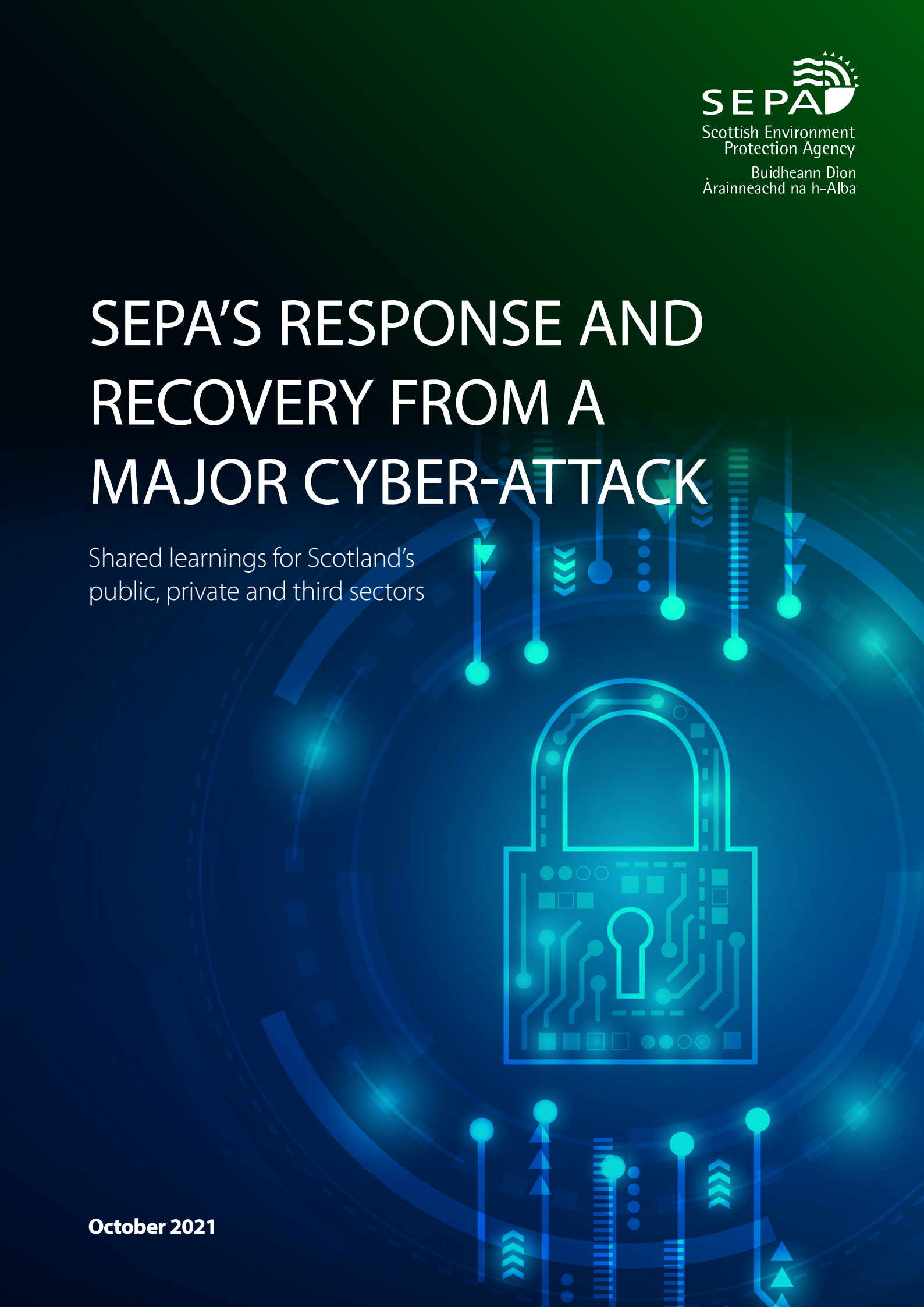
SEPA
Scottish Environment Protection Agency
Buidheann Dìon Àrainneachd na h-Alba

SEPA'S RESPONSE AND RECOVERY FROM A MAJOR CYBER-ATTACK

Shared learnings for Scotland's public, private and third sectors



October 2021

For information on accessing this document in an alternative format or language please either contact SEPA by email, equalities@sepa.org.uk

If you are a user of British Sign Language (BSL) the Contact Scotland BSL service gives you access to an online interpreter enabling you to communicate with us using sign language. contactscotland-bsl.org

www.sepa.org.uk
Strathallan House, Castle Business Park, Stirling, FK9 4TZ

Foreword

Terry A'Hearn
Chief Executive
27 October 2021

On the morning of Christmas Eve last year, I received a call from our Head of Governance who told me the disturbing news that we had been hit by a major cyber-attack overnight. Under our emergency management procedures, I immediately established an Emergency Management Team to lead the organisation through this new emergency. We met three times that first day. Over the next few months, SEPA worked through our initial emergency response and onto general recovery and building up of the organisation's capacities.

Unfortunately, SEPA's story is not unique. Cyber-crime has rapidly expanded around the world. Major organisations such as Apple, the Irish Health Service, LinkedIn, Colonial Pipeline, CitiBank, Sony and many more have been hit by cyber-attacks. It is a hideous crime that has an impact on an organisation, its staff and the external organisations and people who work with it and rely on it.

In the face of this awful crime committed against SEPA, I am immensely proud of the way our team has coped and responded. We have delivered high-priority services to protect Scotland's environment and started building all our services up in new and better ways. In the end, we will have fast-tracked major reforms we had set out to do anyway. In all this work, as CEO of SEPA, I want to acknowledge and thank the outstanding efforts of our workforce and the assistance we have received from partners and all those we regularly work with.

A key element of our recovery has been to set a high level of transparency in our work. On the very first day, we alerted national media and the public to the cyber-attack so that people at least knew we had been affected. From then on, we have published material, including weekly service updates for several months as one example of the many ways we have kept people informed about our recovery and how to work with us.

In line with this approach, I commissioned independent expert reviews of the cyber-attack in order to help:

1. **ensure that SEPA further enhances our cyber security as we build new systems and practices.**
2. **others learn from our experience to help better protect themselves from cyber-crime.**

No one asked us to commission multiple reviews. No one required us to do so. We simply took the view that this was our responsibility as a public agency.

The majority of organisations hit by cyber-attacks around the world do not publicise much about the attack. Each organisation needs to make its own decisions in its own circumstances and I make no judgement at all about the approaches other organisations have taken. What they judge to be right for them is, by definition, right for them.

We know we have taken an unusual approach, but we are convinced it is the right thing for us to do. We are publishing as much as we can of the reviews so that as many organisations as possible can use our experience to better protect themselves from this growing scourge of cyber-crime.

Information has only been redacted that meets the following legal and governance criteria:

- Evidence related to ongoing criminal investigations.
- Personal information or information that could identify an individual.
- Information that could cause substantive prejudice to SEPA's ability to deliver on our statutory purpose including that relating to SEPA's current or future cyber security arrangements.

I encourage you to read the reviews and take from them whatever lessons you think will help.

Finally, I would like to thank the staff of Police Scotland, the Scottish Business Resilience Centre and Azets for their dedicated work on the reviews and to our colleagues in Scottish Government and my own team for the work to support the review process.

Terry A'Hearn
SEPA Chief Executive Officer

In the face of this awful crime committed against SEPA, I am immensely proud of the way our team has coped and responded.

Scotland's Environment Protection Agency

- Founded in 1996, the Scottish Environment Protection Agency (SEPA) is Scotland's principal environmental regulator.
- As a non-departmental public body of the Scottish Government, our role is to make sure that the environment and human health are protected, to ensure that Scotland's natural resources and services are used as sustainably as possible and contribute to sustainable economic growth.
- Through the delivery of One Planet Prosperity we are committed to making Scotland stronger. We work with Scottish businesses to ensure they comply with Scotland's environmental laws, and we work to ensure as many as possible will go even further.
- We also help Scotland to prepare more powerfully for future increased flooding and are the national flood forecasting, flood warning and strategic flood risk management authority.
- With around 1,300 people based across Scotland, from the Highlands and Islands to the Borders, we regulate and advise on a wide range of environmental activities.

SEPA's recovery

In the last 10 months we have

DELIVERED SCOTLAND'S COVID-19 WASTE WATER TESTING PROGRAMME

SUPPORTED SCOTLAND'S BATHING WATER SEASON, ASSESSING

85

DESIGNATED BATHING WATERS

ISSUED WEEKLY

WATER SCARCITY REPORTS

LAUNCHED NEW, SIMPLER DIGITAL REGISTRATION SYSTEMS

PROGRESSED THE REMEDIATION OF DALGETY BAY

CONSULTED ON

14

FLOOD RISK MANAGEMENT PLANS

COMPLETED

OVER 5,000

AUTHORISATIONS (I.E. PERMIT AND LICENSE APPLICATIONS)

RESPONDED TO ALL **CATEGORY ONE** and **CATEGORY TWO** ENVIRONMENTAL INCIDENTS

ISSUED

182

FLOOD ALERTS AND

191

FLOOD WARNINGS

IMPLEMENTED A FRAMEWORK TO TRIAGE PLANNING AND DEVELOPMENT CASES, CLEARING THE PLANNING BACKLOG AND

RESPONDING TO

1,413

PLANNING APPLICATIONS

DEVELOPED ACTION PLANS FOR

35

COMMUNITY IMPACT SITES

International serious and organised cyber-crime

- In June 2021, following his inauguration six months earlier, the President of the United States of America, Joe Biden, met the President of the Russian Federation, Vladimir Putin in Geneva. Officials reported that top of the agenda was international cyber-crime, with President Biden being clear that attacks on critical infrastructure should be "off-limits".
- London Business School examined comments by investors in 12,000 listed firms in 85 countries over two decades. The study concluded that cyber-risk more than quadrupled since 2002 – and tripled since 2013. The pattern of activity has become more global and has affected a broader range of industries. Between the 1 October 2019 and 30 September 2020, 59% (global average) of organisations detected attackers within their own environments. This was a 12% increase over the previous year. Victims have ranged from Apple and LinkedIn, to Sony Pictures, Marriot Hotels, Colonial Pipeline, Citi Bank, JP Morgan Chase.
- Closer to home, victims have ranged from the NHS, Hackney Council, Tesco and Talk Talk, to Ireland's Health Services, Dundee and Angus College, Aspire Housing Association and, most recently, The Weir Group.

Image ©

- In the UK Cyber Security Breaches Survey 2021, four in ten businesses (39%) and a quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months. Like previous years, this is higher among medium businesses (65%), large businesses (64%) and high-income charities (51%).
- Scottish Business Resilience Centre (SBRC) states that in the fourth quarter of 2020, attacks utilising PowerShell grew by 208% while malware leveraging Microsoft Office increased by 199%. The same study also identified that attacks targeting public sector entities increased by 93%.

Timeline: key milestones

From Christmas Eve onward, there was a huge amount of activity directed by SEPA's Emergency Management Team every single day. The timeline below lists a handful of the key actions that were taken to provide some flavour of the nature of the initial response over the first two months.

DEC 2020

Post-attack analysis identified that a data theft had taken place shortly before the ransomware was activated at 00:01hrs on Christmas Eve.

CHRISTMAS EVE 2020

SEPA targeted by likely international serious and organised crime ransomware attack.

SEPA's Emergency Management Team (EMT) met at 09:30hrs.

Contact was made with the Scottish Government Cyber Resilience Unit (CRU) which instigated the national cyber incident response coordination arrangements providing structure and support at that early stage. By 11:00hrs on Christmas Eve, a multi-agency partnership was beginning to form.

SEPA confirms serious and significant cyber-attack to staff, stakeholders and media.

Critical services maintained and essential Flood Warnings issued.

Data breach reported to the Information Commissioner's Office (ICO).

31 DEC 2020

Emergency Special SEPA Board meeting held.

7 JAN 2021

SEPA confirms that cyber-attack is ongoing and that the agency is continuing to work with Scottish Government, Police Scotland and the National Cyber Security Centre.

14 JAN 2021

SEPA confirms ongoing ransomware attack likely to be by international serious and organised cyber-crime groups 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.

21 JAN 2021

SEPA confirms that data stolen by what was likely to be international serious and organised cyber-crime groups has now been illegally published online. Work to notify and support data subjects.

28 JAN 2021

SEPA sets out overarching approach to the delivery of services for the first half of 2021 and published the first in a series of weekly service status updates available at sepa.org.uk/servicestatus

23 FEB 2021

SEPA Chief Executive Terry A'Hearn speaks out on readiness, response and recovery during Scotland's Cyber Security Week with:
David Ferbrache OBE – Chair – National Cyber Resilience Advisory Board, The Scottish Government;
Malcolm Graham – Deputy Chief Constable;
Crime & Operational Support – Police Scotland;
Prof Ciaran Martin CB – Former Chief Executive Officer – National Cyber Security Centre (NCSC);
Jude McCorry – CEO – Scottish Business Resilience Centre.

ONGOING

SEPA issues further update and continues weekly service status updates available at sepa.org.uk/service status

Executive summary

- Working with Scottish Government, Police Scotland, the National Cyber Security Centre (NCSC) and the Scottish Business Resilience Centre (SBRC), SEPA worked to a clear recovery strategy in response to a complex and sophisticated cyber-attack.
- SEPA was clear that it would not use public finance to pay serious and organised criminals intent on disrupting public services and extorting public funds.
- Police Scotland has been clear that "SEPA was not and is not a poorly protected organisation".
- Within the confines of a criminal investigation, SEPA was vocal and transparent on the criminal attack, the theft and illegal publication of data, the impact on our services and progress towards its recovery.
- Since Christmas Eve, teams across the agency worked flat-out to support our staff, partners and customers and to restore our systems and services as quickly as possible.
- SEPA knew that communities and citizens depend on public services which is why, even on Christmas Eve, the organisation prioritised critical frontline services including vital Flood Warnings to safeguard families, communities and public services.
- SEPA issued weekly updates on recovery and service status to be clear on what those it worked with could expect and how it would prioritise progress whilst continuing to listen to staff, customers, communities and stakeholders.
- Sadly, as seen from attacks including Irish Health Service, cyber-crime is an increasing challenge for businesses and public sector partners. It is clear that service recovery takes time.
- Through SEPA's experience, it is highlighting and speaking openly about international serious and organised cyber-crime. It is sharing the learnings widely so that the organisation, and all others with an interest, can benefit from its experience in readiness, response and recovery.
- SEPA's CEO commissioned independent expert reviews of the cyber-attack in order to help:
  - ensure that SEPA further enhances its cyber security as it builds new systems and practices.
  - others learn from its experience so they can better protect themselves from cyber-crime.
- No one asked SEPA to commission multiple reviews. No one required SEPA to do so. SEPA simply took the view that this was its responsibility as a public agency.
- SEPA has published:
  - Police Scotland (Cyber-Attack Response Debrief)
  - Scottish Business Resilience Centre (Cyber-Attack Preparedness Review)
  - Azets (Cyber-Attack: Response; Cyber-Attack: Lessons Learned)
  - SEPA's response and recovery from a major cyber-attack
- SEPA is publishing as much as it can of the reviews so that as many organisations as possible can use the experience to better protect themselves from this growing scourge of cyber-crime. Information has only been redacted that meets the following legal and governance criteria:
  - Evidence related to ongoing criminal investigations.
  - Personal information or information that could identify an individual.
  - Information that could cause substantive prejudice to SEPA's ability to deliver its statutory purpose including that relating to SEPA's current or future cyber security arrangements.
- A series of learnings were identified for Scotland's public sector.
- 44 learnings were identified for SEPA. All have been accepted.
- The learnings are the focus of a joint SEPA, SBRC and FutureScot online event, 'Cybercrime: Ready, Resilient & Responsive', held on 27 October 2021 for public, private and third sector stakeholders.

Even on Christmas Eve, the organisation prioritised critical frontline services.

Key learnings

Summary

- Police Scotland investigation confirmed that the attack was likely perpetrated by international serious organised criminals utilising sophisticated 'Ransomware' tactics and techniques.
- Police Scotland acknowledged that this incident could happen to any sector, organisation etc. on the basis that there is a clear and real threat.
- SBRC noted that the attack displayed significant stealth and malicious sophistication with a secondary and deliberate attempt to compromise SEPA systems as the team endeavoured to recover and restore back-ups.
- Azets found SEPA's response following the triggering of the ransomware on December 24 2020, to be effective. SEPA communicated clearly and regularly with stakeholders, quickly mobilised an Emergency Management Team to lead on the response to the attack, engaged with support partners, and identified critical business processes for prioritisation purposes. In addition, SEPA's leadership issued effective communications from the first day of the attack, the CEO took a visible lead in efforts to respond to the attack and SEPA has created procedures to ensure that security is built into projects going forward.

Leadership and Commitment

- Azets found that the CEO played a significant and high-profile role in leading SEPA's response to the cyber-attack. The Emergency Management Team was chaired by the CEO and included various other members of the Agency Management Team who were involved in evaluating the situation and making key decisions. Unison, SEPA's recognised Trade Union, also sat on the Emergency Management Team.

Readiness

- Police Scotland found that as a Category 1 responder, SEPA had a strong culture of resilience, governance, incident and emergency management. As such, it regularly tested its emergency response capability and had undertaken a trial cyber exercise. The context of the event was unique in terms of the combined potential impact from EU Exit, the ongoing COVID pandemic and the impact that that was having on 'normal' working practices, such as working from home etc.
- SBRC determined SEPA's cyber maturity assessment as high with the implementation and adherence to recognised frameworks and the implementation of best practices with the recognition that complete cyber security to prevent such an attack is aspirational. No implementation regime can be 100% secure.
- SBRC found that sophisticated defence and detection mechanisms were implemented and operating correctly prior to the incident.
- SBRC noted that none of the parties interviewed had any concerns with regards to the security of SEPA's infrastructure prior to the incident. All respondents indicated that they believed the posture was quite advanced with regards to cyber security, especially when comparing themselves against other public sector organisations.
- SBRC noted that their review identified a most positive eagerness at executive level and within the Information Security provision to mature SEPA's cyber security posture by obtaining Cyber Essentials + accreditation. In addition, SEPA had implemented various components within the Information Technology Infrastructure Library framework to assist with governance and management of its IT processes.
- SBRC noted that senior managers had attended external cyber resilience training. Throughout the autumn of 2020, mandatory cyber training was also provided and completed by 1,252 staff with 70 remaining outstanding.
- SRBC and Azets recommended that SEPA investigate options for the engagement of a 24-hour Security Operations Centre (SOC).
- Police Scotland recommended that SEPA and the wider public sector organisations within Scotland should consider the value of retaining a Cyber Incident Response (CIR) specialist company to ensure availability of the necessary expertise at the earliest opportunity.
- Police Scotland recommended that SEPA and the wider public sector organisations within Scotland should 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 theft attack.
- Police Scotland recommended that Scottish Government Cyber Resilience Unit in collaboration with key stakeholders should 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 proactive approach to the identification of learning and an appropriate 'end-to-end' process that ensures learnings identified become lessons learned and that they are captured within a single repository and communicated accordingly.

Response

- Police Scotland noted a high quality of response provided by SEPA.
- Police Scotland found that the stand-up of national cyber incident coordination arrangements worked well.
- Police Scotland found that to assist with the criminal investigation and support recovery efforts, a number of organisations collaborated in a coordinated manner.
- SBRC recognised SEPA for being open and honest about their learnings during this horrific period, and for the way they collaborated and used the expertise among all the agencies in a collaborative way. For being an organisation that "Team Scotland" wanted to help. They noted there has been a huge collective and a "want to" effort among the agencies to support SEPA. Everyone SBRC dealt with commented on the camaraderie and commitment within SEPA and also the way SEPA employees and executive team dealt with all the agencies and also conducted themselves externally, which is admirable with everything that has been going on internally at SEPA around this attack. They also thanked SEPA for undertaking this "lessons learned as the learnings of this attack will aid discussions going forward around the establishment of the proposed Cyber Centre of Excellence", and also the help they have given to other organisations who are going through the pain of an attack.
- Police Scotland identified that reaching out to multi agency partners and organisations relied on personal contacts due to an inability to access Business Continuity Plans (BCP) and contact databases held on SEPA's network. It was also difficult to be sure that the right contact points within partner agencies were being reached where there were no established relationships or contacts e.g. specialist cyber security consultants.
- Azets identified that emergency management and incident management procedures were not stored offline and offsite. This meant that procedures became inaccessible when system access was lost, and staff had to rely on their knowledge and experience to carry out emergency management and incident management steps.
- Azets found that staff responded to the attack just after midnight on 24 December 2020 but could not escalate it to normal escalation contacts until the morning. During this period the on-call staff followed the arrangements in place and worked to analyse the alert and start to carry out containment procedures. They recommend that SEPA improve awareness and communications between incident management and emergency management to all staff. If staff are part of an escalation route for emergency procedures, then they must be contactable even when out of hours.
- Police Scotland recommended that as part of ongoing review of existing Cyber Incident Response Plans, SEPA and the wider public sector organisations within Scotland should 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.
- Police Scotland noted that 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.

A Strategic Plan

- Police Scotland noted that "taking the time at an early stage in the incident to step back and produce a broad plan with long term targets, rather than reacting to events as they unfolded was extremely valuable. This plan allowed SEPA to manage expectations with internal and external partners and also helped focus requests for support from external partners. In addition, it provided the strategic backdrop for key decision-making sessions with the Emergency Management Team to allow SEPA to begin rebuilding new systems.
- Following the cyber-attack on Christmas Eve, SEPA enacted its business continuity arrangements and took immediate action to limit the impact of the incident. The Emergency Management Team met early on Christmas Eve and appointed an Incident Manager. Its initial focus was on establishing a situational report on the scale of the incident, protecting systems, assessing the impact on business critical services, and initiating a multi-agency response, with Police Scotland.

  SEPA set out clear external priorities:

  - Protecting Scotland's environment.
  - Providing priority services to individuals and businesses across Scotland.

  SEPA moved to set a clear Recovery Plan for the period March to June 2021. This was followed by the publication of a revised Annual Operating Plan in July 2021, which clearly set out clear priorities for the remainder of 2021 - 2022.

Protecting Critical Services

- Police Scotland recognised a number of SEPA's key business critical services (i.e. flood forecasting and warning and pollution hotline) were maintained despite the core network being offline. This was due to the structures and processes implemented by SEPA as part of its resilience planning.
- Police Scotland acknowledged that this is best practice and enabled SEPA to maintain essential business services in the early stages of the attack, the question as to the ability of other sectors to do the same was raised.

Backups

- SBRC noted that backups were taken in line with NCSC best practice in that there were three copies of the data, located at two separate locations, with one copy stored offline. However, the design of the network meant that both sites were affected. This attack displayed significant stealth and malicious sophistication with a secondary and deliberate attempt to compromise SEPA systems as the team endeavoured to recover and restore backups.
- SBRC identified SEPA implemented best practice in backup policy following the 321 principles, however, could have achieved greater maturity with increased offline storage capacity and speed. Similarly, best practice was identified in Network Segmentation where stricter management and filtering controls across the network would advance SEPA's cyber maturity.

Data Theft and Illegal Publication

- Police Scotland found that the data publication on the threat actor's site was picked up quickly.
- Police Scotland noted that taking the advice from the co-ordination group discussion SEPA developed a data recovery plan in anticipation of the data being published and enacted this. SEPA as a regulator with enforcement capability has certain skills sets around investigation which assisted in this process.
- Police Scotland further noted that, as the victim, the advice and support provided to SEPA [by partners] was invaluable in terms of the data breach and managing the statutory responsibilities in this regard which enabled SEPA to risk assess and mitigate accordingly.
- Police Scotland and SEPA are fortunate in terms of the skills sets within the organisations however, undertaking a data recovery plan may prove difficult where the necessary skills are not present within the organisation.

Cyber Incident Response External Partner

- Police Scotland found that the partnership between SEPA, Police Scotland, Cyber Incident Response (CIR) Company, the NCSC and Scottish Government worked well and there were a number of structured meetings held to capture feedback.
- Police Scotland found that in the early stages of the incident liaison between Police Scotland and SEPA's external cyber response partner did not take place as quickly as Police Scotland would have preferred. This was due to the CIR company following usual practice and working to their client ensuring permissions to share data went through the client. This was quickly rectified by SEPA by authorising the direct exchange of relevant information from the CIR company to Police Scotland.
- Police Scotland found that in significant cyber incident investigations it may be beneficial for Police Scotland, the victim organisation and CIR company to agree parameters at the outset to enable Police Scotland to engage the CIR directly to facilitate the flow of critical information to support incident, intelligence and investigation needs.

Our Staff

- As noted previously, Police Scotland recognised the role of staff in ensuring a number of SEPA's key business critical services (i.e. flood forecasting and warning and pollution hotline) were maintained despite the core network being offline.
- Azets noted that the commitment and dedication shown by SEPA staff during the response has been significant. Staff have worked well beyond their normal hours and have demonstrated considerable flexibility, have worked through or given up annual leave, and public holidays.
- Azets noted that senior leaders of SEPA placed emphasis on staff wellbeing and emotional resilience. This was through having a proactive approach in place to manage employee wellbeing and communications.
- SBRC engaged with staff directly involved in the response. Those interviewed represented less than one percent of the organisation. Whilst 100% of interviewees responded that they felt respected in their workplace and 80% of respondents felt that the organisation cared about them, the review identified a moderate to low morale posture prior to the incident which increased during the incident, as everyone had a single focus and drive, but which decreased in the aftermath of the incident. This latter fall was attributed to bureaucracy and processes.

Speaking Out for Scotland

- Police Scotland found that SEPA had engaged previously with a number of Scottish Government digital education programmes and forums which proved valuable in terms of contacts and knowing what questions to ask. Whilst such programmes assisted in providing confidence and active consideration as to all the preparatory measures that could be taken, this incident proved to challenge such measures.
- Police Scotland found that the education sector had been attacked prior to SEPA however no learning from that particular attack had been shared to date which would have been helpful.
- Azets noted effective communication with internal and external stakeholders following the attack.
- Azets further noted that communications with stakeholders were transparent and concise. Stakeholders were regularly updated. Communications were specific to the needs of each type of stakeholder.
- Police Scotland noted that SEPA and Police Scotland established a communications team which was effective both in terms of internal and external communications, adopting a flexible approach in this regard.
- Police Scotland noted that the communications cell between SEPA and Police Scotland was one of the most successful aspects of the response and the advice and support provided by Police Scotland was key.
- Police Scotland noted that despite SEPA's network being offline, the SEPA senior management team did an excellent job on their communications plan and identifying their priorities. There was evidence of strong and clear leadership. This helped the multi-agency co-ordination group perform its function. Furthermore, SEPA was realistic in understanding the extent of the scale of the attack and did not try to minimise this to key partners.

Building Back Better

- Azets found that since the attack, SEPA has pro-actively worked to ensure that security is built into new processes and systems to limit the impact of a future attack.
- SBRC concluded that SEPA should not recover unsupported systems to a production state.
- The criminal cyber-attack was not a change opportunity SEPA wanted, but it is one the agency is determined to take. SEPA has made the decision to build from new rather than re-establish legacy systems. The agency established a refreshed set of design principles and standards. SEPA will not recover unsupported systems to a production state. Legacy systems that are recovered will be designed and delivered via an appropriate environment.

Stakeholder commentary

Police Scotland: Deputy Chief Constable Malcolm Graham

"I think it's also worth emphasising... that SEPA is not, was not a poorly protected organisation. Again our assessment of that is that there were a lot of measures in place that you would expect to see from an organisation of that type and actually again it's just a reminder to us that demonstrates the ability of organisations that have the backing of the nature of some of the groups that we know are behind some of the software and the networking that we see in the likes of this attack are going to be able to overcome some fairly sophisticated and secure protection barriers that people have in place round about their organisations as well."

Scottish Business Resilience Centre: Chief Executive Officer Jude McCorry

The reaction from SEPA has been exemplary given the circumstances, McCorry believes, and the stiff upper lip attitude taken by the public authority has been admirable. Repeatedly, SEPA has made it clear it will not pay a ransom or engage with cybercriminals – a tactic which she says is critical in the fight against ransomware. "Certainly in terms of crisis communications they've been great. The way they've handled things with the press, with staff and partners has been very pro-active and they appear to have just gotten on with the day job as much as they can," she says. "When the time is right to come out and speak to organisations, I think it will be very helpful to a lot of people out there to listen to a case study on how SEPA handled things, what they've learned and how they dealt with it."

Professor Ciaran Martin CBE (Former Chief Executive Officer, National Cyber Security Centre)

"It's a real privilege to listen to Terry and having been through it I think the candour which he brought to the discussion is really powerful and I think people learn from that but also frankly the moral courage of the organisation refusing to pay the ransom is a huge deal and is to be commended. There is no specific answer to all cyber-crime and some of it is state backed, some of it's not, some of it is for money, some of it is for political advantage so you know, it's as variable as crime and malign activity in the non-digital world, but one of the reasons why ransomware has reached epidemic proportions is that it is being incentivised and the more Terrys and SEPAs we have then the less advantageous it will be."

National Farmers Union Scotland: Environmental Resources Policy Manager Sarah Cowie

"The scale of the cyber-attack SEPA faced was unprecedented and it was clear there were going to be implications and they have been very good at communicating with us and working on effective and pragmatic ways to resolve these issues."

FutureScot: Kevin O'Sullivan, Editor

"Some victims have been very open and kudos to @ScottishEPA whose Chief Executive @TerryAHearn was happy to go on the record and share lessons learned."

BBC: Joe Tidy, Cyber Reporter

"Great honesty from the Scottish environment agency about the impact."

SEPA Unison: Zia Hussain, Secretary

"Unison members of the Scottish Environment Protection Agency play a vital role in safeguarding Scotland's environment, regulating industrial sites and protecting communities from flooding. Many SEPA Unison members cancelled festive leave with families and loved ones to respond to the cyber-attack and members remain working around the clock to restore essential public services. "We appreciate and welcome the active engagement from SEPA management during this period and will continue to work with SEPA management to ensure our members remain supported and services are delivered to the Scottish public over this period."

Ready, resilient and responsive: Support for Scottish businesses and organisations

The Scottish Business Resilience Centre (SBRC), originally the Scottish Business Crime Centre, was established in 1996 and has evolved since then to reflect the changing needs of business and members. SBRC is funded by a range of private and public partners including the Police, Scottish Government, Association of Scottish Clearing Banks, the Drinks Industry, Scottish Fire and Rescue Service, and a wide range of business investors and members across Scotland.

SBRC provides a wide range of business resilience services, delivered by its expert team of trusted professionals, seconded police and fire officers and innovative Ethical Hacking students from Abertay University.

SBRC works in partnership to protect people, places and processes and is constantly looking at new ways to keep businesses free from risk.

Readiness

SBRC offers a free, 90-minute non-technical workshop which helps organisations find out how resilient they are to cyber-attacks and practise their response in a safe environment. Registration is available from the SBRC website.

'Exercise in a Box' is completely free, and you don't have to be technical to get involved. Exercise in a Box can be best described as a tool that recreates real world business scenarios and tests cyber-resilience in each scenario. It was developed by the National Cyber Security Centre and started its life as a self-use tool to help organisations test and practise their internal response to a plethora of cyber issues. It is, in essence, a box full of exercises based around real world scenarios with probing questions attached to each scenario. It allows your organisation to do them in your own time, in a safe environment, as many times as you want. It includes everything you need for setting up, planning, delivery, and post-exercise activity, all in one place.

Register for the workshop from the SBRC website (sbrcentre.co.uk/prevent-protect/cyber-services/exercise-in-a-box).

Response

In partnership with Scottish Government and Police Scotland, SBRC operates a helpline for Scottish organisations in the event of a cyber-attack

The free helpline will help organisations confirm they have been the victim of an attack and, if so, provide expert guidance to get them back to secure operations.

The number to call is **01786 437 472**

Resources

- SBRC Cyber Security Resources
  sbrcentre.co.uk/resourcelibrary/cyber-security-resources
- Police Scotland Cyber Security
  www.scotland.police.uk/advice-and-information/internet-safety/cybercrime/
- National Cyber Security Centre
  ncsc.gov.uk/

Recommendations

- SEPA has published:
  - Police Scotland (Cyber-Attack Response Debrief).
  - Scottish Business Resilience Centre (Cyber-Attack Preparedness Review).
  - Azets (Cyber-Attack: Response; Cyber-Attack: Lessons Learned).
  - SEPA organisational response.
- SEPA is publishing as much as it can of the reviews so that as many organisations as possible can use the experience to better protect themselves from this growing scourge of cybercrime. Information has only been redacted that meets the following legal and governance criteria:
  - Evidence related to ongoing criminal investigations.
  - Personal information or information that could identify an individual.
  - Information that could cause substantive prejudice to SEPA's ability to deliver on its statutory purpose including that relating to SEPA's current or future cyber security arrangements.
- A series of learnings were identified for Scotland's public sector.
- 44 learnings were identified for SEPA. All have been accepted.
- The learnings are the focus of a joint SEPA, SBRC and FutureScot online event, 'Cybercrime: Ready, Resilient & Responsive', held 27 October 2021 for public, private and third sector stakeholders.

Lessons learned for SEPA

Understanding and managing areas of cyber security risk

Evolve the use of frameworks and leading practices

Number	Lessons Learned	Status
1	SEPA will review and document security standards and build audits against these standards into the ongoing audit programme	Accepted
2	SEPA will seek to continue to adopt leading practice approaches.	Accepted

Allocation of resources

Number	Lessons Learned	Status
3	Management will review the ongoing resourcing requirements of the IS function.	Accepted

Cross-organisational approach to cyber

Number	Lessons Learned	Status
4	SEPA has already adopted digital first standards for the design and delivery of all new services. SEPA will continue to use agile methodology with dedicated business leads embedded in the process.	Accepted
5	SEPA will only introduce software, systems and IT equipment that has been approved by Agency Management Team. These will go through SEPA's change Control Board and be evaluated to ensure compliance with SEPA's security and governance standards prior to installation/connectivity to the network.	Accepted
6	SEPA will review and introduce best practice approaches such as maturity assessments to aid with decommissioning of systems.	Accepted

Protection of assets

Network segmentation

Number	Lessons Learned	Status
7	SEPA is working with contractors to design, review and implement a new network configuration. SEPA have introduced firewalls to allow the build of a new environment for outbound services. SEPA has enhanced its core Active Directory (AD) configuration by implementing advanced protection.	Accepted
8	As SEPA builds new systems, it will continue to work with a range of external contractors to design and build new IS systems. This will include appropriate network design, security monitoring systems, network traffic monitoring and end point device control and back up capacity.	Accepted

Privileged account management

Number	Lessons Learned	Status
9	A new password management policy complying with current NCSC guidance has been approved by AMT and introduced. The policy includes guidance for privileged access accounts.	Accepted
10	SEPA has developed and introduced an elevated access privilege policy to manage administrator accounts. This has been applied across all SEPA domains and applications.	Accepted
11	SEPA has separated all day-to-day accounts from administrative level accounts across all of SEPA's systems in line with recommended best practice.	Accepted
12	SEPA has worked with external contractors to develop and introduce a new enhanced end-point design to restrict and monitor user actions such as command-line tools and actions. Users have no administrator rights on the devices and are blocked from installing software not sanctioned by IS.	Accepted
13	SEPA has reviewed the usage of all shared administrator resources. In the new limited network, SEPA has introduced only a few very tightly controlled administrative accounts.	Accepted

Authentication

Number	Lessons Learned	Status
14	A new password policy was approved (number 9). All staff have dual reset of their passwords and access is only available via multi factor authentication.	Accepted
15	Sessions token revocation with two-factor authentication has been re-established in SEPA's new network.	Accepted
16	Multi-factor authentication for external login to SEPA services has been re-established in SEPA's new network	Accepted

Training and awareness

Number	Lessons Learned	Status
17	Technical training will be an important part of SEPA's recovery. This will be accessed by staff to maintain current skills and develop new skills.	Accepted
18	When introducing a new technology platform or developing a new service, SEPA will use a blended approach working with external contractors alongside existing staff to facilitate knowledge transfer and practical learning.	Accepted
19	As part of the recent roll out of systems, all staff were required to go through a mandatory "onboarding" session where cyber training was given to staff.	Accepted
20	SEPA will re-introduce mandatory cyber training for all staff. The take up of this training will be monitored. In addition, where there is intelligence of specific vulnerabilities, bespoke notices, advice and training will be given.	Accepted

Documentation and understanding of data held

Number	Lessons Learned	Status
21	SEPA uses data flow modelling for the design of new services. SEPA will build on this work and use it in the diagnosis and investigation of incidents going forward	Accepted

Secure design

Number	Lessons Learned	Status
22	SEPA has made the decision to build from new rather than re-establish legacy systems. SEPA has designed a refreshed set of design principles and standards.	Accepted

Detecting an attack

Threat detection

Number	Lessons Learned	Status
23	As SEPA builds new systems, it will continue to work with a range of external contractors to review its approach to security incident management and make improvements where appropriate. This will include reviewing the available resource for security incident management, providing training for staff, development of procedures for investigating intrusion detection alerts and playbooks for dealing with identified threats. This approach will be approved by AMT and fully linked to SEPA's cyber incident response plan.	Accepted
24	SEPA is seeking external advice and working with partners such as Scottish Government to investigate if a 24-hour Security Operation Centre (SOC) to provide overall threat protection including monitoring, direct action and logging across the whole of SEPA's IT infrastructure is a cost effective and appropriate way forward for SEPA.	Accepted

Endpoint protection

Number	Lessons Learned	Status
	SEPA has worked with external contractors to develop and introduce a new enhanced end-point protection (number 11)	Accepted

Responding to an incident

Availability and testing of plans

Number	Lessons Learned	Status
25	SEPA has established a "home" page on a third party website to store its 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.	Accepted
26	SEPA's Resilience team will work with document owners to ensure that they are kept up to date with periodic reviews.	Accepted
27	SEPA's suite of business continuity and disaster recovery documentation. These will be exercised periodically.	Accepted
28	Document owners will ensure that, as appropriate, individuals hold hard copies of relevant plans.	Accepted
29	SEPA will develop cyber-attack playbook routines	Accepted

Communication of an attack

Number	Lessons Learned	Status
30	SEPA will provide refresher training and support for staff involved in the investigation and escalation of incidents.	Accepted

Incident Logging

Number	Lessons Learned	Status
31	SEPA is seeking advice from external contractors on the best approach to storing and handling logs within reasonable space constraints. This work includes investigating the possibility of sending logs of all devices to a centralised logging storage area. This will allow implementation of event and incident management logging across all of SEPA's IT infrastructure.	Accepted
32	SEPA will maintain its current Security Incident Response Group approach for monitoring and managing incidents. On completion of the design of the network, SEPA will review its existing approach to security incident reporting and make improvements where appropriate.	Accepted

Availability of specialists

Number	Lessons Learned	Status
33	SEPA has reviewed and let a contract with a specialist cyber incident response company to ensure the availability of necessary expertise.	Accepted

Recovering from an attack

Backups

Number	Lessons Learned	Status
34	SEPA will seek to review and where necessary enhance its policies and processes for information and data retention.	Accepted
35	As new systems are built, SEPA will continue to work with a range of external contractors to design and build new IS systems. This will include appropriate network design, security monitoring systems, network traffic monitoring, end point device control and back up capacity.	Accepted

Recovering securely

Number	Lessons Learned	Status
36	SEPA has made the decision to build from new rather than re-establish legacy systems. SEPA has established a refreshed set of design principles and standards. SEPA will not recover unsupported systems to a production state. Legacy systems that are recovered will be designed and delivered via an appropriate environment.	Accepted
37	SEPA has undertaken a full active directory rebuild.	Accepted
38	SEPA has blocked all indicators of compromise in the firewalls. A separate rule has been applied to the new Checkpoint configuration. SEPA will continue to monitor CREW and CISP and other available monitoring services for compromised environments and threats and take action to block access where appropriate.	Accepted
39	SEPA has up to date anti-virus scanning software. In addition, SEPA has introduced a comprehensive subscription based advanced threat protection package. This includes anti-phishing, anti-spam, safe attachments, anti-malware, safelinks and domain key identified mail signatures.	Accepted
40	SEPA is building a new network. Devices which have been reused from the old network have been scanned and cleansed.	Accepted
	SEPA will only introduce software, systems and IT equipment that has been approved by Agency Management Team. These will be verified by SEPA's Change Control board to ensure compliance with security and governance standards prior to go live. (Number 5)	Accepted
41	SEPA has secured additional technical support to further strengthen its business continuity arrangements which will include improving the resilience of its services. Particular consideration will be given to the impact of medium to long term incidents (such as Covid or Cyber) on SEPA's services.	Accepted

Recovery Plan

Number	Lessons Learned	Status
42	SEPA's future workload priorities will be developed and approved through its Annual Operating Plan. This will be considered in conjunction with the review of ongoing resourcing requirements of the IS function.	Accepted

Emergency recovery

Number	Lessons Learned	Status
43	SEPA will review existing business continuity and disaster recovery plans. SEPA will work with partner agencies and key contacts across the public sector to explore options for temporary IT and mutual aid support.	Accepted
44	SEPA will document all network connections with external stakeholders and engage with them on withdrawal protocols in the event of a cyber incident.	Accepted

SEPA
Scottish Environment Protection Agency
Buidheann Dìon Àrainneachd na h-Alba

www.sepa.org.uk
03000 99 66 99
The Castle Business Park, Strathallan House, Stirling FK9 4TZ