## Cyber Risk Protector Supplemental Questionnaire - Ransomware

This Supplemental Questionnaire is applicable to Cyber Risk Protector coverage. As used herein, "**Applicant**" includes the **Company** applying for Cyber Risk Protector coverage and its subsidiaries.

Note:
- Response boxes shaded this color require an individual selection, effectively, which response option best describes the **Applicant**.
- Response boxes shaded this color represent questions where multiple responses may be selected. Note, these questions will also specify "select all that apply".

Full Name of Applicant: Canara Bank

| | | |
|---|---|---|
| 1 | With respect to the Applicant's efforts to mitigate phishing, select all that apply | |
| | Applicant provides security awareness training to employees at least annually. | X |
| | Applicant uses simulated phishing attacks to test employees' cybersecurity awareness at least annually. | X |
| | Where the Applicant is conducting simulated phishing attacks, the success ratio was less than 15% on the last test (less than 15% of employees were successfully phished).(ISS) | X |
| | Applicant 'tags' or otherwise marks e-mails from outside the organization. | X |
| | Applicant has a process to report suspicious e-mails to an internal security team to investigate. | X |
| | None of the above. | |
| | Additional Commentary on efforts to mitigate phishing: | |
| | | |
| 2 | Does the Applicant have a documented process to respond to phishing campaigns (whether targeted specifically at the Applicant or not)? | |
| | Yes | X |
| | No | |
| | If "Yes", please describe the principal steps to respond: | |
| | As per approved Email policy and the Guidelines On Reporting Of Unusual Cyber Security Incidents of the bank | |
| 3 | With respect to the **Applicant's** efforts to block potentially harmful websites and/or email, select all that apply: | |
| | **Applicant** uses an e-mail filtering solution which blocks known malicious attachments and suspicious file types, including executables. | X |
| | **Applicant** uses an e-mail filtering solution which blocks suspicious messages based on their content or attributes of the sender. | X |
| | **Applicant** uses a web-filtering solution which stops employees from visiting known malicious or suspicious web pages. | X |
| | **Applicant** uses block uncategorized and newly registered domains using web proxies or DNS filters. | X |
| | **Applicant** uses a web-filtering solution which blocks known malicious or suspicious downloads, including executables. | X |
| | **Applicant's** e-mail filtering solution has the capability to run suspicious attachments in a sandbox. | X |
| | **Applicant's** web filtering capabilities are effective on all corporate assets, even if the corporate asset is not on a corporate network (e.g. assets are configured to utilize cloud-based web filters or require a VPN connection to browse the internet). | X |
| | None of the above. | |
| | Additional commentary on efforts to block malicious websites and/or email: | |
| | ***E-mail solution is having anti APT Solution. Anti-phishing, Anti-Malware and Anti -spam policies are in place to filter the malicious mails at the gateway level. Mailicious email ids and domains are blocked.*** | |
| 4 | With respect to authentication for employees who are remotely accessing the corporate network and any cloud-based services where sensitive data may reside (including VPN access, and cloud-based email and CRM; together 'remote access to corporate resources'), select the description which best reflects the **Applicant's** posture: (As used herein, "multi-factor authentication" means authentication which uses at least two different types of the possible authentication factors (something you know, something you have, and something you are); the Applicant can provide further explanation below) | |
| | Remote access to corporate resources requires a valid username and password (single factor authentication). | |
| | Multi-factor authentication is in place for some types of remote access to corporate resources, but not all. | |
| | Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented. | X |
| | **Applicant** does not provide remote access to employees. | |
| | Additional commentary on authentication for employees: | |
| | | |
| 5 | With respect to authentication for independent contractors and vendors who are remotely accessing the corporate network and any cloud-based services where sensitive data may reside (including VPN access, and cloud-based email and CRM; together 'remote access to corporate resources'), select the description which best reflects the **Applicant's** posture: (The Applicant can provide further explanation below) | |
| | Remote access to corporate resources requires a valid username and password (single factor authentication). | |
| | Multi-factor authentication is in place for some types of remote access to corporate resources, but not all. | |

| | | |
|---|---|---|
| | Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented. | X |
| | **Applicant** does not provide remote access to independent contractors/vendors. | |
| | Additional commentary on authentication for independent contractors/vendors: | |
| | | |
| 6 | Does the **Applicant's** multifactor authentication implementation also meet the criteria that the compromise of any single device will only compromise a single authenticator?<br>(For illustration: where authentication requires a password (knowledge) and a token (possession), this would not meet the criteria above if the token to prove possession is<br>kept on a device the password is also entered into, exposing both if the device is compromised) | |
| | Not Applicable (**Applicant** does not use multi-factor authentication) | |
| | No; **Applicant's** multi-factor implementation does not meet the above criteria. | |
| | Yes; the **Applicant's m**ulti-factor implementation meets the above criteria. | X |
| | Additional commentary on Multi-factor authentication implementation: | |
| | | |
| 7 | With respect to the **Applicant's** endpoint security of workstations (desktops and laptops), select all that apply: | |
| | **Applicant's** policy is that all workstations have antivirus with heuristic capabilities. | X |
| | **Applicant** uses endpoint security tools with behavioral-detection and exploit mitigation capabilities. | X |
| | **Applicant** has an internal group which monitors the output of endpoint security tools and investigates any anomalies. | X |
| | None of the above. | |
| | Additional commentary on endpoint security capabilities: | |
| | **All Endpoints are Managed by Active Directorty Solution and we use Symantec Advanced Persistent Threat (APT) Protection to mitigate the Zero-day vulnerabilities.** | |
| 8 | With respect to monitoring the output of security tools, select the description which best reflects the **Applicant's** capabilities:<br>(The Applicant can provide further explanation below) | |
| | **Applicant** does not have staff dedicated to monitoring security operations (a "**Security Operations Center**"). | |
| | **Applicant** has a **Security Operations Center**, but it's not 24/7 (can be internal or external). | |
| | **Applicant** has a 24/7 monitoring of security operations by a 3rd party (such as a Managed Security Services Provider). | |
| | **Applicant** has 24/7 monitoring of security operations internally. | X |
| | Additional commentary on security monitoring: | |
| | | |
| 9 | What is the **Applicant's** average time to triage and contain security incidents of workstations year to date? (The Applicant can provide further explanation below) | |
| | **Applicant** does not track this metric/Do not know | |
| | <30 minutes | X |
| | 30 minutes-2 hours | |
| | 2-8 hours | |
| | >8 hours | |
| | Additional commentary on average time to remediate: | |
| | ***As per approved SOP for SECOPS(Ticketing tool).*** | |
| 10 | With respect to access controls for each user's workstation, select the description which best reflects the **Applicant's** posture:<br>(The Applicant can provide further explanation below) | |
| | No employees are in the Administrators' group or have local admin access to their workstations. | |
| | **Applicant's** policy is that employees by default are not in the Administrators' group and do not have local admin access; all exceptions to the policy are documented. | X |
| | Some of **Applicant's** employees are in the Administrators' group or are local admins. | |
| | Do not know. | |
| | Additional commentary on access controls for workstations: | |
| | | |
| 11 | With respect to protecting privileged credentials, select all that apply with respect to the **Applicant's** posture: | |
| | System administrators at the **Applicant** have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.). | X |
| | Privileged accounts (including Domain Administrators) require multifactor authentication. | X |
| | Privileged accounts are kept in a password safe that require the user to "check out" the credential (which is rotated afterwards). | X |
| | There is a log of all privileged account use for at least the last thirty days. | X |
| | Privileged Access Workstations (workstations that do not have access to internet or e-mail) are used for the administration of critical systems (including authentication servers/<br>Domain Controllers). | |
| | None of the above. | |
| | Additional commentary on protecting privileged credentials: | |
| | | |
| 12 | Indicate the **Applicant's** use of Microsoft Active Directory (across all domains/forests): | |

| | |
|---|---|
| **Applicant** does not use Microsoft Active Directory (indicate to the right) | |
| Number of user accounts in the Domain Administrators group (include service accounts - if any - in this total): | 11 |
| Number of service accounts in the Domain Administrators group:<br>("service account" means a user account created specifically for an application or service to interact with other domain-joined computers): | 4 |
| Additional commentary on the number of Domain Administrators: | |
| | |

| | | |
|---|---|---|
| 13 | How many users have persistent privileged accounts for endpoints (servers and workstations)?<br>(For the purposes of this question, "privileged accounts" means entitlements to configure, manage and otherwise support these endpoints; users who must 'check out' credentials should not be included. The Applicant can provide further explanation below) | |
| | Please enter an integer: | 0 |
| | Additional commentary on the number of privileged accounts: | |
| | ***For servers:NIL. PIM is used for accessing servers*** | |
| 14 | With respect to the security of externally facing systems, select all that apply to the **Applicant's** posture: | |
| | **Applicant** conducts a penetration test at least annually to assess the security of its externally facing systems. | X |
| | **Applicant** has a Web Application Firewall (WAF) in front of all externally facing applications, and it is in blocking mode. | X |
| | **Applicant** uses an external service to monitor its attack surface (external/internet facing systems) | X |
| | None of the above. | |
| | Additional commentary: NOC-Bank has Perimeter Firewalls, Intrusion Prevention System and Web Application Firewalls in place for better security posture of externally facing applications and systems | |
| 15 | What is the **Applicant's** target time to deploy 'critical' – the highest priority – patches (as determined by the **Applicant's** standards for when patches must be deployed)? | |
| | There is no defined policy for when patches must be deployed. | |
| | Within 24 hours. | X |
| | 24-72 hours. | |
| | 3-7 days. | |
| | > 7 days. | |
| | Additional commentary on target times for patching: | |
| 16 | What is the **Applicant's** year to date compliance with its own standards for deploying critical patches?<br>(The Applicant can provide further explanation below) | |
| | **Applicant** does not track this metric/Do not know | |
| | >95% | X |
| | 90-95% | |
| | 80-90% | |
| | <80% | |
| | Additional commentary on patching compliance: | |
| 17 | With respect to the **Applicant's** network monitoring capabilities, select all that apply: | |
| | **Applicant** uses a security information and event monitoring (SIEM) tool to correlate the output of multiple security tools. | X |
| | **Applicant** monitors network traffic for anomalous and potentially suspicious data transfers. | X |
| | **Applicant** monitors for performance and storage capacity issues (such as high memory or processor usage, or no free disk space). | X |
| | **Applicant** has tools to monitor for data loss (DLP) and they are in blocking mode. | X |
| | None of the above. | |
| | Additional commentary on network monitoring: | |
| 18 | With respecting to limiting lateral movement, select all that apply to the **Applicant's** posture:<br>(The Applicant can provide further explanation below) | |
| | **Applicant** has segmented the network by geography (e.g. traffic between offices in different locations is denied unless required to support a specific business requirement). | X |
| | **Applicant** has segmented the network by business function (e.g. traffic between asset supporting different functions – HR and Finance for example – is denied unless required to support a specific business requirement). | X |
| | **Applicant** has implemented host firewall rules that prevent the use of RDP to log into workstations. | X |
| | **Applicant** has configured all service accounts to deny interactive logons. | X |
| | None of the above. | |
| | Additional commentary on segmentation: | |
| 19 | Enter the date of the **Applicant's** last ransomware exercise; check the box if none has been conducted. | |
| | **Date:** | |
| | | X |
| 20 | Does the **Applicant** have a documented plan to respond to ransomware of a 3rd party provider/vendor or customer? If yes, please indicate principle steps. | |
| | No | |
| | Yes | X |
| | 3rd party ransomware response principle steps: | |

| | |
|---|---|
| | Yes. The same is made part of RFP documents where 3rd party vendors/service providers has to comply with bank's policies such as ISP, CSP, CCMP etc. Further, steps to respond for a ransomeware incident has been defined in bank's CCMP. |

| | | |
|---|---|---|
| 21 | With regards to verifying the efficacy of security controls, select all that apply to the **Applicant**:<br>(The Applicant can provide further explanation below | |
| | **Applicant** uses Breach and Attack Simulation (BAS) software to verify the effectiveness of security controls. | X |
| | **Applicant** has an internal "red team" that tests security controls and response. | X |
| | **Applicant** has engaged an external party to simulate threat actors and test security controls in the last year. | X |
| | None of the above. | |
| | Additional commentary on controls verification: | |
| | | |
| 22 | With regards to disaster recovery capabilities, select all that apply to the **Applicant**: | |
| | A process for creating backups exists, but it is undocumented and/or ad hoc | |
| | **Applicant** has a documented Disaster Recovery Policy, including standards for backups based on information criticality. | X |
| | At least twice a year, **Applicant** tests its ability to restore different critical systems and data in a timely fashion from its backups. | X |
| | None of the above. | |
| 23 | What is the **Applicant's** Recovery Time Objective (RTO) for critical systems? | |
| | **Applicant** does not have an RTO/Does not know | |
| | < 4 hours. | X |
| | 4-24 hours. | |
| | 1 to 2 days. | |
| | 2-7 days. | |
| 24 | With respect to backup capabilities, select all that apply to the **Applicant**: | |
| | **Applicant's** backup strategy includes offline backups (can be stored on site) | X |
| | **Applicant's** backup strategy includes offline backups stored offsite | X |
| | **Applicant's** backups can only be accessed via an authentication mechanism outside of our corporate Active Directory. | X |
| | Additional commentary on backup capabilities: | |
| | | |
| 25 | Does the **Applicant** have a policy that all portable devices use full disk encryption? | |
| | Yes | X |
| | No | |
| | Additional commentary: | |
| | | |

**THIS SUPPLEMENTAL QUESTIONNAIRE IS INCORPORATED INTO AND MADE PART OF ANY APPLICATION FOR CYBER RISK PROTECTOR COVERAGE BY THE APPLICANT. ALL REPRESENTATIONS AND WARRANTIES MADE BY APPLICANT IN CONNECTION WITH SUCH APPLICATION ALSO APPLY TO THE INFORMATION PROVIDED IN THIS SUPPLEMENTAL QUESTIONNAIRE.**

**SHOULD INSURER ISSUE A POLICY, APPLICANT AGREES THAT SUCH POLICY IS ISSUED IN RELIANCE UPON THE TRUTH OF THE STATEMENTS AND REPRESENTATIONS IN THIS SUPPLEMENTAL QUESTIONNAIRE OR INCORPORATED BY REFERENCE HEREIN. ANY MISREPRESENTATION, OMISSION, CONCEALMENT OR INCORRECT STATEMENT OF A MATERIAL FACT, IN THIS SUPPLEMENTAL QUESTIONNAIRE, INCORPORATED BY REFERENCE OR OTHERWISE, SHALL BE GROUNDS FOR THE RESCISSION OF ANY POLICY ISSUED.**

Signed: _____

(Duly authorized representative, by and behalf of the **Applicant**)

Date: _____