Op CLAYBILL

Structured Debrief

Date: Wednesday 28th April 2021

Location: MS Teams

Background

During December 2020 SEPA was subject to a significant cyber-attack. This culminated in a catastrophic impact upon the agency's IT infrastructure and networks on Christmas Eve. Subsequent investigation confirmed that the attack was likely perpetrated by international serious organised criminals utilising sophisticated 'Ransomware' tactics and techniques.

To assist with the criminal investigation and support recovery efforts, a number of organisations collaborated in a co-ordinated manner. Whilst the crime remains undetected and the investigation ongoing, the initial forensic investigation has concluded and the involvement of the various stakeholders is being rationalised.

Purpose

The purpose of the Op CLAYBILL debrief held over Microsoft Teams on Wednesday 28th April 2021 was to identify learning through reflection, gathering information and developing processes for future reference should operations of a similar nature be undertaken.

The debrief focussed on operational structures and processes with a view to highlighting new opportunities for learning and effective practice. The debrief did not cover a deep dive on the technical aspects of the attack, this has been subject to a separate assessment.

Aim

On behalf of the debrief Sponsors, the Aim was to conduct a debrief of Op CLAYBILL and to identify effective practice, organisational learning, and any areas for development.

Objectives

The Op CLAYBILL debrief centred on a number of Objectives as follows;

- **The initial multi - agency response** including consideration as to the structures, processes and coordination aspects, the key stakeholders engaged and the circumstantial implications of this type of incident and resilience to respond

- **The criminal investigation** including consideration as to the levels of support provided by Police Scotland

- **Data theft and publication** including considerations as to the approach adopted to management of this aspect and the associated risks and mitigations

- **The role of the victim (SEPA)** including consideration as to the implications of this 'unique' situation for the victim and resulting requirements and expectations

- **Public Sector (Scotland) preparedness** including consideration as to preparedness overall and implications for wider partners and agencies

- **Communication** including consideration as to both internal and external communication

Whilst the above Objectives were set, the debrief participants were encouraged and provided the opportunity to raise and share observations that were out with the scope of the Objectives where relevant.

Debrief Summary:

The following points highlighted in this summary have been drawn from comments and observations made by the participants both via debrief questionnaires and discussion at the debrief session. In response to such comments and observations, suggested Recommendations have been provided for the consideration in line with the following themes;

- Organisational Preparedness

- Emergency Recovery

- Communication

- Data Theft

- Roles and Responsibilities

- Training, Testing and Exercising

Please note that the below summary reflects the 'flow' of discussion at the debrief session itself in terms of the Objectives and the order in which they were addressed which may differ to the above breakdown.

OBJECTIVE: The Initial Multi-Agency Response

OBSERVATION

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 cyber exercise. The context of the event was incredibly 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.

Despite being Christmas Eve, notification and awareness of the event was achieved at an early stage which is in line with the practiced process of alerting Emergency Management Teams (EMT) within SEPA. At that early stage, the focus was on establishing a situational report and the scale of the incident. In terms of the Incident Manager role, the priorities were to protect systems, assess the impact on business critical services, and attain a status update.

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.

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 1100hrs on Christmas Eve, a multi-agency partnership was beginning to form.

The approach adopted by the on call Police Scotland Cyber team to access key contacts and plans out with the organisational network was outlined. In terms of the challenges experienced in establishing communications with key partners, the assistance that was provided by the on call Police Scotland Cyber team was highlighted.

At a Scottish Government level, the provision of on call support for cyber resilience is included in the Scottish Public Sector Cyber Incident Central Notification and Coordination Policy. Included in this policy and process, which has been in place for a number of years and is supported by the CRU on a 24/7 basis, is the engagement of Police and the National Cyber Security Centre (NCSC) where certain thresholds are met and indeed, CRU, Police and NCSC are in regular contact.

The early notification and engagement of the CRU in this incident was welcomed and a clear brief was provided despite the limited information available at that time. From that brief, it was evident that the incident met the thresholds set out by the aforementioned policy and that there were clear consequences and implications for wider public services. As a result, a multi-agency cyber incident coordination group was stood up which engaged key stakeholders including NCSC, Police Scotland and relevant Scottish Government departments to manage liaison, coordination and communication. The CRU undertook management of the multi-agency response and commenced assessment of the incident whilst making the necessary support available to SEPA.

At the time, there were wider issues being played out across the media and so there was real concern in relation to promulgation of the incident and threat across the public sector. **The stand-up of national cyber incident coordination arrangements worked well. Furthermore, the practical support provided by Police Scotland and the Cyber Incident Response (CIR) Company engaged to support SEPA, despite the timing of the incident and the lack of formal contract to provide support, was noted as being**

exceptional.

SUGGESTED RECOMMENDATION 1

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

In terms of the wider Scottish Government response, ordinarily, the Scottish Government Resilience Room (SGoRR) would have stood up to lead the coordination of such a significant event. That forum however remained focussed on COVID at that time, thus a Multi-Agency Cyber Incident Coordination Group chaired by the CRU was stood up to support SEPA. A similar group had previously been established to manage the SolarWinds Orion compromise. **As a result, national cyber incident coordination arrangements have been adapted to reflect this change.**

The Multi Agency coordination group meeting enabled partners to understand the incident, investigations and recovery priorities. Furthermore, the meeting enabled Ministers to be properly briefed and the lead Scottish Government policy team to better understand the risks and consequences of the attack and limitations on SEPA's ability to undertake its function.

In line with its role and remit to lead the Scottish Government response and the cyber incident coordination group, the CRU provided Ministers and the Scottish Government Lead Policy Area with a brief at the earliest opportunity based on the facts known. The gravity of the unfolding situation was further articulated by the CRU through internal communications. **This process, which is embedded practice, worked effectively and efficiently in support of the SEPA incident.**

From a Policing perspective, there are structures and processes in place via the 101/999 service to assist in identifying the scale and impact of an incident and initiate prompt contact with the Scottish Government.

It was commented on that where an operational policing partner such a SEPA is victim to an attack of this nature, it is important that Police Scotland can inform internal, Police Scotland departments that may be effected to ensure awareness, understanding and allow for mitigation where required. **Whilst this was achieved via the Force Intelligence structures the best route for this internal notification was not obvious.**

SUGGESTED RECOMMENDATION 2

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

Whilst SEPA had achieved a level of preparedness through regular testing and exercising (T&E), SEPA colleagues were extremely grateful for the level of support provided, particularly that from experts in the field.

In terms of the objectives set on Day 1 of the incident, these were achieved in as much as the network was isolated, business services were operating and the necessary contacts had been made with support being provided by the CIR company under the Scottish Government Framework contract which continued in to Christmas Day. Furthermore, the SEPA EMT had met 3 times that day focussing on incident management.

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 EMT to allow SEPA to begin rebuilding new systems.

Of particular note in terms of this incident was the impact of the SolarWinds Orion compromise on the threat landscape and subsequent decision making process. **The high quality of response provided by SEPA** was highlighted, particularly taking in to consideration the severity of the incident and implications and whilst there were a lot of unknowns at the time, there were methods and strategies in place in order to get the information required.

A number of SEPA's key business critical services i.e. flood forecasting and warning and SCC pollution hotline were maintained despite the core network being offline. **This was due to the structures and processes implemented by SEPA as part of their resilience planning.** In terms of normal business communications (email, telephone, MS Teams etc) being unavailable to SEPA as an organisation, an independent telephone based system was available as part of SEPA's BCP which allowed the quick time stand up of the EMT and effective communication with key groups and the wider body of staff in relation to the situation.

Acknowledging 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.

SUGGESTED RECOMMENDATION 3

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

OBJECTIVE: Data Theft and Publication

OBSERVATION

In the very early stages of the attack SEPA isolated its network from the wider network. This was a prudent, precautionary step to prevent the spread of contagion however in a controlled measured manner it was necessary to re-establish connection to the network to allow the upload of specialist software to undertake the forensic analysis. This was achieved with the support of specialist forensic contractors.

Recognising that in circumstances where there has been a serious cyber-attack on an organisation, others with physical network connections to that organisation are likely to withdraw services without notice as a preventative measure, the act of which may have unseen consequences. A level of assurance that such a withdrawal and /or reconnection does not pose a risk to others is therefore required.

SUGGESTED RECOMMENDATION 4

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

As an organisation SEPA holds both sensitive personal information and sensitive environmental information

Technical logs from SEPA monitoring software were shared with the CIR at an early juncture and analysis identified that a data exfiltration had taken place shortly before the ransomware was activated. Despite some file information the exact nature of the data stolen was not clear. Whilst forensic analysis did take time, turnaround timescales were considered good in the circumstances.

SEPA and partners within the multi-agency co-ordination group discussed the implications of the Data theft. Whilst there was some indication of the nature of the data that had been exfiltrated it was clear that the digital forensic investigation was unlikely to reveal the level of detail and sensitivity. Research into the potential threat actors involved in this type of attack revealed that data exfiltration was a tactic used to force the victim to negotiate and could also be used to double extort on threat of publishing the data.

Key issues discussed were:

- SEPA network data did contain sensitive site information
- SEPA network data did contain sensitive personal information
- The lack of access to back-ups made recovery of this data a key consideration
- Some aspects of the unrecoverable data was in the public domain, held by partners or clients which provided opportunities to recover
- Publication of the stolen data by the threat actor on the dark web would give other criminals, security researchers and investigative reporters access.

- There was a desire to monitor known leak sites to give the earliest indication of the type of data stolen.
- Publication of the stolen data by the threat actor on the dark web or clear web provided an opportunity for some data recovery without reverting to negotiation or payment
- Security and integrity risks associated with accessing and using data published by the threat actor.
- The impact of the disclosure of sensitive data.

Advice from partners within the co-ordination group was to work towards an assumption of a worst case scenario around data sensitivity and plan around this. This is considered to be best practice.

Recognising that intelligence indicated that there was a probability that the threat actor would publish the data from a known leak site consideration was given to monitoring the locations used and assessing from previous disclosures the likely timeline which would see this disclosure thus enabling planning for the public disclosure. Research identified that the threat actor had been using a leak site on the clear web. This meant that Police Scotland, the CIR and SEPA had the capability to monitor this for any signs of disclosure. It was recognised that the partners had different drivers around any publication of stolen data. Police Scotland were interested in the evidential aspect whilst SEPA and the CIR were primarily concerned about identification of the content type and its recovery.

Furthermore it was recognised that the publication of the stolen data whilst presenting an opportunity to both identify and recover the data was not without risk. Firstly it could be withdrawn at any time therefore action would be required quickly. Secondly there could be cyber security risks associated with engaging with the leak site and or published data and thirdly the data integrity would require to be confirmed if it was to be relied upon at a later stage.

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.

The data publication on the threat actors site was picked up quickly. It was recognised that a data leak by a threat actor can take place at any time after the theft and it is therefore prudent that clarity should be sought and agreed on where the responsibilities lie with those involved in monitoring activity.

It was suggested that ongoing monitoring is a joint responsibility. From a policing perspective there is an evidential requirement in this regard. Recognising the joint approach required, it is suggested that there is a need for the victim, SEPA in this case, to undertake and adhere to a risk assessment plan in relation to monitoring and viewing data published by the threat actor which would be more efficient and effective from an assessment and resourcing perspective.

As the victim, the advice and support provided to SEPA 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. SEPA are fortunate in terms of the skills sets therein however, undertaking such tasks may prove difficult where the necessary skills are not present within an Agency/ organisation.

When considering data theft sites and the 'double dip' extortion tactic now being deployed and the fact that the responsibility for ongoing monitoring lies primarily with the victim, it was further acknowledged that the capability to do so may not be there. This tactic continues to evolve at a pace, and as such, moving forward, the role of CIR companies may become more prevalent. **There are a number of considerations in this regard including the capability of the victim and the ability and authority of the CIR to capture and download data. This is a complex problem which requires to be addressed in light**

of the data theft tactic and evolution of the same.

SUGGESTED RECOMMENDATION 5

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

OBJECTIVE: The Role of the Victim (SEPA)

OBSERVATION

SEPA used an external, NCSC approved CIR company to provide two key services – firstly to secure SEPA's IT systems and help contain and eradicate malware and threats, and secondly to carry out a forensic investigation into the attack and with Police Scotland, secure the necessary forensic evidence to support a prosecution.

In comparison to other non-cyber or traditional crimes it would be accepted practice for the victim to secure any assets with their CIR company. As such, **the requirement for SEPA to secure contractors, at a cost, to undertake detailed forensic analysis that would also support any prosecution was regarded as unusual.**

It was acknowledged that the need to understand the difference in priorities, roles and capability of a Police investigation versus that of CIR companies could perhaps have been clearer at the outset. Police involvement recognises the need for support to victims but there is a focus on evidence and evidential recovery. CIR deployment is often from a broader perspective - to understand what happened and how, with findings often relevant to the Police.

It is also recognised across Law enforcement that Private Sector CIR companies hold significant resource and capability in this regard. Consideration could be given to a cyber-crime scene being treated in the same way as a 'traditional' crime scene – Police only - however, this may not be wholly viable due to the volume of reported crimes and may also discourage reporting to the police who acknowledge a joint CIR / Police response serves both the investigation and the victim best. As such**, the focus remains on a collaborative approach to evidential capture, setting realistic expectations and clarity of role and remit.**

In this incident, there was an identified need to rapidly exchange information between the CIR company, the victim organisation (SEPA) and Police Scotland in order that the incident, intelligence and investigation priorities could be addressed. **In the early stages of the incident this did not take place as quickly as Police Scotland would have preferred.** This is directly due the CIR company working to their client and as such, permissions to share data had to go through the client. **Whilst understandable and quickly rectified by SEPA authorising the direct exchange of relevant information from the CIR company to the Police, this has the potential to impact on intelligence and investigation dividends as some date sources are time limited.**

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.

Furthermore, it was suggested that from an investigative perspective, with the CIR taking on incident response and digital forensic work, **more regular set updates to feed into the Police response and investigative strategy may have been prudent.** A programme of set updates initiated by SEPA to assist the flow of information was established, recognised as useful and should be adopted as future best practice.

SUGGESTED RECOMMENDATION 6

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

Overall the level of team work was excellent with particular note in relation to the balanced and pragmatic approach adopted by Police Scotland in relation to evidence gathering and support to SEPA.

OBJECTIVE; The Criminal Investigation

OBSERVATION

The partnership between SEPA, Police Scotland, CIR Company, the NCSC and Scottish Government worked well and there were a number of structured meetings held to capture feedback. Apart from slight uncertainty at one meeting when there was a handover between CIR teams, these strategic meetings were positive. The value in adopting this approach going forward was noted.

The issues caused by the handover between CIR teams was acknowledged however this is not usual practice, rather it was a consequence of the incident timing in terms of being over the Christmas period etc. **From a CIR perspective, these meetings were extremely positive which should be captured as part of any future playbook.** Indeed it was highlighted that during the investigation, SEPA were very good in the engagement area. Any queries or requests of data to aid the incident response process were actioned in a timely manner by SEPA wherever possible.

Whilst the multi-agency working/information sharing between Police, NCA, NCSC, SEPA and Scottish Government was positive, there was a concern in relation to volume of people at the virtual meetings and clarity of role therein. That being said, it was noted that **getting relevant partners around the table early in the enquiry can really focus support and where actions need to sit.**

Due to the level of law enforcement knowledge and expertise within SEPA, SEPA personnel played an active part in the collation of evidential productions (*an item that holds information or evidence of value*). A question in terms of whether this posed any challenges or was indeed regarded as best practice was raised.

It is recognised in such cases, where a network spans 1000s of end points and servers that not everything analysed will hold information or evidence of value and therefore become a production. The processes supporting that analysis do however need to be well managed.

The mutual understanding of such processes provided a comfort from a policing perspective however the overall impact was not significantly different. In terms of production management specifically, movement of potential productions is not approached the same way in a cyber incident as it would be in 'conventional' incidents. Learning in this regard is ongoing however there was a confidence in terms of how potential productions were managed in this case. That being said, the incident provided **wider and enhanced consideration as to the evidential chain and management of Digital productions between Police, victim and IT recovery (CIR).**

The level of financial investment that SEPA had to commit to the engagement of specialist contractors and the somewhat unique situation that cyber-attacks present was highlighted. From a policing perspective, this point was acknowledged and underlines **the need to understand victim expectations during this type of incident and who is responsible for what.**

SEE 'SUGGESTED RECOMMENDATION 6'

OBJECTIVE; Public Sector (Scotland) Preparedness

OBSERVATION

Under the Scottish Government Framework Contract, SEPA was provided access to crucial support from the CIR company. Furthermore, the Scottish Government Itecs team provided SEPA with [redacted] laptops and access to the Scottish Government network. The availability and access to these resources was not part of a pre-planned package of support, it was simply a reaction based on the given need and existing availability. Whilst there were some logistical challenges in this regard, they were rolled out by 31st December. **This was highlighted as an example of good practice in terms of organisations within the public sector working to support each other.**

A number of difficult considerations had to be had when addressing the rebuild of the SEPA network and platforms. This resulted in a lot of pressure on a small SEPA team who worked exceedingly long hours. **The Scottish Government Itecs team embedded with the SEPA IS team to reclaim and rebuild SEPA systems which was key to assisting and alleviating some of the pressures on SEPA staff.**

The ability to surge resources to perform a variety of tasks was identified as key during an Incident. It was suggested that regular incident response drills would highlight the resource areas that may need augmentation during an incident as well as ensuring an even more efficient and effective incident response going forward. In support of this, **it was highlighted that organisations in the Scottish Public Sector need to not only have cyber incident management plans in place but to actively test and exercise against known and credible cyber scenarios, particularly destructive attacks such as Ransomware attacks.**

SUGGESTED RECOMMENDATION 7

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

It was acknowledged that this incident could happen to any sector, organisation etc. on the basis that there is a clear and real threat. In terms of public sector preparedness, a Cyber Resilience strategy has been in place for a number of years in addition to a Public Sector Action plan that underpinned the delivery of improvements in the Scottish Public Sectors cyber maturity. Furthermore, a specific project delivered a generic Cyber Incident Response Plan and 5 common attack scenario Playbooks which were published and made available to public sector bodies to adapt for their own needs. That being said, it was acknowledged that **there is a need to learn and understand the gaps in capability and core skills sets.** With the significant increase in notifications in recent times, there is a real need, particularly in light of the level of interconnectivity across the public sector, to **move forward proportionately and reasonably, recognising the limitations present.**

The timeline of response was acknowledged and the enormous challenge it is for SEPA to fully recover. **The implications for larger public sector organisations, should they experience a similar attack, was raised and the need to look at the ability to stand up replacement ways of working in such times, such as secondary communications channels.** This point was further emphasised as there is little evidence of an ability to identify the threat actor and deploy the necessary tools to stop them in their tracks and indeed enterprise level **attacks of this type are becoming much more common and can happen to any organisation at any time no matter how prepared they may be.**

Further to this, the barriers to entry for threat actors have lowered and less sophisticated attackers are more common. As such, the acceptable levels of what needs to be defended have risen. On that basis, it was suggested that **the focus needs to be on the ability to recover and mitigate the consequences of an attack before considering defence measures.**

When considering the wider public sector and speed of recovery, **key learning from the SEPA incident was the need to focus on identifying priorities and securing them accordingly**. As a result, discussions are now centring on what needs protected as opposed to mass protections. This has been a difficult lesson for SEPA but is having an impact across the public sector and considerations as to how it would recover.

SEE ' SUGGESTED RECOMMENDATION 3'

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. It was further identified 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.

The need to address the issue of lessons identified, and the stage at which they are identified, which are currently being held internally and seldom shared, was acknowledged and the subsequent need for a central learning repository in support of the same, which remains in the conceptual phase. The SEPA incident has raised lots of questions in relation to learning and there are examples of Local Authorities undertaking exercises of a similar nature to identify their own learning.

There is therefore a need to find ways of **collating and sharing lessons identified from incidents for the benefit of the collective which will in turn enable the response to be continuously refined and improved.**

SUGGESTED RECOMMENDATION 8

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

Whilst the Scottish Government education and awareness events helped, **the support of a 24/7 Public Sector Security Operations Centre (SOC) was raised as a mechanism that would have further assisted in this incident.** In incidents such as this it is key to identify threats early and have sufficient resources to monitor and react to telemetry from the environment. It was felt that in terms of both prevention and response**, some form of continuous monitoring capability would have greatly assisted and that the enterprise environment is of a sufficient size and complexity to require this capability.**

[redacted]

Work on disseminating the lessons learnt has already begun with SEPA's CEO presenting at a number of high profile events such as Scotland's Cyber Week. It was suggested that **this type of work should continue with senior level engagement and commitment being key and is a role that sits with the CRU at Policy level.**

Leadership events are indeed being progressed in conjunction with the Scottish Business Resilience Centre (SBRC) which have been received positively to date. These events centre on an education programme of consequences etc in the context of leadership and decision making. Moving forward, it will be important to engage SEPA in this programme to enable reflection and an understanding of the risk posed. Adopting a layered approach, such events need to be extended to technical senior managers also.

The value in establishing a cadre of individuals who have experience and expertise in this type of incident to draft a response manual based on the SEPA learning was raised. Furthermore, it was recognised that **public sector bodies often lack the capacity and need to consider how organisations can support each other with skills and resources as mutual aid in moments of crisis.**

This was further emphasised on the basis that Scottish Public Sector organisations are uniquely interconnected in their networks and as such a serious attack on one raises the concerns that others could be infected through these connections. **Intelligence sharing is therefore a critical early consideration to ensure organisations can take mitigating action, or do not unnecessarily break these connections (as there would be consequences to this) because they do not feel they have sufficient information on the risk.**

SEE 'SUGGESTED RECOMMENDATION 4'

OBJECTIVE; Communication

OBSERVATION

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. Furthermore, a meeting was established, bringing together all of the external partners to provide a forum for updates and requests for assistance to be tabled.

The Scottish Government policy role was key to ensuring visibility, support and engagement of the Ministers. Communications in relation to the incident both internally and externally was important in addition to the communication around the data theft which was focussed on keeping people informed quickly and openly whilst providing the necessary support in this regard.

It was highlighted 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 were realistic in understanding the extent of the scale of the attack and did not try to minimise this to key partners.**

Currently, the level of communications considerations are not particularly detailed in cyber incident playbooks. Furthermore, there is a lack of training across the public sector in general (it should be noted that SEPA did have communications training) which Police Scotland can assist with in support of victims. **Indeed, 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.**

Communications considerations, internal and external are both broad ranging and critical when dealing with significant cyber-attacks and merit the development of a clear crisis communications plan. The CRU have identified and circulated a Cyber Crisis Communications Framework developed by Prof Jason Nurse which helps address the complexity of communications requirements that surround a significant cyber-attack.

SUGGESTED RECOMMENDATION 9

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

Whilst communications were positive, within the public sector **there were tensions in relation to the desire for more detailed indicators of compromise and updates from SEPA following the early sharing information.** Whilst Police Scotland Cybercrime Investigation Unit identified and agreed with SEPA an early and limited dissemination which was greatly welcomed by the wider community, this dissemination coupled with the public knowledge of an attack resulted in a significant number of requests both to the CRU and directly to SEPA for more detailed information from organisations that had some form of relationship with SEPA.

It was acknowledged that there is always a natural, and understandable, tension between the victim organisations priorities which focus on recovery and the demand for information from external partners which isn't easily addressed. That being said, **the cyber incident coordination process provides the conduit for the CRU to seek to address and balance this tension.**

OVERALL

OBSERVATION

SEPA recognised the invaluable support and assistance it received from a range of partners around the table during and after this incident.

A formal thank you was expressed to the debrief team.

SUMMARY OF SUGGESTED RECOMMENDATIONS

SUGGESTED RECOMMENDATION 1

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

SUGGESTED RECOMMENDATION 2

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

SUGGESTED RECOMMENDATION 3

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

SUGGESTED RECOMMENDATION 4

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

SUGGESTED RECOMMENDATION 5

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

SUGGESTED RECOMMENDATION 6

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

SUGGESTED RECOMMENDATION 7

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

SUGGESTED RECOMMENDATION 8

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

SUGGESTED RECOMMENDATION 9

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

CONCLUSION

This report and Suggested Recommendations contained therein will be submitted to the Debrief Sponsors for ownership and circulation to all participating agencies in addition to the Scottish Business Resilience Centre in support of wider preparedness considerations. It should be noted that this debrief forms part of a wider SEPA 'lessons learned' programme that has been commissioned by SEPA [redacted].

APPENDIX A – LIST OF PARTICIPATING AGENCIES/ ORGANISATIONS/ COMPANIES

- Police Scotland Cybercrime Investigations
- Scottish Environment Protection Agency (SEPA)
- Scottish Government Cyber Resilience Unit (CRU)
- Scottish Government ITecs Team
- Scottish Government Environment and Forestry Directorate
- The CIR Company