Report to the Audit and Risk Committee

Creation of additional Corporate Risk – 7.3 Cyber Security

Appendix 1

Background

- A&R Committee 21st March 2022
  - Annual SIRO Report
    - Increased cyber security risk
    - Ukraine crisis
    - Commonwealth Games
  - Report Back to Committee
    - Creation of New Risk 7.3 Cyber Security
    - *The Fire Authority is unable to prevent, respond to or recover from malicious attempts to damage or disrupt devices, services and networks - and the information on them.*

External Landscape

- Birmingham hosting Commonwealth Games 2022
- Previous similar events
  - Gold Coast CWG 2018
    - Blocked "about 176,000" potential attacks during the event
    - News Report
  - Japanese Winter Olympics 2018
    - Cyber Attack during opening ceremony
    - News report
- Russian/ Ukraine Crisis
  - Cyber attacks before military action
    - National Cyber Security Centre (NCSC) Report
- Requirement for more secure systems
  - Support Digital Transformation
  - Mitigate against loss of systems, data, finance
  - Reputational damage

Areas from CR 7.1.

- 7.1.1

Appropriate cyber security governance processes are not in place

- 7.1.7

Highly privileged accounts are compromised by a common cyberattack.

- 7.1.8

Common cyberattack is undetected

- 7.1.9

The organisation does not have a defined, planned and tested response to cyber security incidents that impact sensitive information or key operational services.

- 7.1.10

The organisation does not have well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise.

Worked Example Content (Move from existing Risk CR 7.1)

- Risk Trigger From CR 7.1.1
  - Appropriate cyber security governance processes are not in place

- Trigger Control Measure

1. There shall be clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operational services.
2. There shall be appropriate management policies and processes in place to direct the organisation's overall approach to cyber security.
3. The organisation shall identify and manage the significant risks to sensitive information and key operational services.
4. The organisation understands what their key operational services are .
5. The organisation shall ensure that senior accountable individuals receive appropriate training and guidance on cyber security and risk management and should promote a culture of awareness and education about cyber security across the service.

Example - Effectiveness of Control Measure

- RAG status
- 5. The organisation shall ensure that senior accountable individuals receive appropriate training and guidance on cyber security and risk management and should promote a culture of awareness and education about cyber security across the service.
- Rationale
  - Follow guidance from NCSC for Board members
  - NCSC - Cyber Security Toolkit for Boards
  - Cyber Security Toolkits for Boards (2)