**Police Scotland - Operation Claybill Structured Debrief Review**

**SUGGESTED RECOMMENDATIONS**

**SUGGESTED RECOMMENDATION 1**

**ORGANISATIONAL PREPAREDNESS;** SEPA and the wider public sector organisations within Scotland to consider the value of retaining a Cyber Incident Response (CIR) specialist company to ensure availability of the necessary expertise at the earliest opportunity.

**SEPA Response**
SEPA has reviewed and let a contract with a specialist cyber incident response company to ensure the availability of necessary expertise.

**SEPA Action complete.**

**SUGGESTED RECOMMENDATION 2**

**ORGANISATIONAL PREPAREDNESS;** As part of ongoing review of existing Cyber Incident Response Plans, SEPA and the wider public sector organisations within Scotland to adapt and/or develop appropriate plans, **accessible out with the organisational network**, that ensure optimum organisational preparedness and response capability in the event of a cyber-attack either internally or externally.

**SEPA Response**
We have already established a 'home' page on [redacted] to store our recovered resilience and business continuity management plans including incident and emergency management plans, Business Impact Assessment, Service Recovery Plans, etc. Secure access to this site will be given to all staff who are required to access these plans. Training will be provided to staff authorised to use the site. SEPA's Resilience team will work with document owners to ensure that they are kept up to date with periodic reviews. Document Owners will ensure that, as appropriate, individuals hold hard copies of relevant plans.

**SEPA Action underway.**

**Deadline date:** [redacted]

**SUGGESTED RECOMMENDATION 3**

**EMERGENCY RECOVERY;** SEPA and the wider public sector organisations within Scotland to review existing Business Continuity and Disaster Recovery Plans to adapt and/or develop appropriate structures and processes that enable effective emergency recovery from a cyber-attack and encompasses key considerations such as access to emergency communication systems, temporary IT facilities and mutual aid.

**SEPA Response**
SEPA will review existing business continuity and disaster recovery plans. We will work with partner agencies and key contacts across the public sector to explore options for temporary IT and mutual aid support.

**SEPA Action underway**

**Deadline date:** [redacted]

**SUGGESTED RECOMMENDATION 4**

**EMERGENCY RECOVERY;** Recognising network connection withdrawal by external partners is an early tactic to preserve the integrity of networks, SEPA and the wider public sector organisations within Scotland should assess, understand and document the network connections with external stakeholders and the implications of a sudden withdrawal. In addition, stakeholder engagement on this specific matter should be introduced to their plans with critical stakeholders being prioritised.

**SEPA Response**
SEPA will document all network connections with external stakeholders and engage with them on withdrawal protocols in the event of a cyber incident.

**SEPA Action underway.**

**Deadline date:** [redacted]

**SUGGESTED RECOMMENDATION 5**

**DATA THEFT;** In support of existing data theft plans and playbooks, Police Scotland to provide guidance in relation to the investigation and mitigation of data thefts including accessing the dark and Clear web, identifying the scale and nature of the data theft (including data monitoring, recovery and integrity considerations) and supporting individuals whose data may have been compromised.

**Response**
Action attributed to Police Scotland.

**SUGGESTED RECOMMENDATION 6**

**ROLES & RESPONSIBILITIES;** Police Scotland to review and provide clarity of roles and responsibilities, and a best practice approach for procuring the forensic investigation, securing the evidential chain, management of evidence and engagement parameters between the victim, CIR Companies and Police Scotland in the event of a cyber-attack.

**Response**
Action attributed to Police Scotland.

**SUGGESTED RECOMMENDATION 7**

**TRAINING, TESTING & EXERCISING;** SEPA and the wider public sector organisations within Scotland to review Cyber Incident Response Plans, Ransomware and Data Loss play books and as an exercise priority test them against an enterprise level ransomware and data exfiltration attack.

**SEPA Response**
SEPA will review its cyber incident response plans and undertake an exercise to test them against enterprise level ransomware and data exfiltration attack.

In addition, SEPA will publish lessons learned from the recent cyber attack and participate in multi-agency exercises.

**SEPA Action underway.**

**Deadline date:** [redacted]

**SUGGESTED RECOMMENDATION 8**

**TRAINING, TESTING & EXERCISING;** Scottish Government CRU in collaboration with key stakeholders to consider the development of an Organisational Learning and Development process in support of Cyber incidents and exercising across the Public Sector to ensure that there is a consistent and pro-active approach to the identification of learning and an appropriate 'end to end' process that ensures learning identified become lessons learned and that they are captured within a single repository and communicated accordingly.

**Response**
This response is attributed to Scottish Government.

**SUGGESTED RECOMMENDATION 9**

**COMMUNICATION;** SEPA and the wider public sector organisations within Scotland to consider development of /or review specific crisis communications plans to reflect the implications of cyber-attacks.

**SEPA Response**
SEPA will review and update its crisis communication plan to take account of learnings from the cyber incident.

**SEPA Action**

**Deadline date:** [redacted]