Aanvullende vragen met betrekking tot operationele technologieën (OT), met inbegrip van maar niet beperkt tot Industrial Control Systemen (ICS), Distributed Control Systemen (DCS) en Internet of Things (IoT)

U bent voor de aanvraag van Hiscox' Cyber & Data Risks verzekering alleen verplicht deze aanvullende vragen te beantwoorden indien dergelijke technologieën in gebruik zijn.

1. Heeft u de volgende beschermende maatregelen genomen om de toegang tot uw OT-netwerken en -systemen op afstand te beveiligen?
   a) Toegang op afstand is niet mogelijk ☐ ja ☐ nee
   b) Er worden altijd beveiligde VPN-verbindingen gebruikt wanneer men op afstand inlogt op het bedrijfsnetwerk ☐ ja ☐ nee
   c) Twee- of multi factor authenticatie* is altijd vereist voor toegang op afstand ☐ ja ☐ nee
   d) Toegang op afstand wordt gecontroleerd en is tijdelijk van aard (de toegang verloopt bijvoorbeeld op basis van tijd) ☐ ja ☐ nee
   e) Anders (leg uit):

2. Welke maatregelen zijn van toepassing op de patching van uw OT?
   a) OT worden gepatcht binnen 30 dagen na afgifte van updates door de fabrikant ☐ ja ☐ nee
   b) OT vertrouwen op legacy software/systemen en worden niet langer ondersteund door de fabrikant ☐ ja ☐ nee
   c) Er bestaat een gedocumenteerd proces voor de implementatie van updates, patches en nieuwe code - inclusief het testen van patches in een niet-productieomgeving voordat ze ergens op het OT-netwerk worden ingezet ☐ ja ☐ nee

3. Zijn er eindpuntbeveiligingsoplossingen toegepast op OT-apparaten en -systemen?

   ☐ Op alle OT-apparaten en -systemen
   ☐ Op sommige OT-apparaten en -systemen
   ☐ Op geen enkel OT-apparaat of -systeem

   Geef het type eindpuntoplossing(en) aan dat in gebruik is (zijn):

4. Bestaat er segmentatie tussen uw IT- en OT-netwerken? ☐ ja ☐ nee

   Zo ja, hoe wordt dit bereikt?
   Indien bijvoorbeeld alleen Egress Data Transfer is toegestaan tussen uw OT en IT netwerken, geef dit dan ook aan.

* Naast het invoeren van een gebruikersnaam en wachtwoord, heeft de gebruiker een tweede factor nodig om in te loggen. Bijvoorbeeld in de vorm van een code die per sms naar de mobiele telefoon wordt toegestuurd.

5. Hoe worden uw IT- en OT-netwerken beheerd?
   a) Dezelfde beheerders zijn verantwoordelijk voor zowel het IT- als het OT-netwerk ☐ ja ☐ nee
   b) De IT- en OT-netwerken hebben hun eigen beheerders ☐ ja ☐ nee
   c) Anders (leg uit):

6. Indien verschillende beheerders verantwoordelijk zijn voor uw IT- en OT-netwerken, vul dan de volgende vraag in: met betrekking tot de grens tussen uw IT- en OT-netwerken, geef aan wie verantwoordelijk is voor het volgende

Controle van firewalls regels en beleid	☐ IT admins	☐ OT admins
Controle van de gebruikersadministratie	☐ IT admins	☐ OT admins
Audit van firewall management activiteiten	☐ IT admins	☐ OT admins
Onderhoud, inclusief patchen	☐ IT admins	☐ OT admins

7. Bestaat er een segmentatie tussen uw IT- en OT-netwerken? ☐ ja ☐ nee
   Zo ja, hoe wordt dit bereikt?

8. Bent u in het bezit van relevante certificeringen tegen internationale normen voor uw sector?

9. Worden er penetratietesten van OT-netwerken uitgevoerd? ☐ ja ☐ nee

   Zo ja, door wie?

   ☐ ja, door een intern team
   ☐ ja, door een extern team

   Hoe vaak worden er penetratietesten uitgevoerd? | |

   Wanneer is de laatste penetratietest uitgevoerd? | |

   Indien de penetratietest materiële zaken aan het licht bracht, geef hier dan aanvullende informatie over de wijze waarop deze zijn of worden verholpen:

10. Heeft u geanalyseerd hoe snel en ernstig het falen van uw OT-systemen van invloed is op uw vermogen om inkomsten te genereren (business impact analyse)? ☐ ja ☐ nee

11. Hoe snel zouden de verkoopcijfers van uw bedrijf worden beïnvloed door een cyberincident dat van invloed is op uw OT-netwerk, inclusief een systeemstoring?

    ☐ <8 uur
    ☐ <24 uur
    ☐ <3 dagen
    ☐ <1 week
    ☐ ≥ 1 week
    ☐ Onbekend

12. Hoe snel kunt u uw OT-netwerk en systemen weer operationeel krijgen na een groot cyberincident (zoals een ransomware-aanval door een hacker die zich op afstand toegang tot uw systemen verschaft) of een systeemstoring?

☐ <8 uur
☐ <24 uur
☐ <3 dagen
☐ <1 week
☐ ≥ 1 week
☐ Onbekend

13. Welke stappen onderneemt u om schaduw-IT binnen uw OT-netwerk te identificeren?

14. Maakt u back-ups of documenteert u de configuratie van uw OT-apparaten?

☐ ja, backup
☐ ja, documentatie/geen van beide)

15. Produceert u IoT-apparaten of -sensoren? ☐ ja ☐ nee

16. Is uw vermogen om inkomsten te genereren afhankelijk van een IoT-apparaat of -sensor? ☐ ja ☐ nee

Zo ja, geef dan een overzicht van de top drie soorten IoT-apparaten die op uw terrein worden gebruikt, en waar ze voor verantwoordelijk zijn:

17A. Op welk netwerk zitten uw IoT-apparaten en -sensoren?

☐ OT-netwerk
☐ IT-netwerk
☐ Overig (openbaar netwerk))

17B. Graag uw toelichting, vooral als deze apparaten en sensoren op een openbaar netwerk zitten. Geef ook aan hoe ze beveiligd zijn:

18. Bent u verantwoordelijk voor de werking van IoT-apparaten en -sensoren die aan klanten kunnen worden verkocht? ☐ ja ☐ nee

Zo ja, graag uw toelichting. Geef ook aan hoe ze beveiligd zijn:

19. Als uw OT zich op meerdere fysieke locaties bevindt, geef dan een overzicht van elke locatie met activiteit, omzet en brutowinst: