
Dual authorization requires the approval of two company personnel.

[15] This does not include company issued devices (purchased by the company), only pertains to employee's personally owned devices

16. a. Please estimate the annual volume of each type of information you process or store, taking into account both electronic and paper files as well as employee and customer information:
- ☐ SSN, individual taxpayer ID, driver's license, passport or federal ID numbers _____
- ☐ Payment card data *(credit or debit cards)* _____
- ☐ Protected health information _____
- ☐ Other confidential or protected information _____

b. How long do you store the above records? _____

	Yes	No
c. Do you have a record retention/destruction policy in place?	☐	☐

[16] Provide yearly totals (dollar amounts & percentages are not acceptable) Please include totals of PII that are both **processed and maintained** *(credit card transactions are considered a part of this)*
This includes but is not limited to credit/debit card and personal information input into 3rd party sites such as square, other digital readers, POS system, franchisor systems, etc.

17. Which of the following are part of the Company's privacy and network security programs *(select all that apply)*?
- ☐ Physical controls on access to computer systems and sensitive documents
- ☐ Password protection on company devices
- ☐ Employee security awareness training
- ☐ Documented regulatory compliance programs *(i.e. HIPAA and GLBA compliance)*
- ☐ Multi-Factor Authentication for remote access to email and both internal and external systems
- ☐ Up-to-date, active firewall and anti-virus software

[17] Physical controls – not accessible to the public (files and computers stored in locked locations)

Multi-factor requires at least **2** types of verification (e.g. password, text, email, call)

18. The Company backs up its primary mission critical systems and data assets: **Yes** **No**

- At least daily/nightly ☐ ☐
  If no, indicate how often _____
- Remotely and securely ☐ ☐
  If no, please provide business continuity plan.

[18] Please answer **ALL** fields of this question (nightly is required to get maximum Ransomware coverage limit)

A business's Mission Critical Data is any information that is imperative to the business's day to day operations

Remotely & securely requires offsite storage, can include cloud storage, servers, external hard drives, etc.

19. Are you compliant with the Payment Card Industry Data Security Standard (PCI-DSS) *(select one)*?

☐ Yes ☐ No
☐ I don't know ☐ We do not process ANY payment card transactions

	Yes	No
20. Does the Company maintain a formal program for evaluating the security posture of its vendors?	☐	☐

21. The Company's policy regarding the encryption of confidential data *(including but not limited to PII)* is that such data should be Encrypted *(select one)*:

- ☐ Never/we do not encrypt
- ☐ Within our network only
- ☐ Within our network and within the cloud
- ☐ Within our network, and the cloud, and on mobile devices *(i.e. smartphones)*
- ☐ Within our networks, the cloud, mobile devices, and removable/transportable storage media *(i.e. USB drives)*

[20] Do you require a review of your vendor's security protocols?

[21] Definition of encryption, the process of converting information or data into a code, especially to prevent unauthorized access.

"I use encryption to protect sensitive information transmitted online"

22. Who monitors the Company's networks for intrusions or other unusual activity *(select one)*?

- ☐ Nobody/we do not monitor
- ☐ Somebody in the Company's IT department
- ☐ A third party/managed security provider
- ☐ Somebody in the Company's IT department AND a third party/managed security provider

23. When did the Company last have a comprehensive *(i.e. inclusive of vulnerability scanning and penetration testing)* network security assessment conducted by a third party *(select one)*?

☐ Last 6 months ☐ Last 18 months ☐ Last 36 months ☐ Never

24. The Company's attempts to mitigate its exposure to media liability by using the following controls *(select all that apply)*:

- ☐ Obtaining all necessary rights to use third party content
- ☐ Social media policy
- ☐ Take-down procedures
- ☐ Legal review of all materials

[22] Computer antivirus software does not fulfill this requirement, must be a person or company.