Scottish Social Services Council

Council
28 January 2020
Agenda item: 10
Report no: 04/2020

Title of report	Cyber Awareness Training
Public/confidential	Public
Action	For information
Purpose of report	To provide assurance to Council that the actions identified by Audit and Assurance Committee regarding mandatory cyber awareness training have been implemented
Recommendations	The Council is asked to: 1. endorse the progress in implementing mandatory cyber awareness training.
Author and Responsible Officer	Name: Laura Shepherd Job title: Director of Strategy and Performance Phone no: 01382 317942
Link to Strategic Plan	The information in this report links to: Outcome 4, Priority 6 – High standards of governance
Link to the Risk Register	Risk 6 - The SSSC experiences disruption or loss or reputation damage from a failure to its systems, physical security or information governance arrangements.
Documents attached	None

1. INTRODUCTION

1.1 Internal Audit recommended that the organisation implements mandatory cyber and information security training for all staff. This was partially accepted by management in the report under explanation that the organisation did not have a system in place to implement mandatory training. The Audit and Assurance Committee rejected management's explanation given the importance of this training and recommended that management formulates proposals and timescales for implementation ahead of the Council's meeting in January.

1.2 This report outlines the plan for the introduction of cyber security training across the SSSC.

1.3 The risk for cyber security remains high and this programme provides mitigating action against the risk of staff creating phishing scam access to information about the organisation and its customers. The training gives staff the knowledge on how to act if they receive something suspicious. While we cannot guard against phishing emails being received, it provides assurances that staff are informed how to manage the risk appropriately.

1.4 The SSSC has several high-level security mechanisms in place to deal with the possibility of a hacking type attack not associated with phishing email. This is where the attacker gains access to the system via another route or denial of service is launched. We have recently gained Cyber Security Plus accreditation which affords a high level of confidence our systems are appropriately monitored. However, there is no 100% complete fail safe against these types of attacks that we can implement.

1.5 The implementation of this training plan has led to wider questions about the organisation's digital skills and digital maturity. It was agreed at Digital Sponsor Group on 14 January 2020 that we would conduct a digital maturity assessment to inform a digital training plan for our own workforce.

2. CYBER SECURITY TRAINING PLAN

2.1 We have procured a web-based eLearning tool from knowbe4. This tool allows us to deliver tracked and targeted training to the organisation via an online portal from any device, using the same login as we use for office 365. We will use the tools and training provided by this software to integrate with the organisation's security practices going forward. The tool integrates with our existing infrastructure and allows us to pull from several training topics and deliver this organisation wide or to specific teams. The system also allows us to track if the training has been completed and escalate to hiring manager where needed. It also allows for advanced reporting and the ability to perform phishing tests to simulate real-world scenarios. Phishing scams are experienced by the organisation, as they are in any organisation with external reaching technology. This product experiences will allow us to build tests that mimic real-world scenarios and determine the risk levels when the organisation experiences phishing scams.

2.2 4 January 2020 - IT will begin by sending out a simulated phishing email to determine how at risk, as an organisation, we are to phishing attacks as a baseline. This will not be promoted to staff, but we will report on the results to the Executive Management team (EMT).

2.3 17 January 2020 - IT will then roll out an organisational wide mandatory training using the standard cyber awareness training provided by the platform. This will be tracked through the system and escalated to hiring manager where needed, we can also report on the results of this training.

2.4 Staff will be given four weeks to complete the training and then a reminder will be sent. Staff will then be given a further two weeks before escalation to their line manager. The Operational Management team (OMT) will be advised to plan the protected time in for staff to complete this module.

2.5 New staff will be required to complete this module within day one or two of commencing in post.

2.6 Repeated simulated phishing campaigns will be carried out to allow users to practice the skills they've learned in the training. This then allows for targeted approaches when repeated failures are occurring.

2.7 The IT team will attend each of the departments team meetings for a cyber awareness session in January/February. Dates for these have been arranged.

2.8 The Communications team is developing cyber awareness training posters for each office and a series of cyber security emails over the course of this programme will be used.

2.9 Going forward we will deliver additional awareness training and even some targeted training for individual teams and those in particular "high risk" roles, in Fitness to Practise and Hearings.

2.10 This tool also gives us some other very useful features such as a phishing alert button that forwards a safe copy of a suspect phishing message directly to the IT team for investigation. Once we establish the programme, we can add additional cyber resilience training and periodically resend the test phishing email.

3. RESOURCE IMPLICATIONS

3.1 The cost of procuring this system from a current supplier has been £2000 (excluding VAT) which was found within existing budget underspend.

4. EQUALITY IMPACT ASSESSMENT

4.1 The work did not require any changes as a result of the equalities impact assessment.

5. LEGAL IMPLICATIONS

5.1 Data breaches arise from phishing scam emails. As with all data breaches these are assessed and reported to the Information Commissioner's Office when necessary.

6. STAKEHOLDER ENGAGEMENT

6.1 The EMT, OMT and Digital Services have been engaged.

7. IMPACT ON USERS AND CARERS

7.1 This programme provides mitigation and reduces the risk that data will be lost or accessed through a data breach caused by a phishing scam.

8. CONCLUSION

8.1 Council can be assured that the implementation and awareness of the requirements to be cyber security aware and reduce the overall risks to the organisation.

9. BACKGROUND PAPERS

9.1 December 2019 Internal Audit Report on ICT security.