Social Security Scotland
Tèarainteachd Shòisealta Alba

Executive Advisory Board Briefing

16 November 2021

Dignity, fairness, respect.

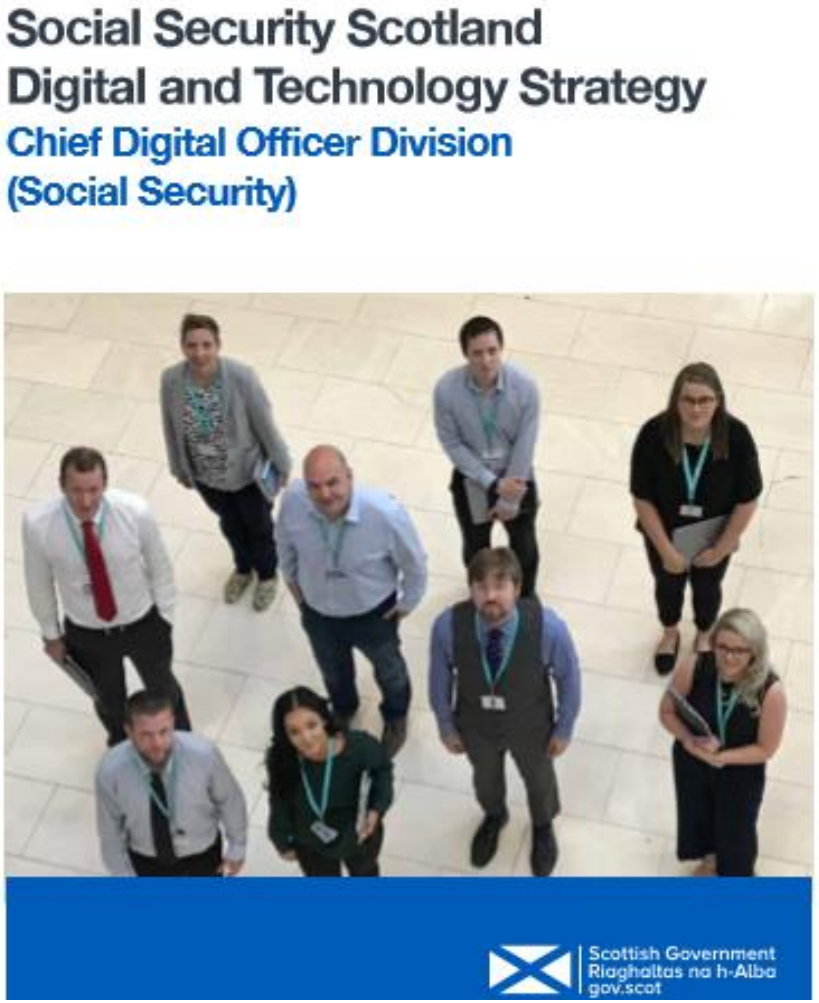
Agenda

1. Overview of the Digital Risk & Security Team
2. National Cyber Security Centre's (NCSC) Board toolkit "5 questions for your Board's agenda"
3. Further engaging the Board with the NCSC Board toolkit
4. Questions

Digital Risk & Security Branch

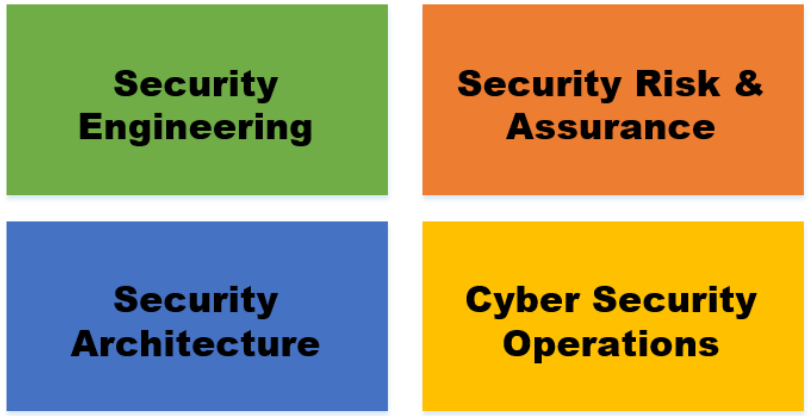
- Established May 2017
- Led by Chief Information Security Officer
- Consists of four close knit teams
- Diverse Workforce
- Focus on personal development and pipeline

[Redacted]



Digital Risk & Security Branch

- **Security Architecture** (Design)
  - Support “secure by design” ethos
- **Security Engineering** (Detect)
  - Real Time Protective Monitoring & Alerting
  - Retrospective Threat Hunting
- **Cyber Security Operations** (Identify, Protect & Respond)
  - Protect the IT environment
  - Manage Vulnerabilities
- **Security Risk & Assurance** (Assure)
  - Risk assess new projects and the ongoing compliance of existing



Security Maturity

- Early design workshops with the National Technical Authority for Cyber Security
- The Security Information Risk Adviser (SIRA) Engagement Model
- Established the Security Baseline Standard SBS Document
- Concept of Umbrella & Threat Risk Assessment
- Created the Security Operational Readiness Statement
- Robust mechanism for pre go-live independent IT Health Checks

Sepa spends nearly £800,000 on cyber attack response

By Andrew Picken
BBC Scotland News

3 April

Scotland's environmental watchdog has spent nearly £800,000 on its response to a major cyber attack, new figures show.

The Scottish Environment Protection Agency (Sepa) had **more than 4,000 of its digital files stolen by hackers** on Christmas Eve.

The files were released on the internet when Sepa refused to pay a ransom.

The public body has warned it could be next year before its systems have fully recovered from the attack.

Figures released to BBC Scotland under freedom of information laws show a total of £790,000 has been spent on Sepa's response and recovery actions so far.

This includes £458,000 on stabilising the watchdog's business IT platform.

Sepa has restored the majority of its key services, such as flooding forecasting, but it is expected a full recovery from the attack will take up the remainder of 2021-22.

1996 vs 2018

Collaborative Effort

- Scottish Government
  1. Cyber Resilience Division *(early on Public Sector Action Plan / Cyber Catalyst)*
  2. Cyber Defence & Security Branch *(cyber)*
  3. Security & Business Continuity Division *(board representation)*
  4. *Digital Directorate (cloud experience)*

- NCSC & UK Government
  1. Formal engagement established with the National Cyber Security Centre
  2. Technical Workshops (Glasgow, Edinburgh & London)
  3. Early design recommendations made
  4. Key feature of consecutive NCSC Annual Reports
  5. Confidence boost for many (including Minister)
  6. DWP Cyber Resilience Centre

"Our engagement with the NCSC has helped us to establish our executive agency, Social Security Scotland, followed by the launch of our public facing cloud based digital platform, which underpins the delivery of the first live devolved benefit payments Scotland. The NCSC has provided us with expert advice and guidance through technical workshops and engaging its partners to share experiences. This has given us valuable assurance in support of our strategic security objectives and our own 'Secure by Design' principle."

John Campbell, Head of Digital Risk & Security Social Security Directorate, Scottish Government

The NCSC Board Toolkit

5 questions for your board's agenda

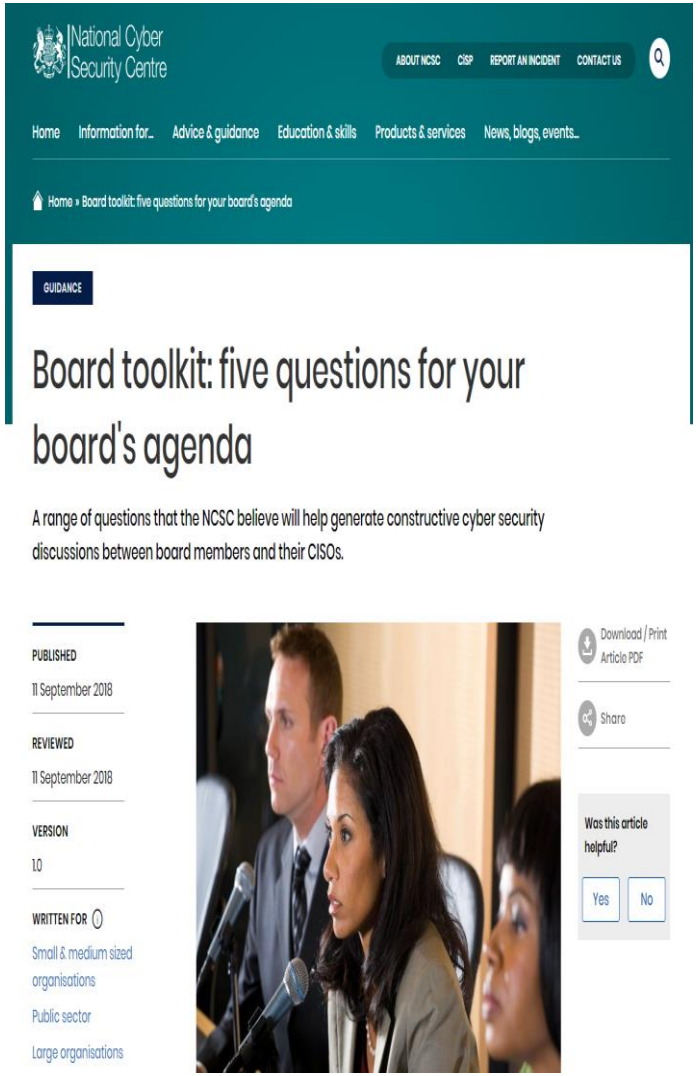
Q1: How do we defend our organisation against phishing attacks?

Q2. How does our organisation control the use of privileged IT accounts?

Q3. How do we ensure that our software and devices are up to date?

Q4. How do we make sure our partners and suppliers protect the information we share with them?

Q5. What authentication methods are used to control access to systems and data?



National Cyber Security Centre
a part of GCHQ

Q1. How do we defend against Phishing attacks?

Phishing describes a type of social engineering where attackers influence users to do 'the wrong thing', such as disclosing information or clicking a bad link. The link could install malware on your system, or direct you to a fake website that asks for sensitive information"

- Laptops and associated services (email, Teams, Internet browsing) are a managed service with accompanying defensive security wrapper

- We complement the service provider's defensive operations in our own environment:
  - **Employee awareness** programs educate users on phishing scenarios
  - [Redacted]
  - [Redacted]
  - Our **threat intelligence** platform searches the Dark Web for any Social Security Scotland credentials which may have been compromised and offered for sale
  - We carry out **scenario testing** related to this using the NCSC "Exercises in a Box"

[Redacted]

Q2. How do we control the use of privileged IT accounts?

All staff should be provided with enough system privileges and rights required to perform their role. Granting elevated system privileges should be carefully controlled and managed, a policy often referred to as 'least privilege'. This principle of least privilege should be assessed as staff leave, join and move departments. It's particularly important that administrators (and those with extensive rights) who move to other jobs don't maintain their privileges. All relevant accounts should be disabled when staff leave the company.

- The Service Desk acts as the **single point of contact for account management** and processes Joiners, Movers & Leavers' system access
- [Redacted]
- [Redacted]

[Redacted]

Q3. How do we ensure that our software and devices are up-to-date?

Patching is the process of applying the updates that suppliers and vendors regularly issue to all your hardware and software. Patching enhances functionality but also fixes security bugs or vulnerabilities, so applying patches is one of the most important things you can do to improve your security.

- Laptops and smartphones are a managed service. We complement the managed service with the following in our own environment:
  - [Redacted]
  - We **regularly scan**, audit and report on critical, high, medium and low vulnerabilities that exist
  - There is a clear and approved **policy** detailing team responsibilities and time frames to patch
  - [Redacted]
  - [Redacted]

[Redacted]

Q4. How do we ensure our partners and suppliers protect the information we share with them?

At some point you will probably need to share your information with your partners and suppliers. There may be occasions where you wish to allow direct network connectivity between your systems and/or services. It's important to gain confidence that any information shared with others will be well protected and looked after.

- We ensure we have **confidence** that our partners are not vulnerable to cyber attack
- At procurement stage we have a **set of criteria** that we verify conformance with, for example the holding of a current and appropriate industry recognised accreditation such as Cyber Essentials+ or ISO27001
- Taking an ongoing **risk based approach**, we may carry out an audit on the supplier
- We **monitor** supplier cyber status using our Threat Intelligence Platform (TIP) – for example last year our TIP notified us of a possible cyber attack on one of our suppliers 24 hours before the supplier informed us.
- [Redacted]

[Redacted]

Q5. What authentication methods are used to control access to systems and data?

Passwords are an easily-implemented, low-cost security measure, with obvious attractions for managers within enterprise systems. However, passwords can be a relatively weak method of authenticating users, and should be complemented by other controls to protect your enterprise.

- User education to educate them on **good password practice**
- [Redacted]
- [Redacted]
- **We search** the Dark Web for any compromised user names and passwords belonging to Social Security Scotland users

[Redacted]

NCSC Board Toolkit – Next Steps

Board members don't need to be technical experts, but they need to know enough about cyber security to be able to have a fluent conversation with their experts, and understand the right questions to ask.

The Board Toolkit therefore provides:

- 1. A general introduction to cyber security.
- 2. Separate sections, each dealing with an important aspect of cyber security. For each aspect, it will:

  explain what it is, and why it's important
  - recommend what individual Board members should be doing
  - recommend what the Board should be ensuring our organisation is doing
  - provide questions and answers which the Board members can use to start crucial discussions with their cyber security experts
- 3. An Appendix summarising the legal and regulatory aspects of cyber security.

Social Security Scotland
Tèarainteachd Shòisealta Alba

Questions