The Solution for Cyber Risk –**Ransomware supplement**

QBE Insurance

Your business

Insured Name (Applicant)

Gross revenue - last completed financial year (USD)

Description of business

Street Address

City State Zip

Statement of fact

1. Phishing

a. How often does the applicant use simulated phishing attacks to test employees?

Do the applicant's privileged users require more extensive training relating to phishing attacks? ☐ Yes ☐ No

b. Please provide the applicant's phishing success ratio:

c. Does the applicant flag external emails? ☐ Yes ☐ No

d. Does the applicant allow users to report suspicious emails? ☐ Yes ☐ No

If yes, does the applicant conduct training on spotting and reporting such emails? ☐ Yes ☐ No

2. Multifactor Authentication

a. Is multifactor authentication (MFA) required for all internal, external, and vendor access to the applicant's network? ☐ Yes ☐ No

b. If not, what are the compensating controls?

3. Email filtering

Does the applicant utilize email filtering protocols such as Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM), or Sender Policy Framework (SPF)? ☐ Yes ☐ No

4. Patching

a. Does the applicant track compliance for deploying critical patches? ☐ Yes ☐ No

If yes, what are the results?

b. Does the applicant have a policy (to enforce) when patches must be deployed? ☐ Yes ☐ No

If yes, what is the timeframe critical patches must be deployed?

c. What is the average time to triage and contain security incidents of workstations year to date?

Please provide further narrative around these response times and the process by which they are tracked.

d. What is the date of the applicant's most recent ransomware exercise?

Please explain the exercise, parties involved and lessons learned/key takeaways.

5. Segmentation

a. Does the applicant segment the network via Next Generation Firewalls, Virtual Local Area Networks (VLAN), demilitarized zones (DMZ), etc.? ☐ Yes ☐ No

b. How does the applicant eliminate or limit lateral movement within its network?

6. Privileged Access

a. How many of the applicant's users are granted Domain Admin Privileges?

b. Do these users require additional credentials to access? ☐ Yes ☐ No

c. Does the applicant utilize a Privileged Access Management (PAM) solution? ☐ Yes ☐ No

If yes, please provide name of PAM vendor:

If not utilizing a PAM solution, what compensating controls exist to protect privileged accounts?

d. Does the applicant restrict Local Admin rights? ☐ Yes ☐ No

e. How many service accounts have Domain Admin Privileges?

f. How many users have persistent privilege?

g. What is the minimum length for passwords?

h. How often are they rotated?

7. Logging and Monitoring

a. Does the applicant implement a Security Information and Event management (SIEM) tool to monitor activity logs and centralize tools? ☐ Yes ☐ No

b. Does the applicant monitor for unusual or suspicious network activity? ☐ Yes ☐ No

c. Is there an Endpoint Detection and Response (EDR) tool deployed on all endpoints? ☐ Yes ☐ No

d. What percentage of the applicant's most vital or critical assets are being logged and forwarded to a SIEM solution?

8. End-of-Life

a. Does the applicant have any end-of-life (EOL) software or applications currently running on the network? ☐ Yes ☐ No

b. If yes, how is that patched and managed?

9. Remote Desktop Protocol

a. Does the applicant utilize remote desktop protocol (RDP)? ☐ Yes ☐ No

b. If yes, does the applicant require strong authentication (e.g., two factor/ MFA)? ☐ Yes ☐ No

c. Is this behind a Virtual Private Network (VPN) or gateway? ☐ Yes ☐ No

d. Is RDP ever exposed to the internet? ☐ Yes ☐ No

10. Backup Strategy

a. Does the applicant perform full backups for databases, applications, endpoints, and servers (operating systems)? ☐ Yes ☐ No

b. How often are full backups performed?

c. Are backups stored offline? ☐ Yes ☐ No

Is all backup data encrypted once replicated? ☐ Yes ☐ No

d. Where are backups stored? ☐ Cloud ☐ Offsite ☐ Onsite

e. What is the applicant's target recovery time objective (RTO) for critical systems?

i. How often is it tested?

ii. Did the applicant hit their target in the most recent test? ☐ Yes ☐ No

f. Can backups only be accessed via an authentication mechanism (i.e., MFA/password vault/separate credentials or credential checkout)? ☐ Yes ☐ No

i. If yes, how are the backups accessed and who can access them?

ii. If no, how is the applicant protecting the backups?

g. Is virus/malware scanning used on the backups? ☐ Yes ☐ No

h. Are backups tested for vulnerabilities/malware prior to restoration? ☐ Yes ☐ No

i. How often are full network failover tests conducted?

What were the results of the most recent test?

j. Does the applicant conduct full vulnerability scans across the entirety of its network? ☐ Yes ☐ No

How often are these scans taken?

11. Encryption

a. Does the applicant have a policy that all portable devices use full disk encryption? ☐ Yes ☐ No

b. Where does the applicant use encryption?

c. How often does the applicant use encryption?

Other information

If applicant has any other information deemed pertinent to the Statement of Fact, please provide it below:

Applicant's cyber claims history

Applicant has not had any cyber or data breach incidents or other incidents that would otherwise have been covered under this policy had it been in force at the time. ☐ Yes ☐ No

If 'Yes', please provide details of the incidents:

Please list the applicants top 5 IT Vendors

Vendor	Type of Service
1.	
2.	
3.	
4.	
5.	

Fraud warning statements

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. **(Policyholders located in AL,**

CA, CO, DC, FL, KS, KY, ME, MD, NJ, NM, NY, OH, OK, OR, PA, TN, VT, VA, and WA must read the Fraud Warning applicable to their states.)

Notice to Alabama applicants: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance is guilty of a crime and may be subject to restitution fines or confinement in prison, or any combination thereof.

Notice to California applicants: For your protection California law requires the following to appear on this form. Any person who knowingly presents false or fraudulent information to obtain or amend insurance coverage or to make a claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state 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 of the third degree.

Notice to Kansas applicants: Any person who commits a fraudulent insurance act is guilty of a crime and may be subject to restitution, fines and confinement in prison. A "fraudulent insurance act" means an act committed by 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 any 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.

Notice to Kentucky applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance 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.

Notice to Maine 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 who 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 New Jersey applicants: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

Notice to New Mexico 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 CIVIL FINES AND CRIMINAL PENALTIES.

Notice to Ohio applicants: Any person who, with intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

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.

Notice to Oregon applicants: Any person who knowingly and with intent to defraud or solicit another to defraud an insurer: (1) by submitting an application, or (2) by filing a claim containing a false statement as to any material fact thereto, may be committing a fraudulent insurance act, which may be a crime and may subject the person to criminal and civil penalties.

Fraud warning statements (continued)

Notice to 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 claim 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.

Notice to Tennessee and Virginia 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 include imprisonment, fines and denial of insurance benefits.

Notice to Vermont applicants: Any person who knowingly presents a false statement in an application for insurance may be guilty of a criminal offense and subject to penalties under state law.

Notice to 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 include imprisonment, fines, and denial of insurance benefits.

Declaration

The undersigned authorized representative of Applicant declares and certifies that all statements set forth in this application (including all attachments, if applicable) are true, correct and complete, and that no material facts have been misstated, misrepresented or withheld. Applicant agrees to inform underwriters of any material alteration to these facts whether occurring before or after the completion of the contract of insurance.

Signing this application shall not constitute a binder or obligate the insurer to provide coverage and does not require the Applicant to purchase the policy. However, it is agreed that this application (including all attachments, if applicable) is and will continue to be relied upon should a policy be issued. If a policy is issued, this application will be attached to and made a part of the policy.

Notice to New York Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim 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 shall also be subject to a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

Signature of Principal/Partner/Director

Date

QBE North America
55 Water Street
New York, NY 10041
212.422.1212
qbe.com/us