| | |
|---|---|
| **Item #:** | 23.13-07 |
| **Item:** | **Cyber-security update including enterprise risk, cyber-security dashboard & [redacted] review of GE23 cyber privacy & resilience readiness** |
| **To:** | Electoral Commission |
| **For:** | Board meeting 13 September 2023 |
| **Prepared by:** | Leigh Deuchars, DCE Strategy Governance and Development |
| | Lucy Hickman, DCE Enterprise Services |

---

Recommendations

It is recommended that the Board:

1. **note** the summarised state of cybersecurity at the Commission (informed by a variety of pieces of work completed and included here)
2. **note** the key focus areas and priorities for cybersecurity in the run up to the election and beyond (informed by a variety of pieces of work completed and included here)
3. **note** the suite of cybersecurity work which has been recently completed, including:
   - Enterprise Risk Deep Dive on cybersecurity
   - Cybersecurity privacy and resilience readiness review from [redacted]
   - Cybersecurity update from the business (presented to the July 28 Board meeting)
4. **note** the management response to the [redacted] action plan, and the activities management have and are taking in response
5. **note** [redacted]
6. **endorse**:
   a. the proposed cyber security priorities for the Commission in the lead-up to the 2023 General Election
   b. the proposed Commission response to the [redacted] cyber security, privacy and resilience readiness review.

**Purpose**

1. This paper updates the Board on the overall cybersecurity context, readiness for the election, key risks and priority work areas.

**Comment**

*How we are informing our assessment of cyber security readiness*

2. Significant work has been undertaken to understand and prepare the election for cybersecurity threats, and EC's technology landscape has changed significantly since the 2020 General Election.
3. Two key reviews have informed our assessment of requirements: [redacted].

4. The cyber threat environment is constantly evolving. The reviews above are complemented by a range of monitoring and intelligence gathered from scanning the environment and a close relationship with specialist agencies such as 6(c), 9(2)(k).

*Where are the risks to the Commission?*

5. Despite considering the challenges from different perspectives, there is general consensus amongst the reviews 6(c), 9(2)(k) about the risks in our context. These are outlined below:

- An escalating risk of ransomware and DDoS attacks and campaigns, particularly toward third parties and key service providers
- The manipulation of staff, either directly or via means such as phishing, leading to access to our network or introduction of malicious software.
- Vulnerability scanning to identify weaknesses - against IP ranges and via phishing
- Hacking or espionage directed at key networks.

6. The 6(c), 9(2)(k) also highlighted the risk of actors impersonating the EC in phishing the general public which would require sophisticated incident and reputation management.

7. 6(c), 9(2)(k)

*How we are responding*

8. The response to these challenges can be categorised in three key areas:

- Systems resilience - Prevention and Protection
- Staff knowledge and processes to respond to problems
- Ability to recover and continue operating.

<u>Systems resilience</u>

9. 6(c), 9(2)(k)

10. 6(c), 9(2)(k)

<u>Staff knowledge and capacity to respond</u>

11. 6(c), 9(2)(k)

12. 6(c), 9(2)(k)

13. 6(c), 9(2)(k) [redacted]

Ability to recover and continue operating

14. 6(c), 9(2)(k) [redacted]

15. 6(c), 9(2)(k) [redacted]

***Priorities before GE 2023***

16. 6(c), 9(2)(k) [redacted]

| Focus | Why important | What is being done |
|---|---|---|
| 6(c), 9(2)(k) [redacted] | | |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | | [redacted] |

| | | |
|---|---|---|
| 6(c), 9(2)(k) | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

***Enterprise Risk Deep Dive on cybersecurity***

17. An Enterprise Risk Deep Dive providing a holistic view of Cybersecurity state of the Commission is attached as **Appendix 1**. Overall it notes that that for identified risks we have plans in place that are pragmatic to manage risk for where we are in the electoral cycle.

6(c), 9(2)(k) ***Cybersecurity, privacy and resilience readiness review***

18. We wish the Board to have a clear view of our readiness and the steps we are taking in the run up to the election. **Appendix 2** contains the report provided by 6(c), 9(2)(k).

19. We do not propose to action the plan as provided by 6(c), 9(2)(k) but have reviewed the recommendations (and the underlying assumptions). **Appendix 3** (Management Comment and Plan in response to draft 6(c), 9(2)(k) review: 2023 GE Cyber, Privacy and Resilience readiness) contains our comments and plans in response to the recommendations received for immediate action.

20. We have comfort that subsequent to this review and further steps as detailed in the management plan attached that the Commission has or is undertaking a wide suite of actions relating to cybersecurity.

***Update from the business: cybersecurity dashboard***

21. Included for your reference as **Appendix 4**, is the Cyber security dashboard provided in the 28 July Board meeting.

6(c), 9(2)(k)

**Next steps**

23. The Board will receive progress updates on implementing improvements indicated in these reports as part of monthly performance updates, and for the assurance items, in detail as part of the forthcoming quarterly assurance updates, which will provide detailed reporting on implementation of recommendations from assurance reviews.

**Appendices**

**1**: Enterprise Risk Deep Dive - cybersecurity

**2**: [redacted] review: 2023 GE Cyber, Privacy and Resilience readiness

**3**: Management Comment and Plan in response to [redacted] review: 2023 GE Cyber, Privacy and Resilience readiness.

**4**: Cybersecurity Dashboard containing business activity

**5**: [redacted]