Minutes of the meeting

Special Board Business Meeting (BD)

Date	**2 August 2023**
Time	**12:00-13:00**
Location	**Online call**
Present	Frank Mitchell (Chair) (FM) Sheila Cowan (SC) Dr Mark Dames (MD) Dr Carol Evans (CE) Nazim Hamid (NH) Graham Hutcheon (GH) Margaret McCaig (MMcC) Christine Pollock (CP) David Rankin (DR) Eileen Russell (ER) Damien Yeates (Chief Executive) (DY)
Attendance	Neville Prentice (NP) George Boag (GB) Laura Barjonas (LB) Paul Clark (PC) Chris Knight (CK) Secretariat Ayah Hatim (AH) Kathleen Nisbet (KN) Elaine MacPherson (EMacP)
Apologies	Tracy Black (TB) Beth Corcoran (BC) Prof David Hillier (DH) Victoria Erasmus (VE) Dr Poonam Malik (PM) Paul Taylor (PT)

1. Apologies and Declaration of Interest

Apologies were received from TB, BC, DH, VE, PM, and PT.

There were no declarations of interest.

2. Introduction

The Chair thanked Board members for attending the Cyber Security session.

Neville introduced the session:

- the session would be divided into two parts, the SDS Cyber Strategy and the action plan and the Enterprise IS (EIS) update;
- the team would look for approval of the SDS Cyber Strategy;
- the Information Management Strategy (IMS) and EIS were both audited by EY;
- the intention was to complete a cyber maturity assessment by the end of the financial year.

3.1 Cyber Strategy

GB provided an update:

- the strategy placed an SDS lens on Cyber resilience and brings together the EIS partnership wide initiatives with SDS initiatives;
- SDS Cyber Strategy was developed over the last eight to nine months and incorporates feedback from audits, cyber exercises and an earlier cyber maturity assessment;
- SDS is currently progressing its third reaccreditation under the cyber essentials plus programme;
- the cyber strategy is aligned to the SDS strategic plan and the wider Scottish government cyber strategy;
- the importance of developing a positive cyberculture across the organisation and with stakeholders to improve resilience is prominent throughout the strategy;
- EY used the National Institute of Standards and Technology (NIST) Cybersecurity Framework in audits. SDS ensured the action plan was aligned with this framework;
- the action plan set out key actions to progress. All of those actions were underway with the majority of them set to be completed and closed by the end of the financial year;
- the immediate priority actions were to be completed by the end of August.

SC asked for clarification on how the goals were prioritised.

GB advised the actions carry individual prioritisation and each goal carries uniform importance.

SC asked for clarification on whether this was dependent on the overall risk for each action.

GB confirmed it did.

NP advised that the prioritisation also considered resource requirements.

DR commented on being pleased with the information provided and the proposed plan. DR requested that a single-page programme plan be developed to highlight the key activities and dependencies, milestones and Red Amber Green (RAG) statuses.

NP advised they would implement this and provide an update at the next Board meeting.

NH asked if there was anything in place to identify and recognise good staff cyber practice.

GB advised this has had some initial consideration through thanking staff for reporting potential phishing and malware. This is included in the action plan and the aim is to expand this into a wider programme of work.

MD had a query on the fourth goal, developing a positive cyberculture throughout SDS and with stakeholders. In terms of external, was there an approach to share good practice and learning with other public sector organisations.

GB advised in terms of EIS, there had been a lot of information shared across the partnership on the Shared Cyber Risk Forum and Security Council. There were also Scottish Government (SG) groups that SDS was involved in.

The Chair asked for clarification on whether a member of staff who failed their phishing test would be auto assigned to training.

GB advised over the last three phishing tests, at the point of being misled, staff would then be directed to an online training session. At the end of the report, the team would be provided with the number of staff who had been misled and who had also completed the training. An online group session was mandatory in addition to the online training. Some staff may have completed the group training but not completed training by the deadline.

The Chair asked for this to be resolved to ensure both the individual and group training was completed by staff. The Chair asked for clarification on when the phishing dashboard would be finalised.

GB advised this would be completed in the next couple of weeks and the team would clarify the process and timelines related to training completion.

CE asked if there were any common demographics of staff who failed more than one phishing test.

GB advised SDS had been running phishing tests for five years and in the last two years there had been no repeat offenders. The latest test showed no common demographics, however, previous tests highlighted staff new to the organisation were more inclined to be misled. Since then, training for new starts had then been strengthened.

The Chair asked for an update to be provided at the next Board meeting.

	The team would look at options for identifying, recognising, and rewarding good cyber practices among staff.
3.2	Cyber Security – Risk Mitigation Update GB presented an overview on the Cyber Audit, Cyber Training, Cyber Exercising, Cyber Risk Monitoring/Action and Cyber Insurance. The Board noted the update.
3.3	Cyber Security – Risk Mitigation Update – EIS (including partners) GB presented an update: - the programme included a number of areas which was supported by 12 months of a work portfolio. SDS had supported other partners in developing their own strategies; - the team had begun to have conversations on what services would look like in the future; - GB provided an overview of the Shared Cyber Risk Forum, Security Council, Security Operation Centre and the out of hours project; - SDS were audited on a yearly basis and was currently going through an audit. The final report would be shared with the Board once received. CK presented an update: - EIS was a shared service and SDS had close relationships with partners; - one of the key areas was the Security Council as all partners attend and share information on threats, responses and strategies; - there was also the Shared Risk Forum to look at risks across all of the partnerships. The risk forum maintained a risk register which informed SDS's annual security program. The final audit report would be shared with the Board once received by the team.
3.4	Cyber Security Dashboard GB presented an update: - this would provide a single-paged plan in the form of a dashboard for the Board to monitor the cyber progress; - there would be a number of actions to track under each goal; - the team would appreciate feedback on the Key Performance Indicators (KIPs) related to cyber resilience. The Board approved the strategy and action plan subject to the three actions raised. The Chair thanked the team for their work on developing the Cyber Strategy. SDS Cyber Strategy was approved, subject to the three actions raised.
	Any other business
	Close of Board Business Meeting
	Date of next scheduled meeting: 13 September 2023, location to be confirmed (10:00 – 16:00 hrs)