beazley

BEAZLEY BREACH RESPONSE APPLICATION

NOTICE: THIS POLICY'S LIABILITY INSURING AGREEMENTS PROVIDE COVERAGE ON A CLAIMS MADE AND REPORTED BASIS AND APPLY ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR THE OPTIONAL EXTENSION PERIOD (IF APPLICABLE) AND REPORTED TO THE UNDERWRITERS IN ACCORDANCE WITH THE TERMS THIS POLICY. AMOUNTS INCURRED AS CLAIMS EXPENSES UNDER THIS POLICY WILL REDUCE AND MAY EXHAUST THE LIMIT OF LIABILITY AND ARE SUBJECT TO RETENTIONS.

PLEASE READ THIS POLICY CAREFULLY.

Please fully answer all questions and submit all requested information.

GENERAL INFORMATION:

Full Name:			
Mailing Address:		State of Incorporation:	
City:		State & Zip:	
# of Employees:		Date Established:	
Website URL's:			
Authorized Officer [1]:		Telephone: E-mail:	
Breach Response Contact [2]:		Telephone: E-mail:	
Business Description:			
Does the Applicant provide data processing, storage or hosting services to third parties?		☐ Yes ☐ No	

REVENUE INFORMATION:

*For Applicants in Healthcare: Net Patient Services Revenue plus Other Operating Revenue

*For all other Applicants, please provide Gross Revenue information

	Most Recent Twelve (12) months: ending:_____	Previous Year	Next Year (estimate)
US Revenue:	USD	USD	USD
Non-US Revenue:	USD	USD	USD
Total:	USD	USD	USD

Please attach a copy of your most recently audited annual financial statement.

[1] This is the officer of the Applicant that is authorized make statements to the Underwriters on the Applicant's behalf and to receive notices from the Insurer or its authorized representative(s).

[2] This is the employee of the Applicant that is designated to work with the insurer in response to a data breach event.

What percentage of the Applicant's revenues is business to business? _____% Direct to consumer?	_____%
Are significant changes in the nature or size of the Applicant's business anticipated over the next twelve (12) months? Or have there been any such changes within the past twelve (12) months?	☐ Yes ☐ No
If 'Yes', please explain:	
Has the Applicant within the past twelve (12) months completed or agreed to, or does it contemplate entering into within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed?	☐ Yes ☐ No
If 'Yes', please explain:	

PRIVACY

Please identify the types of personal information of individuals that you collect, process or store (check all that apply) along with an estimate of the number of records held for each type of information:

Type of Information	Number of Records (Estimated)
☐ Social Security Numbers	☐ <100K; ☐ 100K-500K; ☐ 500K-1M; ☐ 1M-2M; ☐ 2M-5M; ☐ >5M
☐ Consumer Financial Information	☐ <100K; ☐ 100K-500K; ☐ 500K-1M; ☐ 1M-2M; ☐ 2M-5M; ☐ >5M
☐ Payment Card Information	☐ <100K; ☐ 100K-500K; ☐ 500K-1M; ☐ 1M-2M; ☐ 2M-5M; ☐ >5M
☐ Protected Health Information	☐ <100K; ☐ 100K-500K; ☐ 500K-1M; ☐ 1M-2M; ☐ 2M-5M; ☐ >5M
☐ Biometric Information	☐ <100K; ☐ 100K-500K; ☐ 500K-1M; ☐ 1M-2M; ☐ 2M-5M; ☐ >5M

☐ Other (please describe):

Has the Applicant designated a Chief Privacy Officer?	☐ Yes ☐ No
If 'No' please indicate what position(s) (if any) are responsible for privacy issues:	
Does the Applicant require third parties with which it shares personally identifiable or confidential information to indemnify the Applicant for legal liability arising out of the release of such information due to the fault or negligence of the third party?	☐ Yes ☐ No

PAYMENT CARDS

Does the Applicant accept payment cards for goods sold or services rendered?	☐ Yes ☐ No
If 'Yes': How many payment card transactions does the Applicant transact per year?	
Is the Applicant compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g. PCI standards)?	☐ Yes ☐ No
Is payment card data encrypted at the point of sale (e.g., payment card reader or e-commerce payment portal) through transmission to the payment processor?	☐ Yes ☐ No
If the Applicant is not compliant with applicable data security standards, please describe the current status of any compliance work and the estimated date of completion: _____	

COMPUTER & NETWORK SECURITY

Has the Applicant designated a Chief Information Security Officer as respects computer systems and data security?	☐ Yes ☐ No

If 'No', please indicate what position is responsible for computer and data security: _____

Does the Applicant publish and distribute written policies and procedures regarding computer and information security to its employees?	☐ Yes ☐ No
Does the Applicant conduct computer and information security training for every employee that has access to computer systems or sensitive data?	☐ Yes ☐ No
Does the Applicant enforce a process for the timely installation of software updates/patches?	☐ Yes ☐ No
If 'Yes', are critical updates/patches installed within thirty (30) days of release?	☐ Yes ☐ No
Does the Applicant restrict user rights on computer systems such that individuals (including third party service providers) have access only to those areas of the network or information that is necessary for them to perform their duties?	☐ Yes ☐ No
Where does the Applicant have a firewall? (check all that apply)	

☐ At network perimeter ☐ Internally within the network to protect sensitive resources

Which of the following procedures does the Applicant employ to test computer security controls?

Testing	Frequency of Testing
☐ Internal Vulnerability Scanning	☐ Continuously ☐ Monthly ☐ Quarterly
☐ External Vulnerability Scanning against internet-facing IP addresses	☐ Continuously ☐ Monthly ☐ Quarterly
☐ Penetration Testing	☐ Quarterly ☐ Semi-annually ☐ Annually

☐ Other (please describe):

Does the Applicant have network intrusion detection systems that provide actionable alerts if an unauthorized computer system intrusion occurs?	☐ Yes ☐ No

If 'Yes', please describe:

Does the Applicant store data in any of the following environments, and is such stored data encrypted? (check all that apply)

☐ Laptops	☐ Encrypted ☐ Not Encrypted
☐ Portable Media	☐ Encrypted ☐ Not Encrypted
☐ Back-up Tapes	☐ Encrypted ☐ Not Encrypted
☐ "at rest" within computer databases	☐ Encrypted ☐ Not Encrypted

Does the Applicant outsource any of the following? (Check all that apply and please identify the vendor(s)

☐ Data Center Hosting:	☐ Managed Security:	☐ Alert Log Monitoring:

BUSINESS CONTINUITY

Does the Applicant have : A. a disaster recovery plan? B. a business continuity plan? C. an incident response plan for network intrusions and virus incidents?	☐ Yes ☐ No Date last tested: ☐ Yes ☐ No Date last tested: ☐ Yes ☐ No Date last tested:
If the Applicant has a business continuity plan, does the plan contain recovery time objectives for the amount of time within which business processes and continuity must be restored? If 'Yes', what are the current stated and tested recovery time objectives?	☐ Yes ☐ No

Does the Applicant have centralized log collection and management that allows for review of all access and activity on the network? For how long are logs maintained? _____	☐ Yes ☐ No

What is Applicant's process for backing up data? (check all that apply)

☐ Full backup ☐ Incremental ☐ Differential ☐ Mirror ☐ Other:

How often is Applicant's data backed up? _____

Where are data backups stored? (check all that apply) ☐ Secure offsite ☐ Secondary Data Center ☐ Other:

If necessary, how quickly can backed up data be accessed and restored? _____

MEDIA LIABILITY

Please describe the media activities of the Applicant or by others on behalf of the Applicant

☐ Television ☐ Radio ☐ Print ☐ Applicant's Website(s) ☐ Internet Advertising ☐ Social Media ☐ Marketing Materials ☐ Audio or Video Streaming

☐ Other (please describe: _____

Does the Applicant have a formal review process in place to screen any published or broadcast material (including digital content), for intellectual property and privacy compliance prior to any publication, broadcast, distribution or use?	☐ Yes ☐ No ☐ N/A
Are such reviews conducted by, or under the supervision, of a qualified attorney?	☐ Yes ☐ No ☐ N/A
Does the Applicant allow user generated content to be displayed on its website(s)?	☐ Yes ☐ No ☐ N/A

E-CRIME

Are all employees that are responsible for disbursing or transmitting funds provided anti-fraud training, including detection of social engineering, phishing, business email compromise, and other scams on at least an annual basis?	☐ Yes ☐ No
Before processing fund transfer requests from internal sources, does the Applicant confirm the instructions via a method other than the original means of the instruction?	☐ Yes ☐ No
Do the Applicant's procedures require review of all requests by a supervisor or next-level approver before processing fund transfer instructions?	☐ Yes ☐ No
When a vendor/supplier requests any change to its account details (including routing numbers, account numbers, telephone numbers and contact information) and prior to making any changes:	☐ Yes ☐ No
Does the Applicant first confirm all requested changes requested by the vendor/supplier with a person other than the requestor prior to making any changes?	☐ Yes ☐ No
Does the Applicant confirm requested changes via a method other than the original means of request?	☐ Yes ☐ No
Do the Applicant's processes and procedures require review of all requests by a supervisor or next-level approver?	☐ Yes ☐ No

Please identify your telecommunications carrier:	
Have you established strong alphanumeric passwords for administrative controls of your telecommunications system?	☐ Yes ☐ No
Have you configured your telecommunications system to disable (check all that apply): ☐ Remote system administration and Internet Protocol (IP) access ☐ Dialing via remote system access (DISA)	

PRIOR CLAIMS AND CIRCUMSTANCES

Does the Applicant or other proposed insured (including any director, officer or employee) have knowledge of or information regarding any fact, circumstance, situation, event or transaction which may give rise to a claim, loss or obligation to provide breach notification under the proposed insurance? If yes, please provide details:	☐ Yes ☐ No
During the past five (5) years has the Applicant: a. received any claims or complaints with respect to privacy, breach of information or network security, or, unauthorized disclosure of information?	☐ Yes ☐ No
b. been subject to any government action, investigation or subpoena regarding any alleged violation of a privacy law or regulation?	☐ Yes ☐ No
c. received a complaint or cease and desist demand alleging trademark, copyright, invasion of privacy, or defamation with regard to any content published, displayed or distributed by or on behalf of the Applicant?	☐ Yes ☐ No
d. notified consumers or any other third party of a data breach incident involving the Applicant?	☐ Yes ☐ No
e. experienced an actual or attempted extortion demand with respect to its computer systems?	☐ Yes ☐ No
f. experienced an unexpected outage of a computer network, application or system lasting greater than four (4) hours?	☐ Yes ☐ No
If 'Yes' to any of the above, please provide details regarding such incident(s) or event(s):	

THE UNDERSIGNED IS AUTHORIZED BY THE APPLICANT TO SIGN THIS APPLICATION ON THE APPLICANT'S BEHALF AND DECLARES THAT THE STATEMENTS CONTAINED IN THE INFORMATION AND MATERIALS PROVIDED TO THE INSURER IN CONJUNCTION WITH THIS APPLICATION AND THE UNDEWRITING OF THIS INSURANCE ARE TRUE, ACCURATE AND NOT MISLEADING. SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE INSURER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THE STATEMENTS CONTAINED IN THIS APPLICATION AND ANY OTHER INFORMATION AND MATERIALS SUBMITTED TO THE INSURER IN CONNECTION WITH THE UNDERWRITING OF THIS INSURANCE ARE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED, AND HAVE BEEN RELIED UPON BY THE INSURER IN ISSUING ANY POLICY.

THIS APPLICATION AND ALL INFORMATION AND MATERIALS SUBMITTED WITH IT SHALL BE RETAINED ON FILE WITH THE INSURER AND SHALL BE DEEMED ATTACHED TO AND BECOME PART OF THE POLICY IF ISSUED. THE INSURER IS AUTHORIZED TO MAKE ANY INVESTIGATION AND INQUIRY AS IT DEEMS NECESSARY REGARDING THE INFORMATION AND MATERIALS PROVIDED TO THE INSURER IN CONNECTION WITH THE UNDERWRITING AND ISSUANCE OF THE POLICY.

THE APPLICANT AGREES THAT IF THE INFORMATION PROVIDED IN THIS APPLICATION OR IN CONNECTION WITH THE UNDERWRITING OF THE POLICY CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE

EFFECTIVE DATE OF THE INSURANCE, THE APPLICANT WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE INSURER OF SUCH CHANGES, AND THE INSURER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE.

I HAVE READ THE FOREGOING APPLICATION FOR INSURANCE AND REPRESENT THAT THE RESPONSES PROVIDED ON BEHALF OF THE APPLICANT ARE TRUE AND CORRECT.

FRAUD WARNING DISCLOSURE

ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT (S)HE IS FACILITATING A FRAUD AGAINST THE INSURER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT MAY BE GUILTY OF INSURANCE FRAUD.

NOTICE TO ALABAMA, ARKANSAS, LOUISIANA, NEW MEXICO AND RHODE ISLAND APPLICANTS: ANY PERSON WHO KNOWINGLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR KNOWINGLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON.

NOTICE TO COLORADO APPLICANTS: IT IS UNLAWFUL TO KNOWINGLY PROVIDE FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES, DENIAL OF INSURANCE, AND CIVIL DAMAGES. ANY INSURANCE COMPANY OR AGENT OF AN INSURANCE COMPANY WHO KNOWINGLY PROVIDES FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO A POLICYHOLDER OR CLAIMANT FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE POLICYHOLDER OR CLAIMANT WITH REGARD TO A SETTLEMENT OR AWARD PAYABLE FROM INSURANCE PROCEEDS SHALL BE REPORTED TO THE COLORADO DIVISION OF INSURANCE WITHIN THE DEPARTMENT OF REGULATORY AGENCIES.

NOTICE TO DISTRICT OF COLUMBIA APPLICANTS: WARNING: IT IS A CRIME TO PROVIDE FALSE OR MISLEADING INFORMATION TO AN INSURER FOR THE PURPOSE OF DEFRAUDING THE INSURER OR ANY OTHER PERSON. PENALTIES INCLUDE IMPRISONMENT AND/OR FINES. IN ADDITION, AN INSURER MAY DENY INSURANCE BENEFITS IF FALSE INFORMATION MATERIALLY RELATED TO A CLAIM WAS PROVIDED BY THE APPLICANT.

NOTICE TO FLORIDA APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO INJURE, DEFRAUD, OR DECEIVE ANY INSURER FILES A STATEMENT OF CLAIM OR AN APPLICATION CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY IN THE THIRD DEGREE.

NOTICE TO KANSAS APPLICANTS: ANY PERSON WHO, KNOWINGLY AND WITH INTENT TO DEFRAUD, PRESENTS, CAUSES TO BE PRESENTED OR PREPARES WITH KNOWLEDGE OR BELIEF THAT IT WILL BE PRESENTED TO OR BY AN INSURER, PURPORTED INSURER, BROKER OR AGENT THEREOF, ANY WRITTEN, ELECTRONIC, ELECTRONIC IMPULSE, FACSIMILE, MAGNETIC, ORAL, OR TELEPHONIC COMMUNICATION OR STATEMENT AS PART OF, OR IN SUPPORT OF, AN APPLICATION FOR THE ISSUANCE OF, OR THE RATING OF AN INSURANCE POLICY FOR PERSONAL OR COMMERCIAL INSURANCE, OR A CLAIM FOR PAYMENT OR OTHER BENEFIT PURSUANT TO AN INSURANCE POLICY FOR COMMERCIAL OR PERSONAL INSURANCE WHICH SUCH PERSON KNOWS TO CONTAIN MATERIALLY FALSE INFORMATION CONCERNING ANY FACT MATERIAL THERETO; OR CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO COMMITS A FRAUDULENT INSURANCE ACT.

NOTICE TO KENTUCKY, NEW JERSEY, NEW YORK, OHIO AND PENNSYLVANIA APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIMS CONTAINING ANY MATERIALLY FALSE INFORMATION OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME, AND SUBJECTS SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES. (IN NEW YORK, THE CIVIL PENALTY IS NOT TO EXCEED FIVE THOUSAND DOLLARS ($5,000) AND THE STATED VALUE OF THE CLAIM FOR EACH SUCH VIOLATION.)

NOTICE TO MAINE, TENNESSEE, VIRGINIA AND WASHINGTON APPLICANTS: IT IS A CRIME TO KNOWINGLY PROVIDE FALSE, INCOMPLETE OR MISLEADING INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES OR A DENIAL OF INSURANCE BENEFITS.

NOTICE TO MARYLAND APPLICANTS: ANY PERSON WHO KNOWINGLY OR WILLFULLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR KNOWINGLY OR WILLFULLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON.

NOTICE TO OKLAHOMA APPLICANTS: WARNING**:** ANY PERSON WHO KNOWINGLY, AND WITH INTENT TO INJURE, DEFRAUD OR DECEIVE ANY INSURER, MAKES ANY CLAIM FOR THE PROCEEDS OF AN INSURANCE POLICY CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY.

SIGNATURE SECTION

THE UNDERSIGNED AUTHORIZED EMPLOYEE OF THE APPLICANT DECLARES THAT THE STATEMENTS SET FORTH HEREIN ARE TRUE. THE UNDERSIGNED AUTHORIZED EMPLOYEE AGREES THAT IF THE INFORMATION SUPPLIED ON THIS APPLICATION CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, HE/SHE WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE UNDERWRITER OF SUCH CHANGES, AND THE UNDERWRITER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE. FOR NEW HAMPSHIRE APPLICANTS, THE FOREGOING STATEMENT IS LIMITED TO THE BEST OF THE UNDERSIGNED'S KNOWLEDGE, AFTER REASONABLE INQUIRY. IN MAINE, THE UNDERWRITERS MAY MODIFY BUT MAY NOT WITHDRAW ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE.

NOTHING CONTAINED HEREIN OR INCORPORATED HEREIN BY REFERENCE SHALL CONSTITUTE NOTICE OF A CLAIM OR POTENTIAL CLAIM SO AS TO TRIGGER COVERAGE UNDER ANY CONTRACT OF INSURANCE. NO COVERAGE SHALL BE AFFORDED FOR ANY CLAIMS ARISING OUT OF A CIRCUMSTANCE NOT DISCLOSED IN THIS APPLICATION.

SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE UNDERWRITER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THIS APPLICATION SHALL BE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED, AND IT WILL BECOME PART OF THE POLICY.

ALL WRITTEN STATEMENTS AND MATERIALS FURNISHED TO THE INSURER IN CONJUNCTION WITH THIS APPLICATION ARE HEREBY INCORPORATED BY REFERENCE INTO THIS APPLICATION AND MADE A PART HEREOF. FOR NORTH CAROLINA, UTAH, AND WISCONSIN APPLICANTS, SUCH APPLICATION MATERIALS ARE PART OF THE POLICY, IF ISSUED, ONLY IF ATTACHED AT ISSUANCE.

Signed*:_____ Date:_____

Print Name:_____ Title: _____

If this **Application** is completed in Florida, please provide the Insurance Agent's name and license number. If this **Application** is completed in Iowa or New Hampshire, please provide the Insurance Agent's name and signature only.

Agent's Signature*:_____

Agent's Printed Name:_____ Florida Agent's License Number:_____

beazley

RANSOMWARE SUPPLEMENTAL APPLICATION

E-MAIL SECURITY

1. Do you pre-screen e-mails for potentially malicious attachments and links? ☐ Yes ☐ No
2. Do you provide a quarantine service to your users? ☐ Yes ☐ No
3. Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if malicious prior to delivery to the end-user? ☐ Yes ☐ No
4. Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails? ☐ Yes ☐ No
5. How often is phishing training conducted to all staff (e.g. monthly, quarterly, annually)? _____
6. Can your users access e-mail through a web app on a non-corporate device? ☐ Yes ☐ No
   If Yes: do you enforce Multi-Factor Authentication (MFA)? ☐ Yes ☐ No
7. Do you use Office 365 in your organisation? ☐ Yes ☐ No
   If Yes: Do you use the o365 Advanced Threat Protection add-on? ☐ Yes ☐ No

INTERNAL SECURITY

8. Do you use an endpoint protection (EPP) product across your enterprise? _____
9. Do you use an endpoint detection and response (EDR) product across your enterprise? _____
10. Do you use MFA to protect privileged user accounts? ☐ Yes ☐ No
11. Is a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices? _____
12. What % of the enterprise is covered by your scheduled vulnerability scans? _____
13. In what time frame do you install critical and high severity patches across your enterprise? _____
14. If you have any end of life or end of support software, is it segregated from the rest of the network? _____
15. Have you configured host-based and network firewalls to disallow inbound connections by default? _____
16. Do you use a protective DNS service (e.g. Quad9, OpenDNS or the public sector PDNS)? ☐ Yes ☐ No
17. Do you use an endpoint application isolation and containment technology? _____
18. Do your users have local admin rights on their laptop / desktop? ☐ Yes ☐ No
19. Can users run MS Office Macro enabled documents on their system by default? _____

20. Do you provide your users with a password manager software? ☐ Yes ☐ No

21. Do you manage privileged accounts using tooling? E.g. CyberArk _____

22. Do you have a security operations center established, either in-house or outsourced? _____

BACK-UP AND RECOVERY POLICIES

23. Are your backups encrypted? _____

24. Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose? _____

25. Do you use a Cloud syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive) for backups? ☐ Yes ☐ No

26. Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months? _____

27. Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware? _____

OTHER RANSOMWARE PREVENTATIVE MEASURES

Please describe any additional steps your organization takes to detect and prevent ransomware attacks (e.g. segmentation of your network, additional software tools, external security services, etc.).

Signed: _____

Print Name: _____

Title: _____

Company: _____

Date: _____

Follow Up Questions to Beazley Ransomware Supplemental 0820

1. Does the applicant employ any intrusion detection/response solution? Y/N ___

2. Is Multi-factor Authentication (**MFA**) utilized for the following? Y/N
   ___ critical information
   ___ remote access
   ___ personal devices
   ___ noncritical information and applications

3. Does applicant employ any of the following solutions? Y/N
   ___ Domain Keys Identified Mail (**DKIM**)
   ___ Domain-based Message Authentication (**DMARC**)

4. Does the applicant actively monitor all administrator access for unusual behavior patterns? Y/N ___

5. Is Remote Desktop Protocol enabled? Y/N ___

   If so, are the following implemented: Y/N
   ___ Virtual Private Network (**VPN**) Access only?
   ___ Multi-factor Authentication (**MFA**) for access?
   ___ Network level authentication enabled?
   ___ Remote Desk Protocol (**RDP**) honeypots?
   ___ Other? Please describe: _____

6. Training & Awareness: Y/N
   ___ Social engineering?
   ___ Role based training?
   ___ Privacy/data handling compliance?
   ___ Security/threat awareness?

7. Does the applicant conduct regular back up of data? Y/N ___

   How frequently is critical information backed up? Pick one:
   ___ Continuously
   ___ Daily
   ___ Weekly
   ___ Monthly
   ___ Quarterly
   ___ Semi-Annually
   ___ Annually

8. Does the applicant utilize physical backup tapes? Y/N ___

9. Where are backups stored? Pick one:
   ___ Cloud
   ___ On premises
   ___ Offline Storage
   ___ Offsite Storage
   ___ Secondary data center

10. Are backups subject to the following measures? Y/N
   ___ Multi-factor Authentication (**MFA**)?
   ___ Encryption?
   ___ Segmentation?
   ___ Virus/Malware Scanning?

11. Unique backup credentials stored separately from other user credentials? Y/N ___

12. How frequently are backups made to offsite storage? Pick one:
   ___ Weekly
   ___ Monthly
   ___ Annually

13. How frequently is a full recovery from a backup tested? Pick one:
   ___ Monthly
   ___ Quarterly
   ___ Annually

14. In the event of an interruption of the applicant's network, what is that applicant's recovery time objective for critical systems, applications and process? Pick one:
   ___ 8 hours
   ___ 8-12 hours
   ___ 12-24 hours
   ___ 24-48 hours
   ___ greater than 48 hours

15. In the event critical information, or critical systems, applications or processes became unavailable, how long would it take, at most, to materially interrupt the applicant's business? Pick one:
   ___ less than 1 hour
   ___ 1-8 hours
   ___ 8-12 hours
   ___ 12-24 hours
   ___ 24-48 hours