Social Security Scotland
Tèarainteachd Shòisealta Alba

Executive Advisory Body	
Date of Meeting	Tuesday 16 November 2021
Subject	Cyber Security Update
Agenda No.	4
Paper No.	26.2 a
Prepared By	Digital Risk and Security Team
Purpose	Discuss

1. Background

1.1. Cyber-attacks on organisations has increased significantly over the last few years. The London Business School estimates that between October 2019 and September 2020, 59% of global organisations detected attackers within their environment which was a 12% increase on the previous year. Victims ranged from Apple and LinkedIn to Colonial Pipeline, Sony Pictures and Marriot Hotels. Closer to home, victims have included the Weir Group, Dundee & Angus College, Aspire Housing Association and most recently the attack on the Scottish Environment Protection Agency.

1.2. Cyber-attacks can be perpetrated by many and varied groups and can range from individuals with little capabilities through to nation state backed groups with very significant resources and capabilities. For example, Microsoft estimated that a recent attack against Solarwinds was planned, developed and delivered by a team of around 1,000 engineers.

1.3. We commission an externally produced threat assessment each year which informs us as to who our most likely adversaries are, their capabilities and their motivations. This helps to inform our investments, allocation of resources and areas of particular focus.

1.4. We work closely with colleagues in other bodies with expertise in security including, but not limited to, the National Cyber Security Centre for advice and guidance on cyber security and the Centre for Protection of National Infrastructure for advice and guidance on internal threats and physical security as well as with colleagues in the wider Scottish Government community.

1.5. We construct our cyber security protection capabilities in alignment with cybersecurity frameworks which provide guidance on how to structure and organise teams and disciplines in order to manage and reduce cybersecurity risk. We operate our protective regime around the broad areas of Identifying Assets, Protecting Assets, Protective Monitoring, and Incident Response and Recovery.

1.6. Our overall approach is also based on a “secure by design” methodology where we “bake in” security from the outset as opposed to retrofitting it later.

1.7. Whilst a robust and comprehensive cyber security will stop many attacks, it should be recognised that no protection guarantees that an attack will never be

successful. With this in mind, we also develop and regularly review incident response and recovery plans and we have tested these out using the National Cyber Security Centre's, "Exercise in a box" cyber-attack response tools.

2. Key points

2.1. The challenging and real threats from those who would seek to do us harm.

2.2. From the accompanying presentation, the capabilities of the Digital Risk & Security Team.

3. Conclusions

3.1. Presentation is for information and discussion.

3.2. The purpose of this paper is to engage with the Executive Advisory Body more fully with regard to Cyber Security and to use the National Cyber Security Centre's Board Toolkit to start this process.

3.3. The Executive Advisory Body are asked to consider if they would endorse this approach?

Social Security Scotland
Tèarainteachd Shòisealta Alba

4. GOVERNANCE CHECKLIST

Please ensure that you detail which Corporate Plan Strategic Objective the paper contributes to. These strategic considerations should be used to assist you with the content of your paper.

Strategic Objective	Contribution
Helping to deliver a social security system with dignity, fairness and respect.	Not Applicable
Supporting people in Scotland to access devolved benefits that they are entitled to.	Not Applicable
Running our service in a responsible way.	Cybersecurity is a key component of running our systems securely in order to ensure service availability and the protection of citizen data.

State here how the paper considers these areas and any consultation undertaken in the agency. Only complete the section(s) relevant to your paper.

Strategic consideration	Impact
Environment	Not Applicable
Governance	Not Applicable
Data	The paper is relevant to the data held on Social Security Scotland's IT systems and the protection thereof.
Finance	Not Applicable
Staff	Not Applicable
Equalities	Not Applicable
Estates	Not Applicable
Communications and Presentation	Not Applicable – Please delete if applicable and state how the paper considers these areas and any consultation undertaken in the agency.

An Impact Assessment must be carried out during the development of all new Agency policies and services and when making significant changes to policies and services. The Corporate Assurance team should be involved form an early stage to provide guidance and advice relating to completing impact assessments.

Impact Assessment Saltire Page

General Impact Assessment Queries: Corporateassuranceteam@socialsecurity.gov.scot

Equality Impact Assessment Queries: Marion.Logan@socialsecurity.gov.scot

Please complete the below table.

Social Security Scotland
Tèarainteachd Shòisealta Alba

Type of Impact Assessment	Required (Y/N)	If No - briefly state reason e.g. Not relevant/Not eligible – agreed with Deputy Director	If yes – briefly state progress to date, highlight any significant issues.
Business and Regulatory Impact Assessment (BRIA)	N	Not relevant	
Child Rights and Wellbeing Impact Assessment (CRWIA)	N	Not relevant	
Data Protection Impact Assessment	N	Not relevant	
Equality Impact Assessment (EQIA)	N	Not relevant	
Fairer Scotland Duty assessment	N	Not relevant	
Future proofing legislation	N	Not relevant	
Human rights in policy making	N	Not relevant	
Islands Communities Impact Assessment (ICIA)	N	Not relevant	
Strategic Environment Assessment (SEA)	N	Not relevant	