Public Audit Committee

9th Meeting, 2022 (Session 6), Thursday, 17 March 2022

The 2020/21 audit of the Scottish Environment Protection Agency

Introduction

1. On 10 February 2022, the Public Audit Committee took evidence from the Auditor General for Scotland on his Section 22 report on The 2020/21 audit of the Scottish Environment Protection Agency which was published on 1 February 2022.

2. The Committee will take evidence at its meeting today from the Scottish Environment Protection Agency (SEPA) and the Scottish Government.

3. SEPA have provided a written submission, which, along with a copy of the report, can be found in the Annexe.

Clerks to the Committee
14 March 2022

Annexe

WRITTEN SUBMISSION FROM SEPA

Summary

On Christmas Eve 2020, SEPA was the victim of a sophisticated criminal cyber-attack which significantly impacted the organisation. An Emergency Management Team was quickly activated to plan and implement priority actions. The past year has been a very tough one that has seen two key phases of work:

Phase 1 - Response - an immediate response period to June 2021 that focused on the continuity of key services for communities and businesses and bringing all of our staff back online; and

Phase 2 - Recovery – a period from June 2021 to date which has focused on stabilising and recovering the most critical systems and services.

While our key services have now been stabilised, it is important to recognise that SEPA remains significantly impacted by the attack. There are tough choices ahead about what we build back and how and where we invest in new systems and technologies.

While these big challenges remain, they are also opportunities: a chance to reflect on what we *really* need in order to deliver our services better and more efficiently with excellence, innovation and resilience at their core.

We are therefore now moving into a *third phase: a phase of building anew*. This phase recognises that we can't do everything at once but also that enables those tough choices to be made and that accelerates the transformational changes to the Agency we were already embarking upon.

1. Background

SEPA's statutory purpose is to protect and improve the environment in ways that, as far as possible, also help create health and well-being benefits and sustainable economic growth. We do this through the delivery of two core functions:

Regulation – Ensuring that regulated businesses comply with Scotland's environmental laws.

Flooding – SEPA is Scotland's national flood forecasting, flood warning and strategic flood risk management authority.

2. The cyber-attack

On Christmas Eve 2020, SEPA was the victim of a serious and significant ransomware cyber-attack orchestrated by international serious and organised criminals which significantly impacted the organisation.

The attack displayed significant stealth and malicious sophistication with a secondary and deliberate attempt to compromise systems as the team tried to recover and restore back-ups. It resulted in the loss of access to the vast majority of our systems and data which significantly impacted our staff, our public and private partners, and the communities and businesses who rely on our services.

SEPA did not respond to the ransom request and was clear from the start that it would not use public finance to pay serious and organised criminals.

An Emergency Management Team was quickly activated to plan and implement priority actions. A multi-agency group was also convened by the Scottish Government and which included Police Scotland and the National Cyber Security Centre to ensure that we got the widest possible support.

In February, SEPA prepared a response and recovery plan of 103 immediate and longer-term projects for the period to July 2021. This focused on the continuity of key services for communities and businesses and on bringing all of our staff back online.

We published a weekly service status that detailed progress on recovering our affected services so that we were clear with those that we work with what level of service they could expect and how we were prioritising progress.

In early July 2021, once the immediate priorities were complete, we published an Annual Operating Plan which set out remaining projects for the year, including those from the 103 still in progress. We have twenty performance measures in the plan which we continue to use to monitor progress.

At this time, we are still in the process of understanding the full financial impact of the cyber-attack. It is our intention to publish this shortly.

Throughout our recovery we have set a high level of transparency so that as many organisations as possible can use our experience to better protect themselves. In October 2021, we published the findings of independent audits commissioned to review the attack and our response. Whilst the reviews 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 44 learnings for SEPA.

All the learnings were accepted. To date, 35 have been implemented and good progress is being made on the remaining nine. With these learning points now integrated into our work, we have significantly increased our cyber awareness and resilience.

We remain fully committed to working with and helping others to learn from our experiences. We will therefore continue to do everything we can to share our experiences and help others to build their resilience and awareness so that they do not have to go through what we have been through.

3. Continuing to deliver services after the attack

While the impact of the attack was significant, resilience planning and clear prioritisation of actions ensured that our key critical services were restored as quickly as possible. This included:

- *Flood forecasting and warning* – Data were initially processed manually to allow this service to continue and real time flood alerts were issued less than 24 hours after the attack.
- *Incident response* - our 24-hour pollution hotline was quickly re-established and we maintained our ability to attend environmental incidents, prioritising those with the highest potential impacts on the environment and/or communities. Since the attack SEPA has attended around 1,200 in-person environmental event responses.

- *Monitoring compliance* – Within the restrictions placed by Covid, we continued to monitor compliance through desktop checks and site visits. This work was prioritised to illegal activities and sites of high hazard, with significant non-compliance or with the potential for high community impact. We continued to take action against those who do not comply and we continued to take enforcement action where necessary.
- *Bathing waters* – We successfully monitored Scotland's designated bathing waters throughout the 2021 season, providing the public with sampling results for all 85 beaches and, for 29 popular sites, real time water quality predictions.
- *Covid-19 monitoring* – We continued our work to monitor Covid through its genetic footprint in wastewater. We quickly restored capability to analyse 200+ samples a week from wastewater treatment sites across Scotland to support the national programme to monitor the virus.
- *Financial management* – We immediately put in place interim arrangements to pay staff and allow basic financial management. We have now stabilised our core financial systems and have in place appropriate financial controls, tools and data to allow us to report. A replacement system went live in August 2021 that allows us to pay staff, pay suppliers, issue invoices to charge payers and undertake financial performance reporting.

While work through 2021 focused on building organisational capability, the continued delivery of these and other services for the communities we serve and the businesses we regulate was prioritised.

To do this, our staff have worked incredibly hard. Unable to rely on usual systems and processes – and while also working under restrictions imposed by the pandemic - they have improvised, collaborated, and used their knowledge and creativity to find different, and sometimes better ways of delivering our services.

Supporting our staff through the attack was - and remains - a vitally important part of our recovery. We have also received a lot of support and understanding from partners, including the Scottish Government and UNISON, which has been invaluable.

4. One year on: Moving to a new phase

While we were able to deliver our priority services through 2021, it is important to recognise that SEPA remains significantly affected by the attack. While our most critical systems have been built back, many supporting systems and datasets have not. There are tough choices ahead of us about what we build back and how and where we invest in new systems and technologies.

But these challenges are also opportunities: a chance to reflect on what we *really* need in order to deliver our services better and more efficiently with excellence, innovation and resilience at their core.

We are therefore now moving into a different phase: a phase of building anew. This phase recognises that we can't do everything at once, but that also enables those tough choices to be made and that accelerates the transformational changes to the

Agency we were already embarking upon. Doing so will take time and careful planning.

We have already extended our [Corporate Plan](#) for a further year to give us stability and are currently preparing an Annual Operating Plan that will set out our priorities and actions for 2022/23. The Annual Operating Plan will establish the things we will focus our resources and time on in order to build back in a way that improves the services that we provide.

This phase will therefore set us up for long term success: building up a new network, developing new techniques based in the cloud and integrating the best security standards. This digital transformation will allow our services to be more accessible online, making it quicker and easier for communities and businesses.

Being the victim of a significant crime that devastated our systems has meant that the past year has been very painful and one which has had a profound impact on our staff. As we begin to emerge into this third phase of building anew, we are optimistic that we will emerge with better, stronger and more resilient systems that enable us to become a regulator that can powerfully tackle the environmental issues we face today such as helping the nation to transition to net zero emissions.

The 2020/21 audit of the Scottish Environment Protection Agency

Introduction

1. I have received the audited annual report and accounts and the independent auditor's report for the Scottish Environment Protection Agency (SEPA) for 2020/21. I am submitting these financial statements and the auditor's report under section 22(4) of the Public Finance and Accountability (Scotland) Act 2000, together with this report that I have prepared under section 22(3) of the Act.

2. The auditor issued a disclaimer of opinion on SEPA's annual report and accounts for 2020/21. The auditor was unable to obtain sufficient audit evidence over certain transactions and balances within the financial statements. This was due to a cyber-attack and subsequent data loss on 24 December 2020 which resulted in SEPA being unable to retrieve a significant amount of its data, including underlying financial records.

3. I have prepared this report to draw the Scottish Parliament's attention to these issues and to highlight a number of lessons that can be learned from this cyber-attack.

Key messages

1 SEPA was the victim of a sophisticated ransomware attack on 24 December 2020. This led to SEPA being unable to access a significant amount of its systems and data. SEPA did not pay the ransom. More than twelve months on, it is still reinstating some of its systems. It was able to prioritise and find ways to continue delivering key services such as issuing flood alert and flood warnings within 24 hours of the attack.

2 SEPA had to recreate accounting records from bank statements and HMRC records. The auditor issued a disclaimer of opinion on the financial statements as they were unable to obtain sufficient audit evidence to substantiate £42 million of income from contracts.

3 SEPA's management is in the process of understanding the full financial impact of the cyber-attack on the organisation. Management is planning to bring forward the delivery of its digital strategy, focusing on creating a better, more resilient infrastructure to achieve longer-term benefit.

4 SEPA commissioned a number of independent reviews to assist it and other public sector organisations in learning from the incident and help protect itself and others from ongoing cyber threats. The reviews concluded that SEPA had a high level of cyber maturity. They identified areas for further improvement and SEPA has accepted and is addressing the recommendations made in the reviews.

Background

4. SEPA is a non-departmental public body of the Scottish Government and is sponsored by the Directorate of Environment and Forestry. SEPA's role is to protect and improve the environment and human health and contribute to sustainable economic growth. It provides two core functions:

- **Environmental regulation**: SEPA has regulatory powers and duties. SEPA helps businesses to reduce water use, carbon-based energy use, and all forms of waste and pollution, and to comply with required standards. It is the regulator of the Scottish Landfill Communities Fund and supports Revenue Scotland with the administration and collection of the Scottish Landfill Tax.

- **Flood risk management:** SEPA is Scotland's national flood forecasting and warning authority and strategic flood risk management authority.

5. SEPA employs 1,268 people who are based around Scotland. It is funded by Grant-in-Aid from the Scottish Government (£37.6 million 2020/21), income from contracts such as license fees paid by businesses and individuals (£42 million, 2020/21), and other income (£1.8 million 2020/21). In 2020/21, SEPA underspent against its departmental expenditure budget by £1.3 million. However, the auditor was unable to obtain sufficient audit evidence that income from contracts, and related transactions, were free from material misstatement and issued a disclaimer of opinion on the financial statements.

Timeline of the cyber-attack

6. SEPA experienced a sophisticated ransomware attack on 24 December 2020. Employees and customers were unable to access SEPA's systems and data because malware (malicious software) had been installed by external agents after they gained access to the system. The majority of SEPA's data, was encrypted, stolen or lost.

7. SEPA immediately implemented its emergency management arrangements in response to the cyber-attack. It re-established its Emergency Management Team (EMT) to oversee the agency's response and worked with the Scottish Government, Police Scotland, the National Cyber Security Centre (NCSC) and the Scottish Business Resilience Centre (SBRC) to deliver a recovery strategy. Appendix summarises the key timeline of events and SEPA's response.

Independent reviews found that SEPA had a high level of cyber security maturity, but further improvements could be made

8. SEPA commissioned independent reviews of the cyber-attack so that it, and the wider public sector, could learn lessons. Police Scotland, SBRC and SEPA's internal auditors, Azets, were involved in the review process. The cyber-attack is subject to an ongoing police investigation.

9. The independent reviews made 44 recommendations for SEPA to enhance processes and controls in relation to information security. The key findings from the reviews and the auditor's follow-up discussions with management can be summarised under three areas:

- **Readiness** - How prepared and resilient were SEPA for a cyber-attack?

- **Response** - How efficient and effective were SEPA's arrangements in responding to the attack?

- **Recovery** - How effective are SEPA's arrangements in recovering from the incident and ensuring critical services continue to be delivered?

SEPA's readiness

10. The auditor reported that prior to the attack SEPA had been proactive in mitigating the risk of a cyber-attack. Police Scotland's review concluded that SEPA 'was not and is not a poorly protected organisation'. It noted that as a Category 1 emergency responder, SEPA had a culture of resilience, incident and emergency management and that it regularly tested its response capabilities. This included performing a trial cyber exercise. The SBRC review noted that SEPA's cyber maturity assessment was high with the 'implementation and adherence to recognised frameworks and the implementation of best practices'.

11. The auditor noted that due to the sophistication of the attack the investigations to date have not identified the exact route source of where the cyber-attack breached SEPA's systems. However, there are indications that it was through a **phishing attack**. This means there may have been a degree of human error involved, which is very difficult to mitigate against.

> **The NCSC defines phishing:**
> 'when attackers attempt to trick users into doing 'the wrong thing', such as clicking on a bad link that will download malware, or direct them to a dodgy website.'

Backups and data management

12. SEPA was unable to quickly restore its data from its backups. SEPA's backup policy was in line with best practice in that there were three copies of the data, located at two separate locations, with one copy stored offline. However, the sophisticated nature of the attack meant that online backups were targeted and corrupted at an early stage, meaning there was no way of accessing historical records quickly.

Staff awareness and training

13. The independent reviews identified opportunities for enhancing staff awareness and training over cyber risk. The SBRC review found that throughout the autumn of 2020, mandatory cyber training was provided and completed by around 95 per cent of staff. SEPA plans to further roll out training and awareness across the organisation.

SEPA's response

Escalation routes and communication

14. A SEPA staff member received a system alert at midnight on the morning of the 24 December 2020 and went to a SEPA office to investigate. They were unable to reach the key senior management contact to escalate the issue at this point.

15. At the same time operational staff from the contact centre and flood service reported that they were unable to access systems. However, the standard escalation procedures to report such issues did not include Information Services (IS). The independent reviews have concluded that the delays in escalating the issues did not delay the response to try and contain the issue and minimise the impact.

Leadership

16. SEPA is experienced in planning for and responding to emergencies. It has well-established governance arrangements in place to respond. Its EMT was reinstated on the morning of the attack and it engaged with partners including Police Scotland and the Scottish Government. It also notified the Information Commissioner's Office of the incident and potential data loss.

17. The EMT focused on ensuring critical systems such as the flood warning system were re-established. SEPA worked with the third parties who support the system to ensure the service continued to provide messages and alerts from that day.

18. SEPA has been open and transparent from the start to ensure that staff, the public and other public-sector organisations were aware what was happening. Due to the Covid-19 pandemic, most of SEPA's staff were working from home during this time. SEPA used a Business Continuity Messaging Service (BCMS) which was separate from its network to communicate with its staff.

19. The auditor reported that SEPA had a range of business continuity plans and incident response playbooks in place. However, these were stored on its systems and could not be accessed after the attack. Hard copies were kept in the office but only a limited number of staff could access them due to the Covid-19 restrictions. Management had to rely on their knowledge of SEPA's processes to coordinate its initial response. Had EMT and staff not been so familiar with its continuity plans and processes, its response may have been hindered. SEPA plans to establish new working practices to ensure it does not face these issues if there is a future incident.

Recovery

20. The EMT established a recovery plan and identified 103 projects to deliver between March and June 2021. These included the development of basic core and regulatory functions, such as rebuilding finance systems and processes, as well as investigatory and data recovery activity. SEPA also worked with key partners including Revenue Scotland to support the continued administration of the Scottish landfill taxes.

21. It will take time for SEPA to fully recover from the attack. It views this as an opportunity to accelerate the delivery of its digital strategy and get longer-term benefit. It has taken the decision to build from new rather than re-establish legacy systems. It aims to transform the way SEPA operates and delivers services.

Impact of the cyber-attack on financial management and the audit of the annual report and accounts

22. The auditor reported that prior to the cyber-attack SEPA had well-developed systems of internal financial control and reporting. However, the attack meant that SEPA could not access any of its financial systems and a significant amount of its data. This meant, since December 2020, Management has had limited financial information in which to monitor performance and make decisions as it prioritised re-establishing business critical systems.

23. SEPA was unable to record any income received or payments made or match them to pre-existing information held on its systems, such as sales and purchase orders. Many internal controls which management rely on, such as authorisation levels, are inbuilt into financial systems. Without these systems in place the control environment was weakened. Temporary financial arrangements were put in place to ensure there were appropriate controls and authorisation of expenditure, such as paying staff and suppliers.

24. The finance team had to recreate accounting records from the prior year trial balance and record transactions in manual journals. It created payroll/staff costs information from HMRC records, and income and expenditure information from bank records. There are inherent limitations in recreating records this way. It meant there was not the level of detail required to substantiate the completeness, accuracy and authenticity of financial transactions for 2020/21.

25. The auditor reported that, as part of SEPA's ongoing recovery activity, SEPA has sought to re-establish and further enhance its internal financial control arrangements.

The auditor issued a disclaimer of opinion on the annual report and accounts

26. As a result of the cyber-attack and subsequent impact on SEPA's underlying financial records, the auditor was unable to obtain sufficient evidence over income from contracts (£42.097 million) to gain assurance that this was free from material misstatement or fraud, including whether income had been receipted in the correct financial year. This also impacted on bad debts written off in year (£2.197 million) and the deferred income included within trade and other payables (£11.210 million) recorded in the Statement of Financial Position.

27. Income from contracts is a substantial proportion of income received in the Statement of Comprehensive Net Expenditure. As such, the auditor considered this issue to be pervasive to the financial statements as a whole and has provided a disclaimer of audit opinion on the financial statements.

SEPA does not yet know the full financial cost of the cyber-attack

28. Based on management forecasts during the year, the Scottish Government gave SEPA authority to overspend by £2.5 million to cover the impact of Covid-19 and the cyber-attack if required. However, as reflected in SEPA's outturn position (paragraph 5), it did not have to do so.

Financial sustainability

29. SEPA recognises that the cyber-attack has increased the medium to longer term financial pressures on the organisation. Its financial strategy 2020-24 had already identified potential variability in future income and expenditure streams of up to £17.9 million as a worst-case scenario. Fully restoring its financial analysis capabilities is essential to SEPA being able to manage this variability and associated risks.

30. For 2021/22, the Scottish Government has confirmed Grant-in-Aid funding can be used for the recovery and re-establishment of critical systems. SEPA's management has forecast a surplus of £6.2 million that will be used to support strategic investment.

Conclusions

31. The cyber-attack on SEPA's systems on 24 December 2020 was highly sophisticated and continues to have a significant impact on its operations and performance. SEPA continues to monitor its performance against 20 revised targets. It will be challenging for it to meet all of these in the coming year as it recovers and rebuilds.

32. Both the auditor and the independent reviews commissioned by SEPA have identified that the organisation had good cyber security arrangements in place, with a number of areas of good practice. These include, SEPA's quick response and business continuity arrangements that enabled it to continue delivering critical services, and its open and transparent communication with staff and the wider public.

33. The financial impact of this incident is not yet known and SEPA will continue to experience the consequences of this attack for a while to come. Key systems have been rebuilt, such as SEPAs financial accounting system, with others being built from new and data recovered or recreated securely, and this will take time.

34. The independent reviews identified a number of recommendations which SEPA's management has accepted. Public-sector bodies should review these recommendations and learn lessons from what has happened to SEPA. This incident highlights that no organisation can fully mitigate the risk of the ever-increasing threat and sophistication of a cyber-attack but it's crucial that organisations are prepared.

Appendix
Timeline of key events

Date	Event
Pre 24 December 2020	• Estimated date when the cyber-attack penetrated SEPA's systems. Investigations have yet to determine the original source of the attack. However, experts believe that it was most likely through a form of phishing email. • The attackers infiltrated SEPA's infrastructure undetected, leaving complex and sophisticated devices to encrypt and destroy data. This went undetected.
24 December 00:00	• The cyber-attack started with the majority SEPA's data and information being encrypted, stolen or deleted. • SEPA's backup policy was in line with best practise. However, the sophisticated nature of the attack meant that online backups were targeted and impacted in the early stages of the attack. • A SEPA staff member was alerted at home by automatic alarms and immediately logged onto the system to investigate. They then attended the office and, in a phased manner, began isolating and shutting down systems. • Operational staff, including flood warning team, escalated issues around accessibility of key systems.
24 December 08:00	• As the event took place out of hours, further escalation was not completed until early morning. • The Head of Governance was notified of the issue and contacted the IS team member who confirmed the attack. The issue was immediately escalated to the Chief Executive.
24 December 09:30	• An Emergency Management Team (EMT) meeting was established through the use of communications software held separately from SEPA's systems for business continuity purposes.
24 December 09:30-11:00	• EMT met to plan initial emergency response. • Scottish Government Cyber Resilience Unit (CRU) contacted. It initiated the national cyber incident response coordination arrangements providing structure and support at an early stage. • At 11:00 SEPA confirmed a serious and significant cyber-attack had occurred to staff, stakeholders and media. • Data breach reported to the Information Commissioner's Office (ICO). • Critical services maintained and essential flood warnings issued.
31 December	• Emergency SEPA Board meeting to discuss cyber-attack and planned response.

Date	Event
14-31 January 2021	• SEPA confirmed ongoing ransomware attack likely to have been carried out by an international serious and organised cyber-crime group intent on disrupting public services and extorting public funds. • Cyber security specialists identified the theft of circa 1.2 GB of data (equivalent to a small fraction of the contents of an average laptop hard drive). • Dedicated data theft support website, enquiry form and support line available for regulated business and supply chain partners. Data theft mitigation and support package made available to all staff. • SEPA identify and report that data stolen is likely to have been published illegally online and establishes arrangements to notify data subjects that may be affected.
28 January 2021	• SEPA develops its overarching approach to the delivery of services for the first half of 2021. • Weekly service status updates published online.
February – June 2021	• SEPA implements its recovery programme, covering 103 projects, focusing on establishing business critical systems and processes. • The projects are overseen by EMT and Board and includes recreating accounting records to support the 2021 financial statements as well as financial controls and processes for 2021/22.
27 October	• SEPA publishes its lessons learned reports and hosts a webinar - Cyber-crime: ready, resilient, and responsive.
Ongoing	• Next phase of recovery and delivery focusing on the building or buying of new systems and infrastructure, rather than rebuild legacy systems.

The 2020/21 audit of the Scottish Environment Protection Agency

Audit Scotland's published material is available for download on the website in a number of formats. For information on our accessibility principles, please visit:
www.audit-scotland.gov.uk/accessibility

For the latest news follow us on social media or **subscribe to our email alerts.**

✓AUDIT SCOTLAND

AS.4.0