SEPA 12/22

Agency Board Meeting
26 April 2022

Costs of responding to a serious and significant cyber-attack

Summary:	On Christmas Eve 2020, SEPA was the victim of a serious and significant cyber-attack orchestrated by international, serious, and organised criminals that resulted in the loss of access to most of our systems and data. The purpose of this report is to share with the Board, SEPA's analysis of the cost to SEPA in responding to the cyber-attack.
Risks:	There are no risks to SEPA in providing this information, the costs of recovering from the cyber-attack were managed within SEPA's available resources.
Resource and Staffing Implications:	Whilst this information does not affect resource numbers, it is important to highlight that although the critical build of the Finance and HR system is complete, the impacts of the cyber-attack on a small team will continue to be felt for some time as we move into a different phase of our recovery.
Equalities:	None.
Environmental and Carbon Impact:	None.
Purpose and audience of the report:	The Board is asked to note this report for information and discussion.
Report Author:	Stuart McGregor, Chief Officer, Finance
Appendices:	Annex A: Costs of responding to a serious and significant cyber-attack by international, serious, and organised criminals.

1. Introduction

1.1 On Christmas Eve 2020, SEPA was the victim of a serious and significant cyber-attack orchestrated by international, serious, and organised criminals that resulted in the loss of access to most of our systems and data.

1.2 The purpose of this report is to share with the Board, SEPA's analysis of the cost to SEPA in responding to the cyber-attack.

2. Background

2.1 As mentioned at the April Strategy Board meeting, SEPA has been working to finalise, by the end of March, the costs of the cyber-attack. This has now been done and we have shared it with the Scottish Government, the Public Audit Committee, as a follow up to our recent evidence presented to them, and released in response to a number of outstanding Freedom of Information requests.

2.2 This information was circulated to Board Members in advance of the external release and is presented today as a paper for the record.

3. The Issues

3.1 It is possible that there may be some media interest in the release of the cyber costs.

4. Recommendations

4.1 The Board is asked to note this report for information and discussion.

Stuart McGregor
26th April 2022

Annex A

SCOTTISH ENVIRONMENT PROTECTION AGENCY

COSTS OF RESPONDING TO A SERIOUS & SIGNIFICANT CYBER-ATTACK BY INTERNATIONAL SERIOUS & ORGANISED CRIMINALS

MARCH 2022

TOTAL SUMMARY

COST TYPE	SUMMARY	£'000
Cyber-Attack Response	Supporting Our Services	353
Cyber-Attack Response	Supporting Our People	244
Cyber-Attack Response	Independent Audits & Sharing Our Learnings Widely	218
Cyber-Attack Response	Systems Security	495
Cyber-Attack Response	Systems Recovery & Rebuild	1,175
Cyber-Attack Response	Other	1,478
Sub-Total:		**3,963**

COST TYPE	SUMMARY	£'000
Costs Brought Forward From Future Years		1,130
Sub-Total:		**1,130**

SUPPORTING OUR SERVICES

ORGANISATION	SUMMARY	£'000
Kisters and Deltares	Flood Warning Systems	310
Scrimsign (micro electronics) Ltd	Bathing water signage, cyber-attack recovery	31
Labware	Support for laboratory information management system	12
Sub-Total:		**353**

SUPPORTING OUR PEOPLE

ORGANISATION	SUMMARY	£'000
TransUnion	Identity theft protection for our people.	29
Intrado	Intercall group communication service.	20
Scottish Government	Scottish Government staff time and use of laptops	195
Sub-Total:		**244**

INDEPENDENT AUDITS & SHARING OUR LEARNINGS WIDELY		
ORGANISATION	**SUMMARY**	**£'000**
Azets	Independent Audit - Response, impact assessment and lessons learned	48
3X1	Public communication, employee and stakeholder engagement	136
We are Hydrogen	Comms support – Social Media	34
Sub-Total:		218

SYSTEMS SECURITY		
ORGANISATION	**SUMMARY**	**£'000**
NCC Group	Forensic Investigation	151
Forcepoint	Firewall replacement	50
Insight	Pure disk storage units	200
HP Inc UK Ltd	Laptop recovery	94
Sub-Total:		**495**

SYSTEMS RECOVERY & REBUILD		
ORGANISATION	**SUMMARY**	**£'000**
HITC	Enterprise Resource Planning System (Agresso) – Minimum Viable Product Build	537
Insight UK	Architecture consultancy services and new network design	100
Perkin Elmer	Professional service to build & configure MS Azure based Spotfire and Attivo	17
Ikonic	Citrix workspace service agreement	54
Insight (Keystream)	Interim technical resourcing to support recovery	293
PING	Network design work for remote access	18
Insight UK	Increase in our Azure cloud subscription	140
7 Elements Ltd	Backup data recovery	14
JBA	Laptop to enable review of consultancy report	2
Sub-Total:		**1,175**

OTHER		
ORGANISATION	**SUMMARY**	**£'000**
SEPA	Direct increased cyber related staff overtime costs	158
SEPA	Debtors As highlighted in the 2020-21 published Annual Report and Accounts, there was a residual £2,200k of debtors as at 31 March 2021 for which no cash had been received by end of August 2021. Management have fully provided against this balance on the assumption that income will not be received. Some of the debt will be associated with the impact of the Covid Pandemic. We have estimated the split to be: • Pandemic – 40% (£880k) • Cyber – 60% (£1,320k)	1,320
Sub-Total:		**1,478**

COSTS BROUGHT FORWARD FROM FUTURE YEARS		
This represents expenditure that SEPA would have incurred in future years as part of its digital transformation work.		
ORGANISATION	**SUMMARY**	**£'000**
CompanyNet	Establishment of emergency Microsoft services.	60
CompanyNet	SharePoint development and rollout.	312
Softcat	MS365 Package	250
Insight	Pure Storage units backup	200
Vodafone	Vodaphone Contact Centre Management System	308
Sub-Total:		**1,130**

NOTES

- On 24 December 2020, SEPA was the victim of serious and significant cyber-attack orchestrated by international serious and organised criminals. Whilst our story is not unique, we were clear that we would not use public funds to meet a ransom request and that we would share our learnings widely.

- Supported by the Scottish Government, Police Scotland, the National Cyber Response Centre and Scottish Business Resilience Centre, SEPA commissioned independent reviews into our readiness, resilience, response and recovery, which we published in October last year.

- Whilst both the reviews and Audit Scotland found that SEPA's cyber maturity assessment was high and that sophisticated defence and detection mechanisms were implemented and operating correctly prior to the incident, they identified a series of recommendations for the public sector, and (in the case of the independent audits) 44 learnings for SEPA. All the learnings were accepted.

- SEPA is working to a clear Corporate Plan and Annual Operating Plan, with a refreshed Annual Operating Plan due for publication in May 2022.

- The summary above is of direct costs in responding and recovering from serious and significant cyber-attack by international serious and organised criminals on Christmas Eve, 2020.

- The values provided are derived from invoice, purchase order and payroll information.