AIG

Cyber Insurance

Ransomware Supplemental Questionnaire

This Supplemental Questionnaire is applicable to CyberEdge® coverage. As used herein, **"Applicant"** includes the Company applying for CyberEdge® coverage (that is, the **Policyholder**) and its subsidiaries.

Full Name of Applicant:	

Instructions for the following sections:

In the response column, unless the question specifically asks for a "write-in" or specific integer, the drop-down selection will solely allow an answer of Yes. When the **Applicant** leaves the Response as blank, it will be interpreted as a "no" or "not having such control," unless there is a Response option that specifically indicates No, Don't Know, or None of the Above. There are commentary sections after each section that will allow the **Applicant** to provide additional commentary, if desired. *(Additional commentary sections are limited to 1,000 characters; if additional space is needed, please attach a separate document as an appendix)*

The questions below are important to the underwriting of coverage for the **Applicant**. This must be completed by, or with the assistance of, the person(s) responsible for the security of the **Applicant's** information systems. If information security is outsourced to a third party (e.g., a managed security provider), it is understood that the **Applicant** has verified its responses with such third party prior to submitting this supplemental.

Data Security & Business Continuity

	Question	Response
DS/BC #1	*Select one response:* How centralized is the **Applicant's** information security program?	
	Information security at the **Applicant** is centrally managed, and the policies apply to all operations. Where exceptions are made, it's by asset only (as opposed to by operation/legal entity).	
	Information security at the **Applicant** is centrally managed, but exceptions are made for certain operation/legal entities. The controls as outlined below apply to greater than or equal to 98% of total endpoints.	
	Information security at the **Applicant** is centrally managed, but exceptions are made for certain operation/legal entities. The controls as outlined below apply to less than 98% of total endpoints.	
	Information security at the **Applicant** is federated, but the controls outlined below apply to greater than or equal to 98% of total endpoints.	
	Information security at the **Applicant** is federated, and the controls outlined below apply to greater than 50% of total endpoints, but less than 98% of total endpoints.	
	Information security is managed by individual legal entities or operating units. The controls below are based on a survey of all entities and operating units.	
	Other (indicate to the right and describe in comments section at end of Data Security & Business Continuity section).	
	Don't know.	

Data Security & Business Continuity

	Question	Response
DS/BC # 2	*Select all responses that are true:* With regards to the **Applicant's** management of information technology assets (hardware and software):	
	The **Applicant** has an inventory of all enterprise hardware assets - including end-user devices, network devices, appliances, IoT devices, and servers - that includes the network address (if static), hardware address, machine name, and enterprise asset owner, and updates it at least bi-annually.	
	The **Applicant** has an inventory of all enterprise hardware assets - including end-user devices, network devices, appliances, IoT devices, and servers - that includes the network address (if static), hardware address, machine name, and enterprise asset owner, and updates it at least annually.	
	The **Applicant** has a process to discover and identify hardware assets on its network and does so at least daily.	
	The **Applicant** has a process to discover and identify hardware assets on its network and does so at least weekly.	
	The **Applicant** has a process to update its hardware asset inventory at least weekly based on discovery tools or IP Address Management (IPAM) software.	
	The **Applicant** has an inventory of all licensed software installed on enterprise assets and updates it at least bi-annually.	
	The **Applicant** has a process to ensure all software is either supported or is a documented exception with mitigating controls, and the process is repeated at least monthly.	
	None of the above.	
DS/BC # 3	*Select all responses that are true:* With regards to the **Applicant's** management of "Vital Assets": "Vital Assets" means those assets which are key to the organization's success and operation, including, but not limited to, applications which support business production, applications which store business critical and/or sensitive data, and core technology services such as directory services, document repositories, and email.	
	The **Applicant** has an inventory of all data stores - including data owner, the asset it's stored on, sensitivity, retention limits and disposal requirements - for at least all sensitive data and updates it at least annually.	
	The **Applicant** has defined and documented all "Vital Assets".	
	The **Applicant** has a process to actively identify "Vital Assets" and update the inventory of "Vital Assets" at least quarterly.	
	The **Applicant** prioritizes "Vital Assets" by importance to business operations.	
	None of the above.	
DS/BC # 4	What is the "Recovery Time Objective" (RTO) for "Vital Assets"? "RTO" means the amount of time in which "Vital Assets" are expected to be restored by an organization after a disaster/disruption.	
	< 5 hours.	
	5-12 hours.	
	12-24 hours.	
	1-7 days.	
	> 7 days.	
	No RTO is defined/Don't Know.	
DS/BC # 5	*Select all responses that are true:* With respect to the **Applicant's** disaster recovery capabilities:	
	A process for creating backups exists (even if it is undocumented and/or ad hoc).	
	Applicant's documented Disaster Recovery Policy requires weekly or more frequent automated backups and standards for backups based on information criticality.	
	At least quarterly, **Applicant** tests its ability to restore different "Vital Assets" in accordance with the Recovery Time Objective (RTO).	
	None of the above/Don't know.	

Data Security & Business Continuity

	Question	Response
DS/BC # 6	*Select all responses that are true:* With respect to the **Applicant's** backup capabilities:	
	Applicant's backup strategy includes offline (archive) backups stored onsite.	
	Applicant's backup strategy includes offline (archive) backups stored offsite.	
	Applicant's backup strategy includes onsite, regular backups.	
	Applicant's backup strategy includes offsite, regular backups (Cloud or Continuity of Operations Site).	
	Applicant's backups are isolated and separate from the production domain (i.e., they are accessed via an authentication mechanism outside of Active Directory or are otherwise available even if the production domain is compromised) or they are immutable.	
	None of the above/Don't know.	
DS/BC # 7	*Select all responses that are true:* With respect to the **Applicant's** policies for the use of encryption to protect data:	
	The **Applicant** requires that all data on portable devices - including phones, tablets, and laptops – is encrypted (using full disk encryption or file based encryption)	
	The **Applicant** requires that all end user devices - even if not portable - containing sensitive data must use full disk encryption.	
	The **Applicant** requires that all removeable media - USB sticks, CDs, etc. - is encrypted	
	The **Applicant** requires that all sensitive data at rest is encrypted (at either the storage layer or application layer).	
	None of the above/Don't know.	
DS/BC # 8	*Select all responses that are true:* With respect to the **Applicant's** monitoring of "Vital Assets":	
	The **Applicant** has an internal function and/or has an outsourced Managed Security Service Provider ("MSSP") charged with monitoring security event alerts, including alerts on "Vital Assets" (a "Security Operations Center" or "SOC").	
	The **Applicant's** SOC/MSSP is provided an updated list of "Vital Assets" at least quarterly.	
	The **Applicant's** SOC/MSSP uses a Security Information and Event Monitoring (SIEM) solution to automate the collection of logs from "Vital Assets".	
	None of the above/Don't know.	
	If **Applicant** has any additional commentary on any specific question or response in this section, please provide below:	

Identity, Credential, and Access Management Security

	Question	Response
ICA # 1	*Select all responses that are true:* Which of the following tools does the Applicant use for directory services, identity providers (IdP), federation and/or rights management?	
	Microsoft Active Directory (Active Directory)	
	Azure Active Directory (Azure AD)	
	Okta	
	Ping	
	Active Directory Federation Services	
	Google Workspaces	
	Other (details required – provide in the next row)	
	If Other provide details here:	
	None of the above/Don't Know.	
ICA # 2	*Select one response:* What is the source of identity for the majority of **Applicant's** users?	
	Microsoft Active Directory (Active Directory)	
	Azure Active Directory (Azure AD)	
	Active Directory and Azure AD (Active Directory is authoritative)	
	Azure AD and Active Directory (Azure AD is authoritative)	
	An Identity Provider ("IdP"; e.g., Okta or Ping)	
	Cloud-based collaboration (e.g., Google Workspaces)	
	Other (details required – provide in the next row)	
	If Other provide details here:	
	No centralized identity management or don't know.	
ICA # 3	*Select all responses that are true:* With respect to the **Applicant's** account management:	
	The **Applicant** has an inventory of all user and administrative accounts.	
	The **Applicant's** inventory of accounts includes the individual's name, username, start/stop dates, and department.	
	The **Applicant** validates that all active accounts are authorized, at least annually.	
	The **Applicant** validates that all active accounts are authorized, at least quarterly.	
	None of the above.	

Identity, Credential, and Access Management Security

	Question	Response
ICA # 4	*Select all responses that are true:* With respect to the **Applicant's** policies and technical controls on passwords:	
	The **Applicant** educates users on the risks of password reuse and has a policy against it.	
	The **Applicant** has a solution to prevent users from setting common and known-breached passwords, even if they meet complexity requirements (such as "1q2w3e4r5t" and "Passw0rd!").	
	The **Applicant** provides a password manager to its employees.	
	The **Applicant** has implemented a solution to set different, random passwords across all domain-attached computers for local administrator accounts (i.e., Local Administrator Password Solution – Reference: https://support.microsoft.com/en-us/topic/microsoft-security-advisory-local-administrator-password-solution-laps-now-available-may-1-2015-404369c3-ea1e-80ff-1e14-5caafb832f53).	
	None of the above.	
ICA # 5	*Select all responses that are true:* With regards to how the **Applicant** protects user accounts with domain administrative privileges ("Domain Administrator Accounts"): "Domain Administrator Accounts" means those user accounts - excluding "Service Accounts" - which can edit information in whatever solution the **Applicant** is using for directory services, identity provider (IdP), rights management, etc. In an Active Directory environment, this would include Enterprise Admins, Domain Admins, and the (domain) Administrators groups (and any nested groups/accounts); in Azure AD this would include Global Administrators, Hybrid Identity Administrators, and Privileged Role Administrators).	
	System administrators at the **Applicant** have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.).	
	"Domain Administrator Accounts" require multifactor authentication.	
	"Domain Administrator Accounts" are managed and monitored through just-in-time access, are time bound, and require approvals to provide privileged access.	
	"Domain Administrator Accounts" are kept in a password safe that requires the user to "check out" the credential (which is rotated afterwards).	
	In addition to being kept in a password safe, "Domain Administrator Accounts" are not exposed to the administrative user when "checked out", and access is recorded through a session manager.	
	"Domain Administrator Accounts" can only be used from Privileged Access Workstations (workstations that do not have access to internet or email).	
	There is a log of all actions by "Domain Administrator Accounts" for at least the last thirty days.	
	None of the above/Don't Know.	
ICA # 6	*Select one response:* How do the **Applicant's** employees authenticate to remotely access the corporate network?	
	Remote access to the corporate network generally only requires a valid username and password (single factor authentication).	
	Multi-factor authentication (MFA) is in place for some types of remote access to the corporate network, but not others.	
	MFA is required by policy for all remote access to the corporate network, and all exceptions to the policy are documented.	
	Applicant does not provide remote access to any employees.	

Identity, Credential, and Access Management Security

	Question	Response
ICA # 7	*Select one response:* How do vendors of the **Applicant** authenticate to remotely access the corporate network?	
	Remote access to the corporate network generally only requires a valid username and password (single factor authentication).	
	MFA is in place for some types of remote access to the corporate network, but not others.	
	MFA is required by policy for all remote access to the corporate network, and all exceptions to the policy are documented.	
	Applicant does not provide remote access to any vendors.	
ICA # 8	*Select one response:* How do both employees and vendors of the **Applicant** authenticate to those Vital Assets which are SaaS/3rd party applications?	
	Access to externally hosted Vital Assets generally only requires a valid username and password (single factor authentication).	
	MFA is in place for some types of access to externally hosted Vital Assets, but not others.	
	MFA is required by policy for all access to externally hosted Vital Assets, and all exceptions to the policy are documented.	
	Applicant does not use SaaS/3rd party hosted applications which would be considered Vital Assets.	
ICA # 9	*Select all responses that are true:* With regards to how the **Applicant** protects "Privileged" "Service Accounts": "Service Accounts" are accounts used for running applications and other processes; they are not typically used by people outside troubleshooting. "Privileged" means having elevated privileges, and in an Active Directory environment, includes, but is not limited to, Enterprise Admins, Domain Admins, and (domain) Administrators.	
	There is an inventory of all "Privileged" "Service Accounts", and it is updated at least quarterly.	
	"Privileged" "Service Accounts" have password lengths of at least 25 characters.	
	"Privileged" "Service Accounts" have their passwords rotated at least annually.	
	"Privileged" "Service Accounts" have their passwords rotated at least quarterly.	
	"Service Accounts" are tiered such that different accounts are used to interact with workstations, servers, and authentication servers, even for the same service.	
	There is a process in place to review at least annually the current requirements for each service associated with "Privileged" "Service Accounts" to verify the service still requires the permissions the service account has (and deprivilege if not).	
	None of the above/Don't know.	
ICA # 10	*Select one response:* Authenticator Assurance Level (AAL) which best represents the **Applicant's** authentication solution(s). NIST Special Publication 800-63B defines the Authenticator Assurance Levels.	
	AAL1	
	AAL2	
	AAL3	
	Don't know.	

Identity, Credential, and Access Management Security

	Question	Response
ICA # 11	Provide the number of active accounts the **Applicant** has for the categories below. Accounts should not include inactive accounts but should include all nested accounts aggregated across all domains/forests.	
	Number of "Domain Administrator Accounts":	
	Number of "Privileged" "Services Accounts":	
	NOTE: For each "Privileged" "Service Account", use the table provided at the end of the supplemental to indicate i) the name of the account, ii) the privileges it has, iii) the software it supports, iv) what hosts the service account is authenticating to, and v) why those entitlements are required.	
ICA # 12	*Select one response:* Which description below best reflects the **Applicant's** posture with respect to access controls for each user's workstation? For the purposes of this question, where the Applicant is using an endpoint privilege manager or other similar technology to allow users to temporarily request administrative access for certain activities, that should not be considered "admin access".	
	No user's regular, every day account is in the Administrator's group or has local admin access to their workstation.	
	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.	
	Some of the **Applicant's** employees are in the Administrators' group or are local admins.	
	Don't know.	
ICA # 13	*Select one response:* Which description best reflects the **Applicant's** posture with respect to access controls for member servers? This question is regarding employees' everyday user accounts; where the **Applicant** provisions employees with separate credentials for administrative access, those accounts should not be considered for the purposes of this question.	
	No employees are in the Administrator's group or have local admin access to member servers.	
	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.	
	Some of the **Applicant's** employees are in the Administrators' group or are local admins.	
	Don't know.	
ICA # 14	How many of the **Applicant's** users have persistent administrative access to servers and/or workstations other than their own? For the purposes of this question, "administrative access" means entitlements to configure, manage and otherwise support these endpoints, including through the use of a unique administrative account (separate from their everyday user account). Users who must "check out" credentials for administrative access should not be included.	
	Please enter an integer:	
ICA # 15	Does the **Applicant** ingest security logs from all Domain Controllers into their SIEM solution for analysis?	
	Yes	
	No – Applicant doesn't have a SIEM or doesn't ingest security logs into SIEM	
	Not Applicable - not using directory services, IdP, rights management.	

Identity, Credential, and Access Management Security

	Question	Response
ICA # 16	*Select all responses that are true:* What Audit Policies has the **Applicant** enabled on Domain Controllers?	
	Audit Credential Validation (Failure)	
	Audit Process Creation (Success)	
	Audit Security Group Management (Success and Failure)	
	Audit User Account Management (Success and Failure)	
	Audit Other Account Management Events (Success and Failure)	
	Audit Sensitive Privilege Use (Success and Failure)	
	Audit Logon (Success and Failure)	
	Audit Special Logon (Success)	
	None of the above/Don't know.	
	Not applicable (not using Active Directory).	
	If **Applicant** has any additional commentary on any specific question or response in this section, please provide below:	

Security Monitoring and Incident Response

	Question	Response
SMIR # 1	*Select one response:* Which description best reflects the **Applicant's** security operations program?	
	Applicant does not have anyone (internal or external) dedicated to monitoring security operations (a "Security Operations Center" or SOC).	
	Applicant has a SOC, but it's not 24/7 (can be internal or external).	
	Applicant has 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 (regardless of whether or not a 3rd party is also used).	
SMIR # 2	*Select all responses that are true:* With respect to the **Applicant's** security and network monitoring capabilities:	
	Applicant uses a "Security Information and Event Monitoring" or SIEM tool to correlate the output of multiple security tools.	
	Applicant monitors network traffic for anomalous and potentially suspicious data transfers.	
	Applicant monitors for performance and storage capacity issues on all servers (such as high memory or processor usage, or no free disk space).	
	Applicant has tools to monitor for data loss (DLP) and they are in blocking mode.	
	Applicant has tools to monitor for data loss (DLP), but they are not in blocking mode.	
	None of the above/Don't know.	
SMIR # 3	What is the **Applicant's** average time to triage and contain security incidents of workstations for the most recent completed quarter?	
	<30 minutes	
	30 minutes-2 hours	
	2-8 hours	
	8 hours-3 days	
	>3 days	
	Applicant does not track this metric/Don't know.	
SMIR # 4	What percentage of the **Applicant's** "Vital Assets" are being logged and forwarded to a SIEM solution?	
	0-30%	
	31-50%	
	51-70%	
	>= 71%	
	Don't know	
	Not applicable (no SIEM)	

Security Monitoring and Incident Response

	Question	Response
SMIR # 5	How long does the **Applicant's** SIEM solution retain logs?	
	Less than 30 days	
	30-59 days	
	60-89 days	
	90 days or more	
	Don't know	
	Not applicable (no SIEM)	
SMIR # 6	*Select all responses that are true:* With respect to how the **Applicant** validates the efficiency and effectiveness of security controls:	
	Applicant uses Breach and Attack Simulation (BAS) software to verify the effectiveness of security controls.	
	Applicant has a "red team" on staff to test security controls, or at least annually engages experts to perform a penetration test focused on internal systems.	
	Applicant has engaged an external party to simulate threat actors and test security controls in the last year.	
	None of the above.	
	Don't know	
	Not applicable (no SIEM)	
SMIR # 7	*Select all responses that are true:* With respect to the **Applicant's** incident response program and procedures:	
	Applicant has a documented incident response plan.	
	Applicant's incident response plan includes a playbook specifically for a ransomware incident at the organization.	
	Applicant's incident response plan includes a playbook specifically for a ransomware incident of 3rd parties/MSPs.	
	Applicant's incident response plan includes contact of law enforcement once a ransomware incident is confirmed.	
	Applicant's response plan includes a process to resume business operations by restoration of known clean backups.	
	None of the above.	
SMIR # 8	Does the **Applicant** have a documented process to respond to phishing incidents (whether targeted specifically at the **Applicant** or its employees, or not)?	
	Yes	
	No	
	If **Applicant** has any additional commentary on any specific question or response in this section, please provide below:	

Risk Management

	Question	Response
RM # 1	Does the **Applicant** have a vulnerability scanning program which identifies and manages vulnerabilities across “Vital Assets”?	
	Yes	
	No	
RM # 2	*Select all responses that are true:* With respect to the factors the **Applicant** uses to prioritize patching:	
	Common Vulnerability Scoring System (CVSS) score.	
	Correlation with whether the vulnerability affects the **Applicant's** "Vital Assets".	
	Generic threat intelligence (e.g., that threat actors are exploiting a given vulnerability; this includes tools like CISA’s Known Exploited Vulnerability Catalog).	
	Threat intelligence specific to the **Applicant** (including intelligence that threat actors may be targeting the **Applicant** specifically via exploitation of a certain vulnerability, or data from the **Applicant’s** environment which indicates where threat actors are focused).	
	None of the above/Don't know.	
RM # 3	What is the **Applicant’s** target time to deploy the highest priority patches?	
	Within 24 hours.	
	24-72 hours.	
	3-7 days.	
	7-29 days.	
	>= 30 days.	
	There is no defined policy for when patches must be deployed/Don’t know.	
RM # 4	What is the **Applicant’s** compliance rate with its own standards for deploying the most important patches in the most recent completed quarter?	
	>95%	
	90-95%	
	80-89%	
	<80%	
	Not tracked/Don’t know.	
RM # 5	*Select all responses that are true:* With respect to the **Applicant’s** policies for the use of organizational IT assets:	
	The **Applicant** has an "Acceptable Use Policy" (AUP) outlining users' obligations and constraints.	
	The AUP describes consequences for policy violations.	
	Users are disallowed from surfing social media platforms from organizational assets except where this is a defined business need.	
	Users are disallowed from accessing personal email from organizational assets.	
	Administrators are explicitly disallowed from surfing the internet or accessing personal email from their privileged accounts.	
	Users and administrators are responsible for keeping their computer and accounts safe from common risks or issues.	
	Users and administrators are required to report suspected violations.	
	None of the above/Don’t know.	

Risk Management

	Question	Response
RM # 6	*Select all responses that are true:* With respect to the **Applicant's** capabilities to monitor for risky behavior and malicious insiders:	
	Applicant has an insider threat program.	
	Applicant monitors for when a user or administrator account sets an insecure password.	
	Applicant monitors for when "Privileged" accounts access unauthorized websites and services.	
	Applicant monitors for unauthorized remote access to "Vital Assets".	
	Applicant monitors both user and administrator accounts for communication with known malicious websites, IP addresses, and other well-known threat group resources.	
	None of the above/Don't know.	
	If **Applicant** has any additional commentary on any specific question or response in this section, please provide below:	

Phishing Defense

	Question	Response
PhD # 1	*Select all responses that are true:* With respect to the **Applicant's** capabilities for mitigating phishing incidents:	
	Applicant provides security awareness training, including phishing awareness training, to employees at least annually.	
	Applicant uses simulated phishing attacks to test employees' cybersecurity awareness at least annually.	
	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).	
	Applicant 'tags' or otherwise marks e-mails from outside the organization.	
	Applicant has a documented process to report suspicious e-mails to an internal security team to investigate and publishes the process to users.	
	None of the above/Don't know.	
PhD # 2	*Select all responses that are true:* With respect to the **Applicant's** capabilities to block potentially harmful websites and/or email:	
	Applicant uses an e-mail filtering solution which blocks known malicious attachments and suspicious file types, including executables.	
	Applicant uses an e-mail filtering solution which blocks suspicious messages based on their content or attributes of the sender.	
	Applicant uses a web-filtering solution which stops employees from visiting known malicious or suspicious web pages.	
	Applicant blocks uncategorized and newly registered domains using web proxies or DNS filters.	
	Applicant uses a web-filtering solution which blocks known malicious or suspicious downloads, including executables.	
	Applicant's e-mail filtering solution has the capability to run suspicious attachments in a sandbox.	
	Applicant's web filtering capabilities are effective on all organization assets, even if the asset is not on the organization's network (e.g., assets are configured to utilize cloud-based web filters or require a VPN connection to browse the internet).	
	None of the above/Don't know.	
	If **Applicant** has any additional commentary on any specific question or response in this section, please provide below:	

Malware Defense

	Question	Response
Mal # 1	*Select all responses that are true:* With respect to the **Applicant's** endpoint security tool's capabilities:	
	Applicant's endpoint security solution includes antivirus with heuristic capabilities.	
	Applicant uses endpoint security tools with behavioral-detection and exploit-mitigation capabilities.	
	Applicant uses an endpoint threat detection and response (ETDR or EDR) tool which does all the following: monitors for threat indicators; identifies patterns which match known threats; automatically responds by removing or containing threats; alerts security personnel of incidents; provides forensic and analysis capabilities to allow analysts to perform threat hunting activities.	
	Applicant implements application controls across workstations to only allow for execution of authorized applications. Unauthorized applications are blocked, and the list of authorized applications is reassessed at least bi-annually.	
	Applicant has an internal group and/or MSSP which monitors the output of endpoint security tools and investigates any anomalies.	
	None of the above/Don't know.	
Mal # 2	*Select all responses that are true:* With respect to the **Applicant's** deployment of its endpoint security tool(s) (as described above):	
	Applicant's endpoint security tool(s) is/are deployed on all workstations & laptops; all exceptions are documented.	
	Applicant's endpoint security tool(s) is/are deployed on all servers (excluding hypervisor hosts); all exceptions are documented.	
	Applicant's endpoint security tool(s) is/are deployed on all mobile devices (including tablets, phones, etc. but excludes laptops); all exceptions are documented.	
	None of the above/Don't know.	
Mal # 3	*Select all responses that are true:* With respect to the **Applicant's** configuration of its endpoint security tool(s) (as described above):	
	For those tools which require updated definitions, such tools are updating at least daily.	
	Tool(s) is/are configured to block (vs. just notify of) suspected malicious processes/files.	
	Tool(s) is/are configured to find unmanaged assets, which are addressed at least weekly.	
	Anti-tamper features are enabled.	
	None of the above/Don't know.	
Mal # 4	Identify the endpoint security tool(s) used (please be as specific as possible, e.g., "Falcon Prevent, Insight and Overwatch", not "CrowdStrike"):	
	Write in here:	

Malware Defense

	Question	Response
Mal # 5	*Select all responses that are true:* With respect to the **Applicant's** capabilities to limit lateral movement:	
	Applicant has segmented the network by geography (i.e., traffic between offices in different locations is denied unless required to support a specific business requirement).	
	Applicant has segmented the network by business function (i.e., traffic between assets supporting different functions - HR and Finance for example - is denied unless required to support a specific business requirement).	
	Applicant has implemented host firewall rules that prevent the use of RDP to log into workstations.	
	Applicant has configured all service accounts to deny interactive logons.	
	None of the above/Don't know.	
Mal # 6	Has the **Applicant** conducted an exercise simulating the tactics, techniques, and procedures of ransomware actors in the last year?	
	Yes	
	No	
	If **Applicant** has any additional commentary on any specific question or response in this section, please provide below:	

Third Parties & Managed Service Providers Defense

	Question	Response
TP & MSP # 1	*Select all responses that are true:* With respect to the roles of third parties or Managed Service Providers (MSPs) for the **Applicant's** network, including remote access to resources such as cloud and VPNs.	
	Applicant utilizes an MSP for administration of "Vital Assets".	
	Applicant utilizes an MSP for security operations.	
	Applicant utilizes an MSP for data backup and recovery.	
	Applicant utilizes an MSP for cloud transformation.	
	Applicant utilizes an MSP for software development.	
	Applicant provides third parties persistent ("always on") access to corporate resources (access does not require Applicant's authorization).	
	None of the above/Don't know.	
TP & MSP # 2	Does the **Applicant** have a process or technical solution to identify, assess, manage, monitor, and reduce the risks from MSPs and third parties?	
	Yes	
	No	
	If **Applicant** has any additional commentary on any specific question or response in this section, please provide below:	

Perimeter and Internet Defense

	Question	Response
Perimeter # 1	*Select all responses that are true:* With respect to the **Applicant's** capabilities to secure externally-exposed systems, including internet-facing systems:	
	Applicant maintains an inventory of externally-exposed assets.	
	Applicant performs regular vulnerability scans of externally-exposed assets.	
	Applicant has a Web Application Firewall (WAF) in front of all externally-exposed applications, *and it is in blocking mode.*	
	Applicant scans externally-exposed assets for vulnerabilities at least monthly.	
	Applicant uses an external service to monitor its attack surface (internet-facing systems).	
	Applicant disables or blocks on externally-exposed systems those ports, services, and protocols known to allow the spread of ransomware, including, but not limited to RDP, SMBv1, and SMBv2.	
	Applicant's externally-exposed assets are segmented within a demilitarized zone (DMZ), and the DMZ is not directly routable to the corporate network. Users requiring access to DMZ services are routed to the internet for access.	
	Applicant can detect and respond to threats through endpoint and network monitoring solutions.	
	None of the above/Don't know.	
	If **Applicant** has any additional commentary on any specific question or response in this section, please provide below:	

"Privileged" "Service Account" Appendix (if applicable)

Instructions:

For each "Privileged" "Service Account", use the table provided to indicate:

i) the name of the account,
ii) the privileges it has,
iii) the software product it supports,
iv) what hosts the service account is authenticating to, and
v) why those entitlements are required.

"Privileged" "Service Account" Appendix

Name of the Account	Privileges it has	Software product it supports	What hosts it authenticates to	Why those entitlements are required
EXAMPLE ONLY svc_cyberark	*EXAMPLE ONLY Domain Admin*	*EXAMPLE ONLY CyberArk Privileged Access Manager*	*EXAMPLE ONLY Solely Domain Controllers*	*EXAMPLE ONLY DA required to change passwords of sensitive accounts*
	Choose an item		Choose an item	
	Choose an item		Choose an item	
	Choose an item		Choose an item	
	Choose an item		Choose an item	
	Choose an item		Choose an item	
	Choose an item		Choose an item	
	Choose an item		Choose an item	
	Choose an item		Choose an item	
	Choose an item		Choose an item	

This Supplemental Questionnaire is incorporated into and made part of any application for Cyberedge 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 the **Insurer** issue a policy, the **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 fraudulent non-disclosure or misrepresentation in this Supplemental Questionnaire, incorporated by reference or otherwise, shall constitute grounds for the **Insurer** to avoid any policy issued.

The undersigned hereby agrees, warrants, and represents that he or she is a duly authorized representative of the **Applicant**, and is fully authorized to answer and make statements and representations by and on behalf of the **Applicant**.

Applicant's Signature:	Date: D D M M Y Y Y Y
Title:	

Important Notices

This Policy is issued/insured by AIG Australia Limited (AIG), ABN 93 004 727 753 AFSL No

Sydney: Level 19, 2 Park Street, NSW 2000 (1300 030 886)
Melbourne: Level 13, 717 Bourke Street, VIC 3008 (1300 030 886)
Brisbane: Level 11, 120 Edward Street, QLD 4000 (1300 030 886)
Perth: Level 11, 108 St. George Terrace, WA 6000 (1300 030 886)

Duty of Disclosure

Before you enter into an insurance contract, you have a duty to tell us anything that you know, or could reasonably be expected to know, may affect our decision to insure you and on what terms.

You have this duty until we agree to insure you.

You have the same duty before you renew, extend, vary or reinstate an insurance contract.

You do not need to tell us anything that:

- reduces the risk we insure you for; or
- is common knowledge; or
- we know or should know as an insurer; or
- we waive your duty to tell us about.

Subject to the Cancellation General Provision, if you do not tell us anything you are required to, we may cancel your contract or reduce the amount we will pay you if you make a claim, or both.

If your failure to tell us is fraudulent, we may refuse to pay a claim and treat the contract as if it never existed.

Claims Made and Notified

Some coverage sections of *this policy contain claims-made and notified* insuring clauses. This means that those insuring clauses will only cover **Claims** first made against you during the **Policy Period** and notified to the **Insurer** as soon as practicable in the **Policy Period** or any applicable extended reporting period. This Policy may not provide cover for any **Claims** made against you if at any time prior to the commencement of this Policy you became aware of facts which might give rise to those claims being made against you.

Section 40(3) of the *Insurance Contracts Act 1984* provides that where you gave notice in writing to an insurer of facts that might give rise to a claim against you as soon as was reasonably practicable after you became aware of those facts but before insurance cover provided by an insurance contract expires, the insurer is not relieved of liability under the contract in respect of the claim, when made, by reason only that it was made after the expiration of the period of insurance cover provided by the contract.

This Policy excludes prior **Insured Events** (including but not limited to **Claims**) and circumstances as outlined in the "Prior Claims and Circumstances" Exclusion in Section 10 of the Policy Wording.

Privacy Notice

This notice sets out how AIG collects, uses and discloses personal information about:

- **you, if an individual; and**
- **other individuals you provide information about.**

Further information about our Privacy Policy is available at www.aig.com.au or by contacting us at australia.privacy.manager@aig.com or on 1300 030 886.

How We Collect Your Personal Information

AIG usually collects personal information from you or your agents.

AIG may also collect personal information from:

- our agents and service providers;
- other insurers;
- people who are involved in a claim or assist us in investigating or processing claims, including third parties claiming under your policy, witnesses and medical practitioners;
- third parties who may be arranging insurance cover for a group that you are a part of;
- providers of marketing lists and industry databases; and
- publically available sources.

Why We Collect Your Personal Information

AIG collects information necessary to:

- underwrite and administer your insurance cover;
- improve customer service and products and carry out research and analysis, including data analytics; and
- advise you of our and other products and services that may interest you.

You have a legal obligation under the Insurance Contracts Act 1984 to disclose certain information. Failure to disclose information required may result in AIG declining cover, cancelling your insurance cover or reducing the level of cover, or declining claims.

To Whom We Disclose Your Personal Information

In the course of underwriting and administering your policy we may disclose your information to:

- your or our agents, entities to which AIG is related, reinsurers, contractors or third party providers providing services related to the administration of your policy;
- banks and financial institutions for policy payments;
- your or our agents, assessors, third party administrators, emergency providers, retailers, medical providers, travel carriers, in the event of a claim;
- entities to which AIG is related and third party providers for data analytics functions;
- other entities to enable them to offer their products or services to you; and
- government, law enforcement, dispute resolution, statutory or regulatory bodies, or as required by law. AIG is likely to disclose information to some of these entities located overseas, including in the following countries: United States of America, Canada, Bermuda, United Kingdom, Ireland, Belgium, The Netherlands, Germany, France, Singapore, Malaysia, the Philippines, India, Hong Kong, New Zealand as well as any country in which you have a claim and such other countries as may be notified in our Privacy Policy from time to time. You may request not to receive direct marketing communications from AIG.

Access to Your Personal Information

Our Privacy Policy contains information about how you may access and seek correction of personal information we hold about you. In summary, you may gain access to your personal information by submitting a written request to AIG. In some circumstances permitted under the Privacy Act 1988, AIG may not permit access to your personal information. Circumstances where access may be denied include where it would have an unreasonable impact on the privacy of other individuals, or where it would be unlawful.

Complaints

Our Privacy Policy also contains information about how you may complain about a breach of the applicable privacy principles and how we will deal with such a complaint.

Consent

If applicable, your application includes a consent that you and any other individuals you provide information about consent to the collection, use and disclosure of personal information as set out in this notice.

Copyright

Code of Practice

The Insurer is a signatory to the General Insurance Code of Practice. This aims to raise the standards of practice and service in the insurance industry, improve the way that claims and complaints are handled and help people better understand how general insurance works. Information brochures on the Code are available upon request.

Dispute Resolution Process

We are committed to handling any complaints about our products or services efficiently and fairly.

If you have a complaint:

(i) contact your insurance intermediary and they may raise it with us;

(ii) if your complaint is not satisfactorily resolved you may request that your matter be reviewed by management by writing to:

The Compliance Manager
AIG Australia Limited
Level 13, 717 Bourke Street
Docklands VIC 3008

About AIG

American International Group, Inc is a leading global insurance organisation. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services the help businesses and individuals protect their assets, manage risks and provide for retirement security. American International Group, Inc common stock is list on the New York Stock Exchange.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products and services may not be available in all countries, and coverage is subject to actual policy language. Non-Insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insured are therefore not protected by such funds.

AIG

aig.com.au

American International Group, Inc. (AIG) is a leading global insurance organization. AIG member companies provide a wide range of property casualty insurance, life insurance, retirement solutions, and other financial services to customers in approximately 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference herein.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com.
All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries and jurisdictions, and coverage is subject to underwriting requirements and actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

Contact:

Head Office
NEW SOUTH WALES
Level 19, 2 Park Street
Sydney, NSW 2000, Australia

General customer service
Tel: +61 2 9240 1711

AUFLCEOSPBR20220203