Financial Questionnaire

1. Have you suffered any material breaches in the last 12 months? (Radio Button, options listed below)
   * Yes
   * No
2. Do you allow remote network access to critical workers? (Radio Button, options listed below)
   * Yes
   * No
   * Remote Access is not permitted

(*Is Yes select further option from below, Multiple checkboxes, options listed below)*

* IT Support Staff
* Cybersecurity Professionals
* Business Continuity/ Diester Recovery Teams
* Executive Leadership

1. How often do you practice the information security plan you have in place? (Radio Button, options listed below)
   * Annually
   * Biannually
   * Quarterly
   * Monthly
   * Never

*(If ‘Never’ selected answer the following question)*

Do you have a documented information security in place? (Radio button, options listed below)

* + Yes
  + No

1. How often are all critical employees required to complete regular cyber security awareness training? (Radio button, options listed below)
   * Annually
   * Biannually
   * Quarterly
   * No cyber security awareness training is offered

*(If ‘No cyber security awareness training is offered’ selected answer the following question)*

Do you offer alternative training such as workshops or informal training? (Radio button, options listed below)

* Yes
* No

1. How often do you conduct formal incident response training? (Optional) (Radio button, options listed below)
   * Monthly
   * Quarterly
   * Annually
   * Never
2. How often do you conduct a cybersecurity risk assessment of their IT infrastructure? (Radio button, options listed below)
   * Weekly/Daily
   * Monthly
   * Quarterly
   * Other
3. How often do you conduct a cybersecurity risk assessment of their IT infrastructure? (Radio button, options listed below)
   * Weekly/Daily
   * Monthly
   * Quarterly
   * Other
4. Including emergency patches, have you made the necessary patches to prevent an incident? (Radio button, options listed below)
   * Yes
   * No

*(If ‘No’ selected answer the following question)*

Will these patches be made in the next 30 days? (Radio button, options listed below)

* Yes
* No

1. Is all sensitive data encrypted both at rest and in transit? (Radio button, options listed below)
   * Yes
   * No
2. How often is critical data backed up? (Radio button, options listed below)
   * Monthly
   * Weekly/Daily
   * Other
   * Critical data is not backed up
3. Are there controls in place to manage and secure third-party access to your network? (Radio button, options listed below)
   * Yes
   * No
   * I do not have any third parties which I share data or system access
4. What is your process for monitoring and responding to security alerts? (Radio button, options listed below)
   * Response is in real-time
   * Response is within the hour
   * Response is within the day
   * No response
5. Are endpoint detection and response (EDR) tools used on all endpoints? (Radio button, options listed below)
   * Yes
   * No

*(If ‘Yes’ selected answer the following question)*

What endpoint detection and response (EDR) tools are used within your network? (Radio button, options listed below)

* CrowdStrike Falcon
* Microsoft Defender
* SentinelOne
* None
* Other