beazley

Operational Technology Supplemental Application

The purpose of this Application is to assess your Operational Technology (OT) exposure, security, and controls. For purposes of this Application, we define OT as the practices and technology that monitor and control industrial process assets and manufacturing equipment, as well as those systems that sustain the environment for these systems.

OT includes but is not limited to technologies such as supervisory control and data acquisition (SCADA) software, programmable logic controllers (PLCs), physical plant equipment, remote terminal units (RTUs), human-machine interfaces (HMIs), embedded computing technologies, remote industrial software and hardware, and systems for monitoring and controlling any of the foregoing.

The Applicant's responses to this supplemental application apply to all entities to be covered by the insurance sought, including all Subsidiaries as defined under the Policy. If any of your responses require clarification or additional information to be complete, please include commentary in the last section below, Other Cybersecurity Controls & Preventative Measures.

Overview of Security Controls

1. Do you have an OT security policy that includes cybersecurity? □ Yes □ No

2. a. Have you conducted, within the past **two years**, a cybersecurity incident tabletop exercise that includes cyber threats to OT? □ Yes □ No

   b. If yes to a., did that tabletop exercise include the threat from ransomware? □ Yes □ No

3. Do you maintain a complete and up to date centrally held inventory of your OT assets? □ Yes □ No

For applicants >$/£/€500m in revenue, please answer the following additional questions:

4. a. Do you employ individual(s) whose primary responsibility is OT cybersecurity? □ Yes □ No

   b. If yes to a., are they located within the IT Security organization? □ Yes □ No

   c. If yes to a., are they located within the Engineering/Operational Support organization? □ Yes □ No

5. Do you have a separate security budget for your OT environment? □ Yes □ No

Internal Security Controls

6. a. Is your OT environment segmented from your **Information Technology (IT)** environment(s)? □ Yes □ No

   b. If yes to a., how is the segmentation implemented? Choose all that apply.

   i. □ Firewalls ii. □ Unidirectional Security Gateways iii. □ VLANs iv. □ DMZs

7. a. Is your OT environment segmented from the **internet**? □ Yes □ No

   b. If yes to a., how is the segmentation implemented? Choose all that apply.

   i. □ Firewalls ii. □ Unidirectional Security Gateways iii. □ VLANs iv. □ DMZs

8. a. Do you permit employees remote access to your OT environment? □ Yes □ No

   b. If yes to a., do you enforce multi-factor authentication (MFA) for employee remote access to your OT environment? □ Yes □ No

   c. If yes to a., do you require employees to have separate accounts? (i.e., employees do not share accounts) □ Yes □ No

9. a. Do you permit third party remote access to your OT environment? □ Yes □ No

   b. If yes to a., do you enforce MFA for third-party remote access to your OT environment? □ Yes □ No

10. Do you have a defined process for identifying OT devices with critical cybersecurity vulnerabilities and patching or updating those devices? □ Yes □ No

    For OT devices with critical cybersecurity vulnerabilities that can't be patched or updated, please describe other compensating controls that you have in place to prevent exploitation of these devices:

For applicants >$/£/€500m in revenue, please answer the following additional questions:

11. How do you assess and monitor security in your OT environment? Choose all that apply.

    a. □ Risk assessments (at least annually)

    b. □ Penetration testing (at least annually)

       i. □ Across whole OT environment

       ii. □ Specific systems only

       iii. □ Specific vulnerabilities only

       iv. □ Red team/blue team exercise

    c. □ Intrusion detection and prevention system

    d. □ Endpoint detection and response (on supported workstations, servers, and endpoints)

    e. □ Endpoint protection platform (on supported workstations, servers, and endpoints)

12. Do you have any OT assets exposed directly to the Internet? □ Yes □ No

13. For third party and remote access to your OT, do you have any of the following controls? Choose all that apply.

    a. □ Governance policy for remote and third-party access

    b. □ Access to OT is monitored and logged

    c. □ Access to OT is time limited and closed off after each session

    d. □ Access to the OT network goes via the IT infrastructure

14. Does your OT security monitoring feed into a Security Operations Center? □ Yes □ No

15. Does your OT environment contain devices that their manufacturer considers "end of life" or that are no longer supported with security patches or updates? □ Yes □ No

If yes, please use the space under "Other Cybersecurity Controls & Preventative Measures" to describe what you do to prevent these devices from being exploited.

Backup & Recovery

16. Do you maintain backups – at least monthly or when significant process changes are made – of your OT environment? □ Yes □ No

17. a. Do you have a Business Contingency Plan (BCP) created or updated in the past **two years** that involves recovery from an OT cybersecurity event? □ Yes □ No

b. If yes, does your plan include restoring your OT environment in the event of a ransomware attack? □ Yes □ No

For applicants >$/£/€500m in revenue, please answer the following additional questions:

18. Do your backups include the configuration of non-Windows-based devices? □ Yes □ No

19. Are your backups maintained offline or on a separate network from your OT? □ Yes □ No

20. In the past year, have you successfully tested the ability to recover your OT environment from backups? □ Yes □ No

21. Do you have fallback process to allow your OT environment to operate if your IT environment is compromised, shut down, or disconnected for an indefinite period of time? □ Yes □ No

22. Do you have defined investigative procedures in place to contain, eradicate, and determine the root cause of a cyber incident in your OT environment? □ Yes □ No

For **manufacturing** applicants with >$/£/€500m in revenue, please answer the following additional questions:

23. On average, how much stock do you maintain on-hand that would continue to be available if production were halted?

□ ≤1 day □ >1 day but ≤7 days □ >7 days but ≤14 days □ >14 days

24. If you had an OT outage at one production facility, do you have capacity at other production facilities that could make up the shortfall?

□ Yes, for all products □ Yes, for most products □ Yes, for some products □ No

Other Cybersecurity Controls & Preventative Measures

Please use the space below to clarify any answers above that may be incomplete or require additional detail. Please also describe any additional steps your organization takes to detect, prevent, and recover from ransomware attacks (e.g., segmentation of your network, additional software security controls, external security services, etc.) in your OT environment.

Digital signature required below [click the red tab to create a digital ID or import an existing digital ID]:

Signed:

Print Name:

Title:

Company:

Date: