Committee report

Scottish Environmental Protection Agency (SEPA) cyber-attack

Committee Audit and Standards

Date of meeting 26 November 2021 **Date of report** 16 November 2021

Report by Acting Chief Executive

1. Object of report

To advise the committee of a report on the Scottish Environmental Protection Agency (SEPA) cyber-attack and outline the key messages for SPT contained therein.

2. Background

Members may have seen recent news articles (on 27 October 2021) in the media of a report on the cyber-attack on the Scottish Environmental Protection Agency (SEPA).

On 24 December 2020, SEPA were subject to a serious and complex cyber-attack, displaying significant stealth and malicious sophistication, which significantly impacted the organisation, staff, public, partners, and the communities who rely on their services.

The cyber-attack led to SEPA being unable to access its digital network and systems.

In the ten months since the cyber-attack, SEPA have worked with the Scottish Government, Police Scotland, the National Cyber Security Centre (NCSC) and the Scottish Business Resilience Centre (SBRC) on a recovery strategy.

On 27 October 2021, SEPA published a report titled *‘SEPA’s response and recovery from a major cyber-attack’.*

The report says that Police Scotland acknowledged that this incident could happen to any sector or organisation on the basis that there is a clear and real cyber threat.

The report adds that the SBRC noted that in addition to the initial cyber-attack, there was a secondary and deliberate attempt to compromise SEPA systems as they endeavoured to recover and restore back-ups.

SEPA have published the findings of their cyber-attack so that as many organisations as possible can use the experience to better protect themselves from cybercrime.

The full SEPA report can be found at:

https://www.sepa.org.uk/media/593774/sepas-response-and-recovery-from-a-major-cyber-attack.pdf

3. Outline of findings

Members will recall, at the last Audit and Standards meeting on 27 August 2021, the Committee noted the Scottish Government report titled *‘the Strategic Framework for a Cyber Resilient Scotland’* and SPT’s commitment to the highest standard of cyber security arrangements where possible.

Members will also recall that cyber resilience is more than making technologies and systems secure. It is about preparedness to meet cyber risk, and how well-equipped SPT is to withstand, and defend against, manage, recover quickly and learn from cyber incidents.

Since the last meeting, officers have continued to develop digital infrastructure and processes to meet this commitment.

Members are asked to note a report presented to and approved by the Personnel committee on 5 November 2021 titled *‘Information and Cyber Security Policy Review’*.

Members are also asked to note two reports presented to the Strategy and Programmes committee today on the *‘Digital Strategy update’* and *‘Proposed award of Network Managed Service contract’*.

Management will review the lessons learned from the SEPA cyber-attack and continue to develop cyber resilience arrangements and digital capability in service delivery.

4. Conclusions

On 27 October 2021, SEPA published a report titled *‘SEPA’s response and recovery from a major cyber-attack’.* SEPA have published the findings of their cyber-attack so that as many organisations as possible can use the experience to better protect themselves from cybercrime.

Management will review the lessons learned from the SEPA cyber-attack and continue to develop cyber resilience arrangements and digital capability in service delivery to the highest standard of cyber security arrangements where possible.

5. Committee action

The committee is asked to note the contents of this report, the SEPA report titled *‘SEPA’s response and recovery from a major cyber-attack’* and SPT’s commitment to the highest standard of cyber security arrangements where possible.

6. Consequences

Policy consequences	*None.*
Legal consequences	*None.*
Financial consequences	*None.*
Personnel consequences	*None.*
Equalities consequences	*None.*

Risk consequences	*As detailed in the report.*

Name	Neil Wylie	**Name**	Valerie Davidson
Title	**Director of Finance**	**Title**	**Acting Chief Executive**

For further information, please contact Neil Wylie, Director of Finance, on 0141 333 3380.