General Dental Council | protecting patients, regulating the dental team

Item 10
Council
17 May 2018

GDC Cyber Security

Purpose of paper	To report on the stats of Cyber Security at the GDC.
Status	Public
Action	For noting
Corporate Strategy 2016-19	Performance objective 1: To improve our performance across all our functions so that we are highly effective as a regulator.
Business Plan 2018	N/A
Decision Trail	Audit & Risk Committee Cyber Security Presentation 17 June 2017
Next stage	None
Recommendations	The Council is asked to note this report.
Authorship of paper and further information	Keith Geraghty, Head of IT
Appendices	None.

1. Executive summary

1.1. This paper reports on the GDC approach to Cyber Security. Some aspects of the GDC's Cyber Security approach are highly confidential and therefore not described in detail in this report. The Council is asked to note the report.

2. Introduction and background

2.1. Cyber security threats can be described as:

- Cyber threats encompass threats to any combination of information technology and digital assets, the data held on them and the services they run or provide

- The range of cyber threats is constantly evolving, but most of them involve attacking the confidentiality, integrity or availability of data or systems
- Consequences of cyber-attacks are often much wider than a local IT or fraud issue, they can have a significant reputational impact

2.2. The GDC approaches Cyber security using three different, but complimentary, methods. These are described as:

- People Approach
- Process Approach
- Technology Approach.

3. Cyber Security – People Approach

3.1. The GDC cyber security for people approach is based on the attitude to and awareness of roles and responsibilities, security strategies and training. The GDC has processes and procedures in place for security training, awareness raising, for incident logging and reporting of data incidents.

4. Cyber Security – Process Approach

4.1. The GDC has several process-based approaches for cyber security including but not limited to:

- Policies – IT Policies articulate the GDC's values, principles, strategies, and positions relative to a broad IT topic.
- Standard Operating Procedures – procedures within teams to ensure strong controls are followed e.g. Finance new supplier approval, IT change approval
- Audit – internal & external compliance audits to check compliance to standards, procedures and SOPs
- Standards – Compliance with the Data Protection Act, Freedom of Information, GDPR etc.

5. Cyber Security – Technical Approach

5.1. The GDC cyber security technical approach is to have robust independently audited IT security in place. This includes regular internal and external auditing which is reported to the GDC Audit & Risk Committee.

12. Recommendation

12.1. The Council is asked to note this paper on the GDC approach to Cyber Security.