



T: 0131-244 2707
E: Donald.McGillivray@gov.scot

Richard Leonard MSP
Convener
Public Audit Committee

By email only
publicaudit.committee@parliament.scot

19 May 2022

Dear Convener,

Thank you for your letter of 22 April regarding SEPA cyber attack lessons learned.

You sought information on two key areas:-

- The Scottish Government's process for sharing lessons learned and intelligence from the cyber-attack on SEPA with the wider public sector.
- The support and guidance that the Scottish Government provides public sector organisations in relation to cyber security.

Intelligence and lesson sharing across the wider public sector

The Scottish Government works closely with the wider public sector in response to the ever-changing cyber threat and to build cyber resilience. A key element of this is sharing threat intelligence, including indicators of compromise from incidents occurring across public and private sectors, and highlighting significant (software and hardware) vulnerabilities, along with mitigations where known. We do this through direct contact with information/cyber security personnel across the public sector where there is a significant threat, as well as through a dedicated closed online community for public sector bodies on the National Cyber Security Centre (NCSC) Cyber Information Sharing Platform.

In terms of the SEPA incident itself, after the ransomware struck on 24 December 2020, the Scottish Government's Cyber Resilience Unit (CRU) rapidly coordinated a multi-agency response (CRU, Police Scotland and NCSC) to ensure that SEPA had access to the necessary support, and that lessons could be quickly identified and shared across the public sector to avoid further incidents.

On Sunday 27 December 2020 the CRU issued a Cyber Resilience Early Warning (CREW) Notice to key information and cyber security contacts in all public sector bodies. The CREW Notice highlighted an initial tranche of indicators of compromise (IOCs) with advice to protect their networks from communications from suspicious IP ranges linked to the attack. This



enabled organisations to quickly block these IP addresses and potentially avoid similar issues.

A further CREW Notice was issued on 20 January 2021 with more detail of the incident itself and updated indicators of compromise. A final update with further IOCs was issued on 22 February 2021.

The Scottish Government also took part in the incident debrief process used to identify lessons and worked with Police Scotland on the scoping of the Police Scotland review to ensure that lessons identified from the multi-agency response and co-ordination process were, where appropriate, framed in such a way as to apply to the wider public sector.

In terms of sharing the wider lessons, during 2021 lessons identified from the SEPA incident were discussed routinely as part of wider public sector cyber coordination meetings, whilst the official incident reports were awaited. SEPA's CEO and Technical Director made numerous appearances at public sector events and individual organisations' senior management team meetings to share their first-hand experiences and lessons from the incident. This proved to be an incredibly powerful route to influencing the mindset of senior managers across the sector to be more cognisant of cyber security matters for their organisations.

In addition, the Public Sector Cyber Resilience Network came together (virtually) in early October 2021 to look at cyber assurance and how this required to be shaped by the lessons identified not only from the SEPA attack but also other incidents from across the globe. Key emerging topics were discussed at length including incident response plans, testing and exercising, back-up arrangements, cyber insurance/contracts with cyber incident response companies, network monitoring arrangements and general awareness raising for public sector staff around cyber matters like phishing, social engineering and cyber enabled fraud.

The Scottish Government supported SEPA in releasing the incident reports on 27 October, with participation in the Cybercrime Ready, Resilient & Responsive launch event Webinar. Following this, the reports were circulated to the CEOs of all public sector bodies, as well as to their information/cyber security leads, to ensure that all were aware of the findings and ready to implement measures required to tighten security where necessary. We drew their attention to Police Scotland's report which identified a number of lessons that were applicable across the public sector, regardless of which IT systems and arrangements were in place within the organisation.

Finally, the lessons identified have influenced the work programme for the CRU for the year ahead with further dedicated training, exercising and threat/intelligence sharing planned for the public sector.

Cyber Resilience support and guidance to the public sector

The Scottish Government has worked to deliver significant improvements in the cyber resilience maturity across public, private and third sectors since the publication of the first Cyber Strategy in 2015, the Public Sector Action Plan on Cyber Resilience in 2017 and the current Strategic Framework for A Cyber Resilient Scotland. The key achievements for the first strategy are set out in the Cyber resilience strategy 2015-2020: progress report (<https://www.gov.scot/publications/firm-foundations-progress-report-safe-secure-prosperous-cyber-resilience-strategy-scotland-2015-2020/>) and a progress report on the first year of implementing the Strategic Framework will be published in October this year.

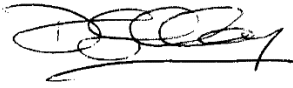
The Scottish Government encourages the public sector to, wherever practical, align to the NCSC's guidance on cyber security. Over time, we have built upon the NCSC guidance, working in partnership with the public sector to undertake key prevention activities, as well as develop specific guidance, tools and support mechanisms, including:

- Establishing a **framework of standards and controls** to help public sector bodies build their cyber security maturity (The Scottish Public Sector Cyber Resilience Framework (January 2020)). This includes setting a baseline, with the aim of progressing past this baseline as individual organisations become increasingly digitalised and the nature of cyber threats changes.
- Introducing the **Cyber Essentials** (CE) pre-assessment scheme - to ensure that the public sector were building on the solid foundations of their cyber security and resilience. A CE pre-assessment voucher scheme started in 2018 meant that 88% of the eligible public sector bodies had achieved Cyber Essentials or Cyber Essentials Plus by November 2020.
- **CyberScotland.com** - a portal for public, private and third sector organisations to easily access resources from Scottish Government, NCSC, Police Scotland and a number of other cyber security partners. Developed by partners, the website provides a one stop shop for cyber advice regardless of whether you are from the public, private or third sector or a member of the public. The site aims to signpost people to the relevant sources of advice and help, including much of the guidance and support outlined in this letter.
- Publication of free [Cyber Incident Response Plan templates and playbooks](#) - to ensure that public sector organisations had access to good practice examples of incident response plans and playbooks in order to improve their own cyber incident response. The templates have since been updated to allow them to be utilised by private and third sector organisations too.
- **Scottish Public Sector Cyber Incident Central Notification and Coordination Policy** – circulated to public sector bodies in December 2017 this policy process encourages the **voluntary reporting of cyber incidents** to the Scottish Government, Police Scotland and NCSC in a consistent way. This allows the Scottish Government to coordinate a multi-agency response to any significant cyber-attacks affecting the Scottish public sector in an effective manner and to ensure that all necessary response, resource and expertise can be swiftly deployed to assist organisations, such as SEPA, in their hour of need.
- **Cyber Resilience Early Warning Notices** (CREW) – the CRU issues CREW notices to the public sector in response to significant or specific cyber threats or vulnerabilities, ongoing incidents (often to share key indicators of compromise or key mitigation measures) or, occasionally, to highlight key guidance from NCSC or incident reports, such as was the case when the SEPA reports were published in October 2021.
- [Supply Chain Cyber Security Guidance](#) – as supply chain cyber security continues to be one of the key areas of vulnerability for the public sector, a guidance note on good practice on obtaining cyber assurance from prospective suppliers as part of the procurement process has been developed and issued the public sector. The guidance was also brought to the attention of public sector procurement professionals through the publication of a [Scottish Procurement Policy Note](#).

- [Cyber Security Procurement Support Tool](#) – a decision making support tool was developed to support the public sector in **applying the supply chain cyber security guidance** in a consistent fashion. The online web service ensures that all public sector bodies have access to a basic process for ensuring cyber security can be factored in to **public sector procurement** at the earliest opportunity.
- Exercise in a Box workshops – the Scottish public sector have traditionally found it difficult to **test cyber incident response arrangements**, despite free to use tools such as NCSC's Exercise in a Box product being released some time ago. The Scottish Government has funded facilitated workshops for the public sector to help them take their first steps in cyber exercising and specifically in testing incident response arrangements against key cyber incident scenarios, including ransomware type incidents. There have now been over 70 facilitated events delivered to over 1,500 individuals across almost 500 organisations since 2020, including 31 public sector bodies.
- **Cyber Executive Education Training** – a series of training sessions are being provided for **public sector leaders**. These sessions are aimed at building CEO, Director and Non-Executive Director level understanding of the cyber risk, their role in cyber security management and how to assess the cyber security maturity of their organisations. 90 public sector leaders participated in 2021-2022. Further sessions are expected to take place during 2022-23
- **Public Sector Cyber Resilience Network** – this network of public sector cyber and information security leads has grown into a well-established and well-respected forum to discuss challenges, share lessons and successes, as well as hear about emerging threats, vulnerabilities and technologies from a range of experts across security services, law enforcement, cyber security specialists and government. The network has grown into a tight knit, supportive community and trust has been built across the sector. This has resulted in organisations not hesitating to share advice and indicators of compromise and help avert further impacts from incidents. The network comes together at least quarterly, although it has met more frequently since the heightened cyber threats resulting from the Russian invasion of Ukraine.
- **Public Sector Cyber Information Sharing Platform (CiSP) Community** – the CiSP is an online information sharing platform created by the NCSC to allow secure sharing of low level threat intelligence, mitigations and good practice. A dedicated closed community for the Scottish public sector was established in 2019 and is now one of the key routes to getting messages out to the cyber/information security professionals across the sector.
- The **Scottish Cyber Coordination Centre (SC3)**, announced in February 2022 will also support the sector when it is fully established. The SC3 will have a key role in **incident response** to ensure that concurrent incidents can be more effectively managed and coordinated in years to come. The centre's provisional work programme includes a focus on sharing of threat intelligence, training and exercising, incident response and management as well as developing technical standards.

I hope you find the information provided above helpful. The cyber resilience of the public sector remains a key priority for the Scottish Government and will continue to be so for the foreseeable future.

Yours sincerely,



D McGillivray
Director (Interim), Safer Communities