Arch | Insurance

Arch Breach Cover
Questionnaire

Contents

Supplemental Forms

If any of the following apply to your organisation, please complete:

Pursuing Better Together®

Duty of Disclosure

Before any person or entity enters into an insurance policy with us, they have a duty under the *Insurance Contracts Act 1984* (Cth) to disclose to us every matter that they know, or could reasonably be expected to know, is relevant to our decision whether to accept the risk of the insurance and if so, on what terms.

They have the same duty to disclose those matters to us before they renew, extend, vary or reinstate the Policy.

The duty applies until the Policy is entered into, or where relevant, renewed, extended, varied or reinstated (Relevant Time). If anything changes between the time disclosures are made and the Relevant Time, the person/entity needs to tell us.

What we do not need to know

A person does not need to tell us about any matter that:

- diminishes our risk;
- is of common knowledge;
- we know or should know in our business as an insurer;
- we tell the person we do not need to know.

Who does the duty apply to?

The duty of disclosure applies in relation to everyone who is insured under the Policy.

What happens if the duty of disclosure is not complied with?

If the duty of disclosure is not complied with we may cancel the Policy and/or reduce our liability under the Policy in respect of a claim. If fraud is involved, we may treat the Policy as if it never existed and pay nothing.

UTMOST GOOD FAITH

The Policy is based on the utmost good faith requiring us and the proposer/Insured(s) (including third party beneficiaries after the Policy is entered into) to act towards each other with the utmost good faith in respect of any matter relating to the Policy. A failure to comply is a breach of the Insurance Contracts Act 1984 (Cth).

NOTICES

We will send all notices in relation to the Policy to:

- the Insured's nominated insurance intermediary until we receive written notice to the contrary from the Insured; or
- if there is no nominated intermediary, the Insured named in this Questionnaire, acting on behalf of all Insureds.

Please provide as much detail as possible when completing this application form.
This will help us provide a more prompt assessment of your cybersecurity posture.

Section 1 – Company Details

1.1 Insured:

1.2 Principle Address:

1.3 Country:

1.4 Core Web URLs:

1.5 Business Description:

i. Date Established:

ii. Primary Currency

1.6 Annual Revenues

i. Previous FY:

ii. Projected Current FY:

iii. Revenue % split by region: (eg Domestic, USA/Canada, Europe etc)

Region	%

iv. Where the organisation has separately operated divisions, please provide revenue split between each entity:

v. Approximate share of revenue attributable to:

B2B Trading

B2C Trading

Online Trading

1.7 Maximum number of unique individuals for whom any form of protected data is collected and stored:

1.8 Total number of records in the custody of the organisation:

i. Personally Identifiable Information (PII)

ii. Protected Health Information (PHI)

iii. Payment Card Information (PCI)

1.9 Number of employees:

1.10 Number of IT employees:

i. Number of employees with IT credentials:

1.11 Number of Cybersecurity Employees:

1.12 Annual IT budget:

1.13 Percentage of IT budget spent on security:

1.14 No. of external IP addresses:

Please use this box to provide any further information in relation to your company details:

Section 2 – Claims History

2.1 Within the past 5 years has the applicant:

- Had any network security incidents or data incidents that resulted in a material financial loss to the organisation? Y N
- Received any complaints, claims or regulatory action relating to allegations of unauthorised information disclosure, theft of information or breach of information security? Y N
- Been required to notify any individuals or entities of a breach of their information? Y N
- Received any extortion demand or threat relating to information systems? Y N
- Been the subject of any government action, regulatory investigation, or subpoena regarding any alleged violation of any privacy/data security law or regulation? Y N

- Experienced an unscheduled network outage, denial of service or substantial loss of IT functionality resulting in a material impact to operations? Y N
- Sustained any damage to property resulting from a cyber-attack? Y N
- Experienced phishing or wire fraud resulting in a financial loss or redirected payments? Y N
- Sustained any network security incident, information breach or outage caused by a 3rd party vendor (e.g., cloud vendors, IT consultants, payroll, data processing)? Y N
- Does the organisation, proposed for this insurance, have knowledge of any form of incident bulleted above that may give rise to a claim? Y N

2.2. If YES to any of in question 2.1, please describe the situation in detail below, including scope, loss and resulting action taken:

Please use this box to provide any further information in relation to your claims history:

Section 3 – Mergers, Acquisitions and Business Change

Please complete this section if your organisation is currently involved or has been involved in M&A or undergone significant business change in the past 5 years.

3.1. Describe in detail the procedures in place to ensure that information security standards are maintained in the event of Mergers & Acquisitions for all parties entities involved?

3.2. Has the organisation been involved in M&A in the past 24 months? Y N

i. If YES, provide further details including the current status of systems integration:

3.3. Is the organisation involved in or planning any M&A activity in the next 12 months Y N

i. If YES, please describe further details including milestone dates, IT/OT tasks, integration tasks, how the final IT/OT infrastructure will be structured, and any additional cyber security measures being undertaken.

3.5. Is the organisation planning any large scale changes in how it operates in the next 12 months? This includes but not limited to new business ventures, change to revenue generating model, new geographical footprint, significant new infrastructure, significant change to staff etc. Y N

i. If YES, please provide details of these changes:

Please use this box to provide any further information in relation to mergers, acquisitions and business change:

Section 4 – Governance

4.1 Do you comply with all applicable privacy and data regulations and legislation in all the jurisdictions under which the business operates? Y N

4.2 Is a dedicated Data Protection Officer or similar role employed? Y N

i. How are the responsibilities of this role delegated by region or operation?

4.3 Do you have a team dedicated to cyber security, separate from IT? Y N

4.4. Will the controls described in this application represent all entities covered by this insurance policy? Y N

4.5 Is central organisational policy applicable across all operations? Y N

4.6 Are information security controls 100% centrally managed? Y N

i. If not, describe the governance management model, how operations are federated and how you ensure the minimum level of compliance across all entities:

4.7 Do you perform cybersecurity risk assessments at least annually? Y N

i. If YES, describe the main risks identified in the last analysis and the action plan performed/planned

Please use this box to provide any further information in relation to governance:

Section 5 – Asset Management

5.1 Is there an inventory of hardware enterprise assets (including end-user devices, network devices, appliances, IoT devices, and servers) and this is updated at least annually? Y N

i. If yes, is this updated at least annually? Y N

ii. Confirm the percentage of hardware assets inventoried: %

iii. If the percentage is less than 100%, please provide some detail on the remaining assets.

5.2 Is there an inventory of software assets and is this updated at least annually? Y N

i. If yes, confirm the percentage of software assets inventoried: %

5.3 Is there an automated an inventory tool to continuously track, identify and manage enterprise assets? Y N

5.4 What is the current number of:

i. Endpoints

ii. Servers

Please use this box to provide any further information in relation to asset management:

Section 6 – Data Protection

6.1 Is there an inventory of all sensitive data? Y N

6.2 Have you established an overall data classification / categorisation scheme? Y N

i. If Yes, which of the following are included:

☐ Data Owner ☐ Storage Location ☐ Sensitivity ☐ Retention Limits ☐ Disposal Requirements ☐ Compliance Categories

6.3 Is the applicant's network segmented based on data classification? Y N

6.4 How do you utilise encryption to protect critical and sensitive information?

☐ At Rest ☐ In Transit ☐ Endpoints ☐ On Removable Media ☐ Mobile Devices ☐ Backups

i. Can you describe your data encryption policy and methodology

6.5 Does the applicant use Data Loss Prevention (DLP) tools? Choose all that apply:

☐ Network DLP ☐ Endpoint DLP ☐ Cloud DLP ☐ Data Discovery Tool

6.6 Do you accept card payments for goods or services? Y N

i. If YES, do you use a third party payment card processor?? Y N

6.7 Approximate number of payment card transactions processed per year:

6.8 If applicable, is the payment card processor (the applicant or third-party) PCI-DSS compliant? Y N N/A

i. If YES, what is the PCI DSS level: ☐ Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4

6.9 Is payment card data point-to-point encrypted or tokenised at all times? Y N N/A
(Payment card data never touches the network in plain text)

6.10 Do you use any externally exposed Managed File Transfer platforms? Y N

i. If YES, please provide further detail on this solution and security controls in place:

Please use this box to provide any further information in relation to data protection:

Section 7 – Identity and Access Security

7.1 Which tools are you using for directory services, identity provision (IdP), federation and rights management (e.g. Active Directory, Azure AD, Okta)?

7.2 Do you have an up-to-date inventory of all user and administrative accounts? Y N

i. How frequently are all active accounts reviewed?

7.3 Describe the access management and privilege revocation procedures when an employee leaves the company:

7.4 Does the organisation have a Privileged Access Management solution (PAM) Y N

i. If YES, provide details of what tool is used and the capabilities implemented (e.g. CyberArk, MFA, Check-in/out, Monitoring etc)

ii. Are **all** privileged service accounts managed in the PAM tool? Y N

7.5 Where no PAM solution exists, or for privileged accounts outside of the PAM tool, describe the privileged access management process, the exceptions and any security controls implemented.

7.6 In regard to Domain Administrator Accounts select all that apply:

- ☐ Are separate from everyday account (only used for admin tasks)
- ☐ Require MFA
- ☐ Can only be accessed from dedicated Privilege Access Workstations
- ☐ Cannot access email
- ☐ Cannot access the internet
- ☐ Credentials stored in a password safe
- ☐ Unique complex passwords. Minimum number of characters

7.7 Do you have an inventory of all privileged service accounts and is this updated regularly? Y N

i. Provide details on how privileged service accounts are managed (Tiering, Passwords, Monitoring etc):

7.8 Do you deny interactive logon for all service accounts? Y N

i. If NO, is specific alerting configured when a service account is logged on interactively? Y N

7.9 Do any users have access to local administrator rights on their workstation? Y N

i. If YES, please provide detail on who has local administrator rights, the approval process and any additional security controls in place:

7.10 Are local administrator credentials stored in either a PAM, LAPS or similar Endpoint Privilege Management solution? Y N

i. Are all local administrator passwords different across all domain-attached systems? Y N

7.11 What is the number of active accounts for:

i. Number of Domain Administrator Accounts:

ii. Number of Privileged Service Accounts:

7.12 Provide the number of users with administrative access to servers/workstations including those with unique administrative accounts separate from their everyday user accounts.
Do not include users who must "check out" credentials for administrative access:

7.13 Is MFA required for all remote access to the corporate network (employees and vendors)? Y N

i. If MFA is not required for all and/or there are exceptions, describe this in detail and any compensating controls in place.

7.14 What forms of MFA are used for remote access to the network? (e.g. SMS, Authenticator App, Physical Key)

7.15 Do you employ MFA number matching or similar to mitigate the risk of MFA fatigue? Y N N/A

7.16 Do you have a documented process that is strictly enforced when adding or reseting an individuals MFA access? Y N

i. If Yes, do accounts require the user to be physically identified or verified by another employee before resetting MFA access?

7.17 Is MFA required for access to corporate email on all devices unless on premises? Y N

7.18. Is Remote Desktop Protocol (RDP) or other similar remote desktop applications allowed on externally exposed systems? Y N

i. If YES, provide details on how these are used and what protections are in place (e.g. VPN, MFA):

Please use this box to provide any further information in relation to identity and access security.

Section 8 – Vulnerability Management

8.1 Do you have a defined patch management policy in place? Y N

8.2 Please give an overview of the vulnerability and patch management process including assessment of risk and categorisation.

ii. What is the documented target time to deploy the most critical patches?

iii. What is the compliance rate with your own standards for deploying the most important patches in the most recent completed quarter: %

8.3 Do you have a vulnerability scanning tool which identifies and manages vulnerabilities? Y N

i. If YES, what percentage of IT assets are covered by vulnerability scans? %

ii. How frequently are vulnerability scans conducted?

☐ Daily ☐ Weekly ☐ Monthly ☐ Longer

8.4 Please confirm if there are legacy/unsupported/end-of-life systems in the IT (not OT) environment. Y N

If YES:

i. Describe what function these systems perform, whether they sit in the same network segment as sensitive data and any plans to update them in the future.

ii. Describe any additional security controls in place to protect these systems (i.e., network isolation, virtual patching, extended support)

iii. Are any of these devices directly exposed to the internet? Y N

iv. Total number of EOL devices:

Please use this box to provide any further information in relation to vulnerability management:

Section 9 – Logging, Monitoring, and Response

9.1 Is there 24/7 monitoring of security operations? Y N

i. Provide details of the Security Operations Center (SOC), what products are monitored (EDR, SIEM etc) and what authority they have to remediate security events:

ii. What is the average time to triage and react to security incidents in the past year? Hours

9.2 Is a Security Information and Event Monitoring (SIEM) tool or similar used to correlate the output of multiple security tools? Y N

i. Are domain controller logs ingested by the SIEM? Y N

ii. What other sources of information does the SIEM ingest?

iii. How long are logs maintained? Days

iv. What percentage of "Vital Assets" are logged and monitored in the SIEM solution: %

v. If the percentage is lower than the 100%, describe the nature of the remaining % and any other monitoring in place.

Please use this box to provide any further information in relation to logging, monitoring and response:

Section 10 – Endpoint Security

10.1 Please provide the approximate number of:

i. Workstations:

ii. Servers:

10.2. Provide the full name of endpoint protection platforms in use

i. What percentage of endpoints, including workstations, laptops, and servers are protected by this tool: %

ii. If less than 100%, provide details of the devices unprotected and the compensating measures/controls in place:

10.3 Is a host based IPS/IDS system deployed? Y N

10.4 Do you have software tools to monitor for data loss (DLP)? Y N

i. If YES, is this tool in configured to block suspicious traffic? Y N

10.5 Are hardened baseline configurations used across devices? Y N

i. If YES, what percentage of devices are deployed with these baselines? %

10.6 Are PowerShell best practices implemented as outlined in the Environment Recommendations by Microsoft? Y N

10.7 Do you allow Bring Your Own Device? Y N

i. If YES, do you have specific policy governing the usage of those devices? Y N

ii. How do you ensure the security of these devices?

Please use this box to provide any further information in relation to endpoint security:

Section 11 – Email and Internet Security

11.1 Please provide details of email platforms in use (include license versions if applicable):

11.2 If you use an additional email monitoring/filtering solution (i.e. MS ATP, Mimecast, Proofpoint) please provide details of the product:

11.3 Which of the following is implemented:

i. Blocking of malicious links, attachments, and suspicious file types Y N

ii. Blocking based on the message content or sender attributes Y N

iii. Evaluation of attachments in a sandbox Y N

iv. Email specific data loss prevention solution (DLP) Y N

11.4 Do you have a DNS web filtering tool that prevents access to newly registered/uncategorised domains and known suspicious or malicious websites? Y N

11.5. Are any of the following enforced on incoming emails: ☐ SPF ☐ DKIM ☐ DMARC

11.6. Do you allow access to web-based email? Y N

i. If YES is MFA enforced? Y N

11.7 Are external emails tagged as originating outside the company? Y N

11.8 Do you disable macros in office software by default or allow only pre-approved macros to run? Y N

i. If YES, are users able to enable macros on documents opened from email? Y N

11.9 Do you have a Web Security Platform in place? Y N

i. If YES, select from the following, which features are implemented:

☐ Prevent access to known malicious sites ☐ Inspect file downloads
☐ Enforce acceptable use policies ☐ Detect compromised device communications

11.10 Are users allowed to access personal email and social media on their corporate workstation? Y N

Please use this box to provide any further information in relation to email and internet security:

Section 12 – Network

12.1 Is your network is segmented? Y N

i. If YES, describe how the network is segmented and any technology utilised the achieve this:

12.2 Do you employ micro-segmentation technology? Y N

12.3 Are firewalls in place at all network perimeter points? Y N

i. Are firewall rules and configurations are reviewed at least quarterly Y N

12.4 Are web application firewalls (WAF) in place protecting all externally exposed assets? Y N

12.5 Have you implemented any DDoS protections, if so provide information on the solutions used?

12.6 Do you use WiFi or another wireless technology in the IT network? Y N

i. If YES, please provide details of what technology is used, what it's connected to and what security measures are in place:

12.7 Do you use a Network Access Control solution to restrict unauthorised devices from accessing the network? Y N

12.8 Do you have a network-based intrusion prevention system (NIPS)? Y N

12.9 Have you implemented a Zero Trust Network Access (ZTNA) solution? Y N

Please use this box to provide any further information in relation to network security:

Section 13 – Planning, Business Continuity and Recovery

13.1 Which of the following plans are in place addressing IT events:

☐ Disaster Recovery Plan ☐ Incident Response Plan ☐ Business Continuity Plan

i. Are all entities proposed for cover under this insurance included in the scope of these plans? Y N

ii. What is the documented Recovery Time Objective (RTO) for critical systems? Hours

iii. Are copies of these documents kept offline and accessible in the event of a network outage? Y N

13.2 Are these plans tested on an annual basis? Y N

i. If YES, have all recommendations resulting from the tests been implemented? Y N

13.3 Has a cybersecurity tabletop exercise been conducted in the past 12 months? Y N

i. Did this include a ransomware event? Y N

13.4 Has the applicant developed specific playbooks for incidents such as ransomware, business email compromise, fund transfer fraud? Y N

13.5 Have you established a process for communicating with critical contacts in the event of ransomware rendering your email platform inaccessible? (e.g. Out of band email accounts) Y N

13.6 Please provide some additional detail regarding the applicant's business continuity and incident response program. Include how often plans are tested and reviewed, lessons learned from previous exercises and future plans.

13.7 How often does the applicant take backups of critical applications and data?

i. How long are these back-ups retained?

13.8 Select from the following all that apply to the your backup solution

☐ Immutable ☐ Offsite ☐ Offline ☐ Encrypted ☐ Physical Tapes ☐ Cloud ☐ On-Prem
☐ Requires MFA for access ☐ Separate credentials required to access ☐ Network Segmented

i. If backups are encrypted do you maintain an accessible decryption key offline? Y N

13.9 Are backups isolated and separate from the primary corporate domain? Y N

13.10 Are you able to ensure the back-up is free from malware before restoration? Y N

13.11 How often is an individual device test restoration conducted from backups?

13.12 Have you ran tabletop scenarios with the teams that manage backups, on how you would restore your entire critical infrastructure in the event of corporate IT systems being rendered inaccessible? Y N

i. What is the time taken to fully restore critical systems?

ii. What is the time taken to fully restore all systems?

13.13 Do you operate a cold/warm/hot backup site? Y N

i. If YES please provide details, including how often failover is tested:

13.14 Please use this box to provide further details on the business continuity program (Include details on specific tools and vendors used):

Please use this box to provide any further information in relation to planning, business continuity and recovery:

Section 14 – Staff Training and Awareness

14.1 Do you provide security awareness training to employees at least annually? Y N

i. If Yes, is this training adapted by role to highlight specific Cyber risks they might face in that position? (e.g. Help Desk staff trained on dangers of password resets or payment staff on email compromise) Y N

14.2 Do you conduct simulated phishing attacks to all staff with access to corporate email?

☐ Annually ☐ Quarterly ☐ Monthly ☐ No

i. If YES, the last recorded click rate was: ☐ <5% ☐ <15% ☐ >15%

ii. Is additional training enforced for those who click the phishing link? Y N

14.3 Do you provide security awareness to employees related to the use of AI tools and applications, to prevent the leakage of confidential and sensitive information? Y N

14.4 Are employees responsible for distributing company funds provided with additional training to detect business email compromise, phishing and other fraud techniques? Y N

Please use this box to provide any further information in relation to staff training and awareness:

Section 15 – Penetration Testing

15.1 Do you have a penetration testing programme in place? Y N

15.2 Have your networks been externally penetration tested within the past year? Y N

15.3 Have your networks been internally penetration tested within the past year? Y N

15.4 Do you conduct web application penetration testing? Y N

15.5 Have all vulnerabilities and threats discovered by all recent penetration test been remediated? Y N

15.6 Please use the box provided to describe the details of the programme including scope covered, vendors used, frequency, the remediation undertaken after the most recent tests and any critical recommendations that have not yet been implemented.

Section 16 – Third Party and Vendor Management

16.1 Do you audit vendors to ensure they are complaint with required security standards prior to and during contract period? Y N

16.2 Describe the due-diligence process undertaken for onboarding new vendors

i. Additionally describe the process for reviewing and updating vendor's access rights, contracts and that they continue to satisfy data security and privacy requirements?

16.3 How is vendor access to your network restricted? (Monitoring, Time restrictions, MFA, credentials provision etc)

16.4 Are vendors contractually required to indemnify you if they contribute to a data breach? Y N

16.5 Do you maintain an inventory of all third parties that have access to or process your organisations information? Y N

16.6 Please identify all vendors that have access to or help manage your systems (e.g. Cloud providers, managed security services, ISPs, data processors etc):

Name of Vendor	Service Provided

Please use this box to provide any further information in relation to third party and vendor management:

Section 17 – Trending

17.1 Does the organisation use any Artificial Intelligence that interact with customers or have access to sensitive data? Y N

i. If Yes, please provide further detail.

17.2 Can you confirm:

i. No systems on the network are vulnerable to the Apache Log4J CVE-2021-44228 Y N N/A

ii. No systems on the network are running vulnerable versions of the MOVEit file transfer software Y N N/A

iii. You have no Citrix Netscaler instances vulnerable to CVE-2023-3519 Y N N/A

iv. You have never had an external instance of WS_FTP Server vulnerable to CVE-2023-4044 Y N N/A

17.3 Do you keep your cyber insurance policy documentation offline, not accessible from your corporate network? (This is related to threat actors targeting it to aid their extortion attempts) Y N

17.4 Do you rely on cellular technology (GSM, UMTS, LTE, 5G) for any network directly connected to critical systems? Y N

Please use this box to provide any further information in relation to trending:

Section 18 – Future Roadmap

18.1 List and describe any security initiatives/projects related to information security that are planned for completion within the next 12 months

18.2 List and describe any fundamental changes to the IT or OT infrastructure planned within the next 12 months

IMPORTANT NOTICE CONCERNING DISCLOSURE

You and anyone representing you has a duty to provide a fair presentation of the risks to be insured, before the commencement of the cover and the agreement of any variations or renewals. A fair presentation is one which, in a reasonably clear and accessible manner, provides the material facts relating to the risk which you, your senior management and or persons responsible for arranging the Policy know or ought to know following a reasonable search. Failing that, the information You provide must be sufficient to warn us that additional enquiries must be made to fully understand the risk. The information provided must be substantially correct, complete and provided in good faith. Should You be in doubt as to whether information is accurate or material, then You must disclose the information to Us and identify any information that may not be accurate. Inaccurate or incomplete information may result in Your Policy being void from its start date and /or Your claim not being paid.

Signature: Date: (DD/MM/YYYY)

Name: Position:

Supplemental 1 – Operational Technology

Responses to this questionnaire should be based on the applicant's Operational Technology (OT) environment. For this application, please consider the OT environment as the software and hardware used to connect, manage, secure and control physical processes, devices, and infrastructure. OT includes but is not limited to technologies such as supervisory control and data acquisition (SCADA), programmable logic controllers (PLCs), distributed control systems (DCSs), physical devices, remote terminal units (RTUs) and human-machine interfaces (HMIs).

Please continue to complete this section if you have Operational Technology (OT) covered by the scope of this insurance application. Please provide as much detail as possible to allow us to establish a clear picture of your OT environment.

Section 1 – Overview

1.1 Please provide an overview of the operational technology used within your organisation. If you require more space, please use section 13.

1.2 Do you have a specific cybersecurity policy for the OT systems, or it is specifically included in the global cybersecurity policy? Y N

1.3 Are cybersecurity personnel employed specifically for OT? Y N

i. If NO, is there IT cyber security personnel whose role specifies OT security tasks? Y N

1.4 In the event of an outage at one facility, is spare capacity available at other facilities to make up for the outage? Y N

i. If YES, briefly describe the process and how long it would take to transfer production to another facility:

1.5 Are any products produced in one single location without the ability to move production to another facility. Y N

i. If YES, what % of sales does this product account for? %

1.6 How many days could stock levels meet demand in the event of an OT incident or system failure?

1.7 If the IT environment was to experience an outage how would this affect the OT environment?

Section 2 – Assets

2.1 Do you maintain an up-to-date inventory of the assets connected to the OT network? Y N

i. If YES, what is the percentage covered: %

2.2 Is an up-to-date list of software including versions for all devices maintained? Y N

2.3 Is a formal process in place for implementing any new system or device onto the OT network? Y N

2.4 Do you utilise automatic asset discovery and inventory tools to detect shadow OT devices? Y N

Please use this box to provide any further information on OT asset management:

Section 3 – Identity and Access Management

3.1 Do you permit employee remote access to the OT environment? Y N

i. If YES, do you enforce MFA for all employee remote access? Y N

3.2 Do you permit third parties to remote access the OT environment? Y N

i. If YES, what security measures are in place? (MFA, Time-Based access, additional monitoring etc)

ii. Do you prohibit vendors installing their own method of remote access into the OT?
(This refers to vendors installing modems into equipment for direct access and monitoring) Y N

3.3 Please describe in detail how all remote connections to the OT environment are established, managed and protected. (Jumpboxes, gateways, DMZ, VPN, MFA etc). Include all connections not originating physically on site.

3.4 If used, is there a separate active directory domain for the OT environment with no trust relationship to IT? Y N N/A

3.5 Does OT access require separate unique credentials (separate from their IT user credentials)? Y N

3.6 Is it standard policy to change or remove default credentials from OT equipment? Y N

Please use this box to provide further detail to any answers you have provided in relation to OT Identity and Access Management:

Section 4 – Vulnerability Management

4.1 Are there End of Life systems in the OT infrastructure? Y N

i. If YES, please describe what function these systems perform and any additional security controls in place to protect them (i.e., network isolation, virtual patching, extended support)

4.2 Does the organisation use IOT devices? Y N

i. If YES, are updates and patching of these formally managed and conducted on a regular basis? Y N

4.3 Is there a formal process for patching OT systems? Y N

i. Please describe how patches are deployed in the OT environment and the frequency of patching critical systems:

ii. Are automated tools utilised to ensure systems are running the most recent security updates? Y N

4.4 Is SMB v.1 enabled anywhere in the OT environment? Y N

Please use this box to provide further detail to any answers you have provided in relation to OT Vulnerability Management:

Section 5 – Logging, Monitoring and Response

5.1 Do logs from OT equipment feed into a SIEM? Y N

i. If YES, what % of devices are covered? %

5.2 Do you employ any tools to centrally monitor ICS/SCADA devices? Y N

i. Are these tools capable of alerting for unusual activity and device behaviour? Y N

5.3 Does the OT environment have 24/7 monitoring of security operations (managed internally, by a third party or hybrid). Y N

i. Is this SOC authorised and able to respond to OT security incidents? Y N

Please use this box to provide further detail on your OT logging, monitoring and response capabilities:

Section 6 – Server and Endpoint Security

6.1 Is an endpoint protection platform or antivirus installed on servers and endpoints including human machine interfaces where feasible? Y N

i. If YES, what is the full name of this tool?

ii. If YES, what % of supported devices are covered? %
(Do not include incompatible devices e.g. sensors/actuators etc)

iii. How do you update this platform?

6.2 Do you allow removable media (e.g. USB Stick) access in the OT environment? Y N

i. If YES, are there processes in place to ensure these are free from malware prior to use? Y N

Please use this box to provide further detail on how your OT endpoint devices are protected:

Section 7 – Email and Internet

7.1 Are users able to access email from devices inside the OT environment? Y N

7.2 Is there Internet access from within the OT environment? Y N

i. If Yes, please provide details on what systems have Internet access, how the Internet traffic is routed (proxies etc) and what protections are in place around this access:

Please use this box to provide further detail on Email and Internet:

Section 8 – Network Security

8.1 Network Segmentation:

i. Is the OT environment segregated from the corporate corporate IT networks? Y N

ii. Where there are multiple OT sites are they segmented from each other? Y N N/A

iii. Please provide details on all OT network segmentation including the technology used (VLANs, Gateways, Firewalls etc):

8.2 Are network-based intrusion prevention/detection systems deployed in the OT network? Y N

8.3. Do you use WiFi or another wireless technology in the OT network? Y N

i. If YES, please provide details of what technology is used, what it is connected to and what security measures are in place:

Please use this box to provide any further information that might be relevant to network security:

Section 9 – Planning, Backups and Recovery

9.1 Does the OT environment have Business Continuity and Disaster Recovery plans in place? Y N

i. Do these plans specifically include restoration in the event of a ransomware attack? Y N

ii. Please provide a short narrative on the OT business continuity process in the event of a system failure:

9.2 Have you conducted an OT specific tabletop exercise for cyber incidents in the past year? Y N

9.3 Select from the following all that apply to the Applicants OT backup solution

☐ Immutable ☐ Onsite ☐ Offsite ☐ Offline ☐ Encrypted ☐ Physical Tapes
☐ Cloud ☐ On-Prem ☐ Removeable Media

i. Please provide detail on the process for backing up critical OT systems (Automation, frequency etc):

ii. Please describe how restoration tests are managed in the OT environment and how often they are conducted:

Please use this box to provide any further information on your OT business continuity planning, backups and recovery:

Section 10 – Penetration Testing

10.1 What penetration testing is conducted in the OT environment? (Include the scope of systems covered, the frequency, red/blue teaming etc).

i. Do they have specialist experience in ICS device penetration testing? Y N

Please use this box to provide any further information on Penetration Testing:

Section 11 – Third Party Management

11.1 Do you conduct security audits of current suppliers and due diligence prior to contracting new suppliers? Y N

11.2 Do you rely on third parties to manage any systems or applications in the OT domain? Y N

i If Yes, please provide information on what third parties are used and the services they provide. Include any specific security measures in place for each vendor.

Section 12 – Additional OT Information

12.1 If you can provide any further detail to help us understand the nature of your OT environment, systems or controls you have implemented please use the box provided. Also include any major changes/projects underway in relation to OT:

DECLARATION

I declare that I have made all necessary inquiries into the accuracy of the responses given in this Questionnaire and confirm that the statements and particulars provided in it are true and complete and that no material facts have been omitted, misstated or suppressed. I agree that if any of the information given by me or the proposer, alters between the date of this Questionnaire and the inception date of the insurance to which it relates, I will give immediate notice thereof to the insurer.

I acknowledge receipt of the Important Notices contained in this Questionnaire and that I have read and understood the content of them, including the duty to take reasonable care not to make a misrepresentation. I agree to the terms of the Privacy Statement. I also acknowledge that the insurance will be provided in whole or in part by overseas insurers.

I confirm that I am legally authorised by the proposer and its partners/principals/directors (if applicable) to complete this Questionnaire and to accept the quotation terms for this insurance on their behalf.

Signature: Date: (DD/MM/YYYY)

Name: Position:

How to contact us

Melbourne

Suite 11.02, Level 11, 360 Collins Street,
Melbourne VIC 3000

P (03) 9629 5444
F (03) 9629 1854

Sydney

Level 10, 155 Clarence Street
Sydney NSW 2000

P (02) 8284 8410
F (02) 8088 1024

Email: **info@archinsurance.com.au**

Privacy Statement

Unless the context otherwise provides, in this section 'we', 'our' or 'us' means Certain Underwriters at Lloyd's and Arch Underwriting at Lloyd's (Australia) Pty Ltd and their related entities.

Personal information is essentially any information or an opinion about an identified individual, or an individual who is reasonably identifiable. See the Privacy Act 1988 (Cth) (the Act) for full details of what constitutes personal information.

This privacy notice details how we collect, disclose and handle personal information.

Why we collect your personal information

We collect personal information (including sensitive information) so we can:

- identify you and conduct necessary checks;
- determine what service or products we can provide to you e.g. offer our insurance products;
- issue, manage and administer services and products provided to you or others, including claims investigation, handling and settlement;
- improve our services and products, e.g. training and development of our representatives, product and service research and data analysis and business strategy development.

What happens if you don't give us your personal information?

If you choose not to provide us with the information we have requested, we may not be able to provide you with our services or products or properly manage and administer services and products provided to you or others.

How we collect your personal information

Collection can take place through websites (from data input directly or through cookies and other web analytic tools), email, by telephone or in writing.

We collect it directly from you unless you have consented to collection from someone other than you, it is unreasonable or impracticable for us to do so, or the law permits us to.

If you provide us with personal information about another person, you must only do so with their consent and agree to make them aware of this privacy notice.

Who we disclose your personal information to

We share your personal information with third parties for the collection purposes noted above.

The third parties include: our related companies and our representatives who provide services for us, other insurers and reinsurers, our claim management partner(s), your agents, our legal, accounting and other professional advisers, data warehouses and consultants, investigators, loss assessors and adjusters, other parties we may be able to claim or recover against, and anyone either of us appoint to review and handle complaints or disputes and any other parties where permitted or required by law.

We may need to disclose information to persons located overseas who will most likely be located in the United Kingdom. Who they are may change from time to time. You can contact us for details or refer to our Privacy Policy available at our website www.archinsurance.com.au.

In some cases we may not be able to take reasonable steps to ensure they do not breach the Privacy Act and they may not be subject to the same level of protection or obligations that are offered by the Act. By proceeding to acquire our services and products you agree that you cannot seek redress under the Act or against us (to the extent permitted by law) and may not be able to seek redress overseas.

More information, access, correction or complaints

For more information about our privacy practices including how we collect, use or disclose information, how to access or seek correction to your information or how to complain in relation to a breach of the Australian Privacy Principles and how such a complaint will be handled, please refer to our Privacy Policy. It is available at our website www.archinsurance.com.au or by contacting us on (02) 8284 8400 EST 9am-5pm, Monday-Friday.

Privacy complaints: We have established a Privacy Complaints Handling Procedure to deal with any complaints you may have about how we have collected, used or managed your personal information. If you would like to make a complaint, please contact:

The Privacy Officer,
Arch Underwriting at Lloyd's (Australia) Pty Ltd,
Level 10, 155 Clarence Street, Sydney NSW 2000

or email complaints@archinsurance.com.au

Your complaint will be taken seriously and investigated thoroughly.

If you are not satisfied with our final decision, you can direct your complaint to the Federal Privacy Commissioner either on 1300 363 992 (for the cost of a local call anywhere in Australia) or by mail to GPO Box 5218, Sydney NSW 2001.

Your Choices: By providing us with personal information, you and any person you provide personal information for, consent to this use and these disclosures unless you tell us otherwise. If you wish to withdraw your consent, including for things such as receiving information on products and offers by us, or persons we have an association with, please contact us.

Arch Underwriting at Lloyd's (Australia) Pty Ltd archinsurance.com.au
ABN 27 139 250 605 AFSL 426746

Sydney: Level 10, 155 Clarence Street, Sydney NSW 2000 | P: +61 2 8284 8400 F: +61 2 8088 1024
Melbourne: Suite 11.02, Level 11, 360 Collins Street, Melbourne VIC 3000 | P: +61 3 9629 5444 F: +61 3 9629 1854

©2024 Arch Underwriting at Lloyd's (Australia) Pty Ltd. All rights reserved.