Scottish Business Resilience Centre

Cyber Review

SEPA

16 | 06 | 21

Executive Summary

In December 2020, the Scottish Environment Protection Agency (SEPA) was subject to a significant ransomware cyber-attack which adversely affected all aspects of its business operations including its contact centre, internal systems, processes and communications.

As a result of this attack, incident response and business continuity arrangements were promptly enacted by SEPA. This response invoked engagement with the internal Emergency Management Team, IS Department, Scottish Government (SG), Police Scotland (PS), National Cyber Security Centre (NCSC), and NCC Group's Cyber Incident Response Team (NCC/CIRT)

1. This report details an examination of SEPA's cyber preparedness prior to this attack against the backdrop of an ever increasing and sophisticated cyber threat landscape. The review identifies a high degree of conformance and implementation of many Information Security (IS) best practices across the technological estate within SEPA. Complete adherence to any one standard or best practice would not, in essence have prevented this cyber-attack.

2. SEPA has displayed a progressive awareness of cyber security and to holistically mitigate such risk had achieved a well-recognised industry IS standard of Cyber Essentials Plus prior to this attack.

3. The report identified that sophisticated defence and detection mechanisms were implemented and operating correctly prior to the incident, though alerting mechanisms, most commonly addressed by a costly 24/7 Secure Operations Centre (SOC) [redacted]

4. The report identifies that the [redacted] Organised Crime Ransomware group responsible for this cyber-attack had been identified in late 2019, however there was negligible threat intelligence available on the group's Tactics, Techniques or Processes (TTP's) prior to the incident. If SEPA had some personnel employed in threat intelligence, this would not have been flagged up, as the [redacted] intelligence was not available until post SEPA attack. Ordinarily this intelligence would have been made available to the relevant resources within SEPA to address any potential attack.

5. This review 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. The review 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.

6. The review identified a most positive eagerness at executive level and within the Information Security provision to mature SEPA's cyber security posture by obtaining CE+ accreditation. In addition, SEPA had implemented various components within the ITIL framework to assist with governance and management of their IT Processes.

The review identified a significant eagerness, commitment and positive dedication across many resources within SEPA in response and recovery to this cyber-attack.

7. The review provides many specific recommendations for SEPA as detailed within this report. Further recommendations to address for the wider stakeholder group in "lessons learned" from this attack comprise the establishment of an integrated Secure Operations Centre (SOC) for similar public sector organisations to protect essential services. This is a high-cost factor normally beyond the budget capacity of such a public sector organisation however now requires serious consideration in managing public funds with the increasing costs of a cybercrime attack and ROI in the prevention such attacks. It would not be feasible or economically viable for all public sector organisations to have one of these of their own, as we are looking at cost of circa £2-3 million depending on staffing, technology and service level agreements, but some sort of local solution needs to be looked at for the public sector in general.

8. To complement the establishment of a SOC capability the stakeholder group of Police Scotland, Scottish Government , SBRC and key collaborative partners seek also to establish a Cyber Centre of Excellence (CCE), which would focus on Cyber Threat Intelligence, Prevent and Protect initiatives, Incident Response and Crisis Communications support. This centre would take away the pressure from the smaller public sector and SME organisations to set up a SOC, incident response and threat and intel sharing. But also gather all the support and expertise asap when an incident happens, and help the organisations rebuild post incident.

Finally, I would like to thank SEPA for three items which are out with the scope of this report -

A. 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.

B. For being an organisation, that "Team Scotland" wanted to help - there has been a huge collective and a "want to" effort among the agencies to support SEPA. Everyone we have dealt with has commented on the camaraderie and commitment within SEPA and also the way SEPA employees and Executive team have 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.

C. 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.

Document Control

Version/Revision Control

Author	Role	Issue Date	Version	Summary of Changes
[redacted]	[redacted]		1.0	Document Creation
[redacted]	[redacted]		1.1	Changes based on feedback
[redacted]	[redacted]		1.2	Executive Summary
[redacted]	[redacted]		1.3	Changes following consideration of additional evidence.

Document Reviewers

The document is required to be reviewed by:

Name	Role	Draft Review (Y/N)	Review (Y/N)	Sign-off Required(Y/N)
[redacted]	[redacted]	✓	✓	
[redacted]	[redacted]	✓	✓	✓

Distribution List

This document should be distributed to

[redacted] Chief Executive, Scottish Environment Protection Agency

Contents

Review

In line with all cyber incident response frameworks/methodologies, and best practice, SEPA has undertaken a comprehensive review exercise to identify lessons gleaned from this cyber-attack to improve, prepare, and protect itself from possible future incidents and share learnings with all concerned partners.

This review was conducted to examine SEPA's overarching preparedness, prior to the incident and provide recommendations under the following headings:

- Horizon Scanning & Threat Intelligence
- Security Standards
- Processes and Documentation
- Governance
- Structure, Skillsets, Roles & Responsibilities
- Resources
- Morale
- Training
- Assurance: Reviews, Audits & Measures
- Actions / Mitigations and Progress made

Methodology

The findings of this report were gathered from process examination and interviews with relevant SEPA staff under agreement that comments or observations used would not be directly attributed to the individual. This condition was imposed to ensure that the individual could be candid, open, and honest, in their answers. It was made clear to all persons interviewed that this review was not a punitive process but exists to help the organisation and its employees to better prepare and protect both the individuals and the organisation from future harms.

Cyber Threat Landscape

The following extracts data from multiple sources in order to contextualise the escalating global cyber threat landscape at the time of the SEPA incident:

Malware exploitation and ransomware proliferation has grown recently with an increasing sophistication and prevalence. International organised crime gangs (OCG's) and malicious actors have adapted their tactics, techniques and processes (TTP) launching malicious attacks on an unprecedented industrial scale. We have witnessed a parallel growth in ransomware as a service (RaaS) and double ransomware extortion attacks on many organisations.

Notwithstanding an increasing threat landscape, the Scottish Public Sector business delivery landscape has fundamentally changed – digital transformation was growing and the COVID-19 pandemic has accelerated this transformation. Working from home (WFH) has accelerated the adoption of remote technologies, accentuated the threat landscape and led to a whole new way of working.

These changes have made cyber security more difficult for organisations, deployment of new endpoints (laptops etc), use of own devices, introduction of new remote working tools (teams, zoom etc), harder to monitor, harder to patch, stretched IT resources impact of pandemic requirement to introduce and service these new technologies at pace.

Between the 1st October 2019 and the 30th September 2020, 59% (global average) of organizations detected attackers within their own environments. This was a 12% increase over the previous year.

Dwell time for attackers inside corporate networks fell below a month, with the median global figure falling to 24 days (Down from 56 days in 2018-2019) and was lower still (12 days) if the source of the detection was internal.

While the increase in organisations detecting compromise within their own environments and the decrease in dwell time of attackers within the organisation would appear positive, both can, at least in part, be attributed to the proliferation of ransomware attacks; 78% of which had dwell times of fewer than 30 days, with the median average being just 5 days,[1] and for which the method of internal detection is largely non-proactive.

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%.[2]

In the final quarter of 2020, Ransomware attacks within the UK grew in prevalence by 80%[3]. Ransomware incidents of note include WannaCry (2017), Eurofins Scientific (2019), and Travelex (2020).

2020 was a year where we were reminded how events in the physical world and cyber security are intertwined. In 2020, we saw how a global pandemic changed business operations and as a result the attack surface and risk profile of most businesses[4]. Organisations around the world struggled with adapting to the new norm and maintaining their defences as attackers took advantage of these unprecedented times.

1. Horizon Scanning & Threat Intelligence

Best practice recommends organisations undertake continuous horizon scanning, threat intelligence assessment, and proactively monitor and assess exposure of technology in use, however this is not common practice. SEPA's approach was no different from many organisations in this respect. SEPA's primary sources of threat intelligence and vulnerability awareness were provided by the Scottish Government's Cyber Resilience Unit (CRU) notices, ad-hoc review of National Cyber Security Centres (NCSC) Cyber Information Sharing Partnership (CiSP) platform, and from direct contact from system vendors and 3rd party suppliers.

[redacted]

[1] https://content.fireeye.com/m-trends/rpt-m-trends-2021
[2] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-apr-2021.pdf
[3] https://www.itpro.co.uk/security/ransomware/357353/uk-ransomware-attacks-increased-by-80-in-past-quarter
[4] https://content.fireeye.com/m-trends/rpt-m-trends-2021

Though this did not give full coverage of the threat landscape, 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.

In addition, the review identified that the lack of a complete package of threat intelligence and awareness could also be attributed to insufficient dedicated resources. Many of those interviewed believe that an external Secure Operations Centre (SOC) would be, amongst other things, a viable solution.

External SOCs are most effective when working in partnership with internal resources to refine and test detection and alerting. A SOC can provide advice and guidance with regards to the technology sets in use and the placement of sensors. Some SOCs do provide threat intelligence which can be used to inform actions to mitigate threats. SOC provision is an expensive entity for any organisation to implement.

The review identified that whilst SEPA undertook horizon scanning that this could be further strengthened by structuring and broadening intelligence sources, and by increasing the available resource.

R1: SEPA should explore options for the engagement of a SOC. [redacted]

Management Response:

As we build new systems we will continue to work with a range of external contractors to review our approach to security incident management and make improvements where appropriate.

This will include reviewing the available resource for security incident management, providing training for our staff, development of procedures for investigating intrusion detection alerts and playbooks for dealing with identified threats. This approach will be fully linked to our cyber incident response plan.

[redacted]

Owner: [redacted]

Deadline date: [redacted]

2. Security & Standards

Prior to the incident SEPA had attained Cyber Essentials Plus accreditation and utilised ITIL methods for governance areas, such as change control. Although not regulated or mandated to, SEPA introduced these additional controls following encouragement from SG to advance their security posture. All those who contributed to Cyber Essentials Plus were proud of their achievements and efforts in gaining the accreditation. Many respondents indicated a desire and support to see the scheme become more robust and expanded in scope to further enhance the standards that had

already been obtained within SEPA though recognised difficulties and challenges in doing so whilst still maintaining some of the business' legacy data and systems.

SEPA also participated in and complied with annual SG digital assessment. SEPA was an early adopter of the digital first standards for the design and delivery of new services and worked extensively with the Scottish Government digital teams. SEPA had successfully transformed a number of services and won awards for their digital licensing services. SEPA had been assessed and passed digital first assessments for these digital services.

With regards to wider security standards and processes: The review identified that when systems were installed, they were configured to best practice standards or adhered to the vendor or contactors recommendations.

Whilst SEPA has demonstrated a foresight to advance their cyber posture in achieving CE+, there is presently no commitment to progress towards more mature frameworks such as ISO 27001 ,CIS, or NIST. If adopted these would provide an ongoing methodology to ensure continual review, method, measurement, or verification against these standards.

While there are too many individual areas of IS to examine with regards to best practice, the key areas of importance in relation to the incident can be summarised thus:

1. **Backups:** Backups were taken in line with NCSC best practice in that there were 3 copies of the data, located at 2 separate locations, with one copy stored offline. However, the design of the network meant that both sites were affected [redacted] **This in itself would not have prevented the incident** [redacted] 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 back-ups. Whilst not a prerequisite for CE+ certification, backing up data is essential best practice.

2. **Networks:** The network was segmented into Virtual Local Area Networks (VLANs) however there was no access control lists (ACLs) in place to filter traffic and all sites and networks could route to each other. [redacted]

3. **Endpoint Protection:** Antivirus protections were installed on all endpoints except for thin client devices. This is an understandable risk acceptance given that the user profiles and data are accessed via a Virtual Desktop Infrastructure (VDI) running antivirus.

4. **System Auditing:** Logging and alerting were in place at the time of the incident. These were (and are) powerful enterprise class magic quadrant products. [redacted]

5. **Administrative Account Management:** IS Department staff do have separate accounts for their day-to-day operational duties and their administrative (privileged) functions. This is convergent with best practice. [redacted]

[redacted]Once compromised, this facilitates lateral movement and privilege escalation. These latter points are not best practise.

6. **Secure Configuration:** Access to facilities such as the command line interface (CMD) and PowerShell were restricted to specialist users These tools were used by the threat actor and play significant roles in the TTP's of other threat groups.

The review identified that recovering systems back to their pre-incident state may present, if implemented, ongoing risks and vulnerabilities. Furthermore, respondents from both within and out with the IS Department indicated that this was undesirable, and that the opportunity may be missed to improve systems and process that had been in place before.

R2: Do not recover unsupported systems to a production state. [redacted]The business should review the necessity of these systems and the data on them. Decisions about if or how the data is reincorporated back into the production environment should be made to ensure that any methods and processes for doing so comply with requirements to only run on supported and up-to-date platforms.

Management Response:

SEPA has made the decision to build from new rather than re-establishing legacy systems. We have 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.

Owner: [redacted]
Deadline date: [redacted]

Respondents indicated that following the incident, the business appears to have a greater appreciation regarding how much IS systems underpin the SEPA's business delivery. This should be leveraged to build a better working relationship and understanding between the business areas and IS.

R3: Utilise business and systems analysts to work with the different business areas to identify better and more effective ways of working. While improving efficiency it will help the analyst better understand the needs and processes of the business as well as what is technologically feasible and may help reduce some of the siloed areas across the business. This may help garner further goodwill towards the IS function as they help the business to improve and work better, [redacted]

Management Response:
SEPA have already adopted digital first standards for the design and delivery of all new services. We will continue to use agile methodology with dedicated business leads embedded in the process.

Owner: [redacted]

Deadline date: [redacted]

3. Processes & Documentation

The review identified from interviews that appropriate documentation had been created and was in place and reviewed as part of overall document management system. Much of this documentation however was unavailable due to the attack.

In general, the review discovered from respondents that associated IS documentation prior to the incident although created was not comprehensive applied to an optimum standard, particularly in relation to older legacy systems. Documentation was not seen as a priority and pressures to deliver projects and undertake routine maintenance took priority. This is not uncommon within organisations, however it may have proven useful during the incident it would not have prevented such a complex malicious attack.

[redacted]

Documentation is often tedious to write, varies in quality and is not something which is well maintained. This is common, and not unique to SEPA. As an approach to combatting this, providing all areas with an overview of how systems are built, interact, dataflows managed, as well as help break some of the siloed mentality.

R4: Introduce suitable dataflow modelling. This would also have the additional benefits of helping the support desk with incident diagnosis and resolution as well as the Change Advisory Board (CAB) in understanding the impacts of changes and outages through simulation of outage and change.

Management Response:

SEPA uses data flow modelling for the design of new services. We will build on this work and use it in the diagnosis and investigation of incidents going forward.

Owner: [redacted]

Deadline date: [redacted]

4. Governance

SEPA demonstrated adherence to best practice by implementing the ITIL framework around governance processes for IS change management. Meetings were conducted weekly and were accepted as being sufficient and necessary without being restrictive. Respondents identified changes going through without following the process and this was attributed to pressures from the business. Some respondents indicated that the process appeared to have improved as members from the Governance Unit now attend.

At a tactical level, SEPA had adopted an agile methodology for service transformation and design, daily stand ups, regular interactions, periodic reviews by independent organisations were all utilised. The [redacted] took an active leadership role in the adoption of new approaches such as agile design and delivery for the transformation and adoption of digital services.

At a strategic level, the Agency Management Team (AMT) provided advice, direction and support to the IS function. AMT had considered papers on the resourcing and structure of the function, the adoption of new technologies and the approach for the design and delivery of new services.

The Board provided strategic direction and support. SEPA had in place a well-established/mature digital strategy which was developed by the board and was approved after direct engagement by the board with the SG [redacted]. SEPA was active members of the EELG digital group and led on a number of areas in the EELG (RAFE Digital strategy). The Board had received papers and demonstration sessions on successful digital transformation of services.

Build standards are already being implemented. Vulnerability management platforms have the capabilities of running audit reports against a number of preconfigured standards and best practices. Custom audit files can be created if necessary.

R5: Decide on what security baselines are going to be used for systems and then either use the inbuilt audit policies within existing vulnerability management systems or create custom policies which meet and check SEPA's own baselines and configuration standards. This will allow easy and repeat verification of best practices/standards, and the tracking of devices which deviate away from those standards.

Management Response:

SEPA will review and document security standards and build audits against these standards into our ongoing audit programme.

Owner: [redacted]

Deadline date: [redacted]

SEPA had achieved the recommended industry standard of CE+ and advanced their security posture with the chronological partial implementation of numerous additional best practices.

R6: To further consolidate their cyber security posture SEPA should implement best practices in their entirety, especially with regards to:

- Reducing the amount of legacy data through appropriate weeding
- Increasing the offline backup capacity to sufficiently allow the retention of the retained data.
- Improving control and understanding of organisational dataflows by analysing network traffic and applying appropriate restrictive access controls between routes and vlans.
- Implementing endpoint device control to reduce methods of infiltration or compromise of SEPA systems.
- Increasing the number of people with access to security monitoring systems and alerting.
- Sending alerts to the support desk for user contact, triage and escalation.
- Utilising the [redacted] framework in order to identify and configure mitigations and alerting. This can also be utilised to identify areas of weakness in defences and allow the business to prioritise activities based on the threats and risks presented.
- Implementing [redacted] on domain member devices and change staff behaviour patterns to use the local administrative password instead of their own domain administrative accounts to access the devices. This reduces the number of accounts that an adversary could potentially access and limits their ability to move laterally around the network using domain credentials.
- Preventing day-to-day accounts from having administrative privilege on a device.
- Restricting access to local drives, and command line tools.

Management Response:

SEPA will seek to continue to adopt best practice approaches including:

- Reviewing and where necessary enhancing our policies and processes for information and data retention.
- As we build new systems, we 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.
- We have engaged specialist contractors to help design and deliver our security posture. We will work with them to [redacted]
- All day-to-day accounts have been separated from administrative level accounts across all of SEPA's systems in line with recommended best practise.
- We have worked with external contractors to develop and introduce a new enhanced end-point design which uses [redacted]

Owner: [redacted]
Deadline Date: [redacted]

5. Structure, Skillsets, Roles & Responsibilities

As in the case of most reviews there were different views from SEPA employees in respect of IS structure and role responsibilities. The review identified that SEPA had an established IS structure with clear roles and responsibilities. The [redacted] function managed 3 units - customer services and application support, security and networking, systems development. The [redacted] is a Certified Information Systems Security Professional (CISSP), which is maintained every year.

A Cyber Incident Response Plan which detailed structure skillsets, roles and responsibilities of individuals/post holders was in existence in SEPA prior to the incident however some SEPA resources perceived that only very senior managers within the IS Department were aware of the existence.

On a most positive note, the organisational Incident Response experience within SEPA gleaned from managing previous critical incidents greatly assisted with a structured agile response to this attack with the expedient establishment of an effective Emergency Management Team (EMT). SEPA hosted an AMT Cyber exercise in February 2019.

There was an acceptance that the IR plan was not recently updated , however those who were aware of it understood their roles, responsibilities, and where they fitted within the structure.

The plan could not be shared during the incident as there was no offline version or hard copy and along with all the other files on the Storage Access Network (SAN), became unavailable as a result of the incident.

Whilst certain staff interviewed stated they were unaware of the Cyber Incident Response Plan, those who played a part in the response were aware of their role within the overall mechanism. Few could state or identify their role title, but all knew their responsibilities. The overall staff awareness was attributed almost entirely to the daily stand-up meetings, which were greatly appreciated, made everyone feel informed, and helped everyone understand their priorities and responsibilities.

In respect of the attack, most of the technical staff interviewed described attempts to recover the systems. Their primary objectives were not the containment and eradication of the threat as would have been ordinarily identified within a Cyber Incident Response plan. Respondents indicated by the time that they arrived on-site, most data was already inaccessible/encrypted.

During the course of the incident all individuals felt like their skillsets and capabilities were optimised and fully utilised. Most respondents identified an inclusive decision-making process in reacting to the incident and a range expertise were engaged in response to the attack namely specialists forensic contractor's, external security consultants, specialists in building new systems and independent support from organisations such as Scottish Government..

[redacted]

R7: Recreate the cyber incident response plan and maintain it within a "battle box" along with other disaster recovery, business continuity, and systems documentation.

These documents, plans, and processes should be shared and practiced by those who should be involved in the response to an incident. These exercises can and should in turn be used to develop internal playbooks for different scenarios. Run these exercises regularly and periodically invite users and members of the executive along to be involved so that they understand the process and impacts of their decisions and actions.

Management response:

We will review and issue our suite of business continuity and disaster recovery documentation.
These will be exercised periodically.

Owner: [redacted]

Deadline date: [redacted]

6. Resources

Some staff interviewed identified that the overall IS department was sufficiently resourced and did not require further resourcing though respondents identified that resources were incorrectly allocated within the department and that reallocation and retraining of resources was required. Interviewees were aware and supported a previously proposed structure from the [redacted]

Reducing or reallocating staff within the public sector is difficult, staff need to be approached with regards to reskilling if the requirement for their current role is diminishing. Continued employment of graduate apprentices should be considered as a method of bringing in new people and ideas and introducing a more flexible approach to deploying staff across broad areas of work.

R8: Restructure the department to more appropriately allocate resourcing.

Management response:

We will review the ongoing resourcing requirements of the IS function.

Owner: [redacted]

Deadline date: [redacted]

7. Morale

The following section should be considered in context. The sample size of respondents represents less than 1% of the organisation's overall employee base, and only 13% of the staff associated with the IS Department.

The review identified a moderate to low morale posture prior to 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.

In order to assess morale within the organisation figures 1 to 4 indicate responses to how resources perceived their recognition, and value within the organisation and the morale that they perceived and felt during the course of the incident.

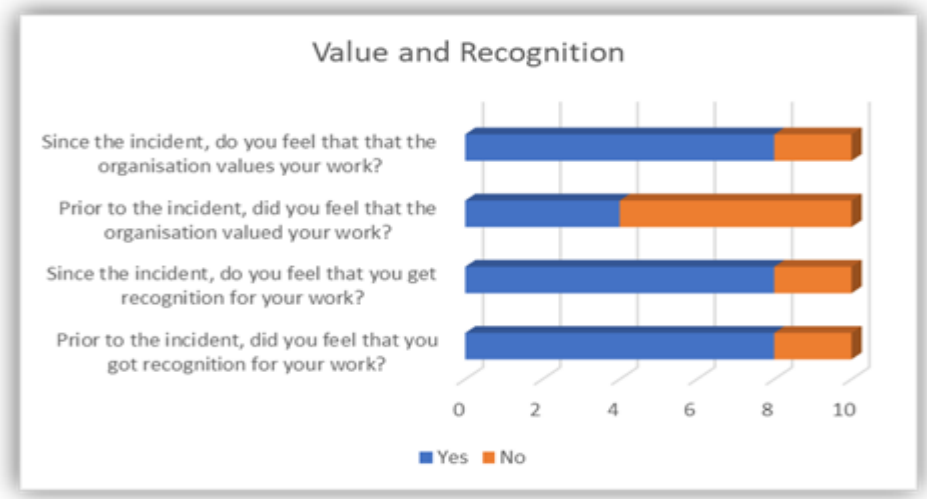
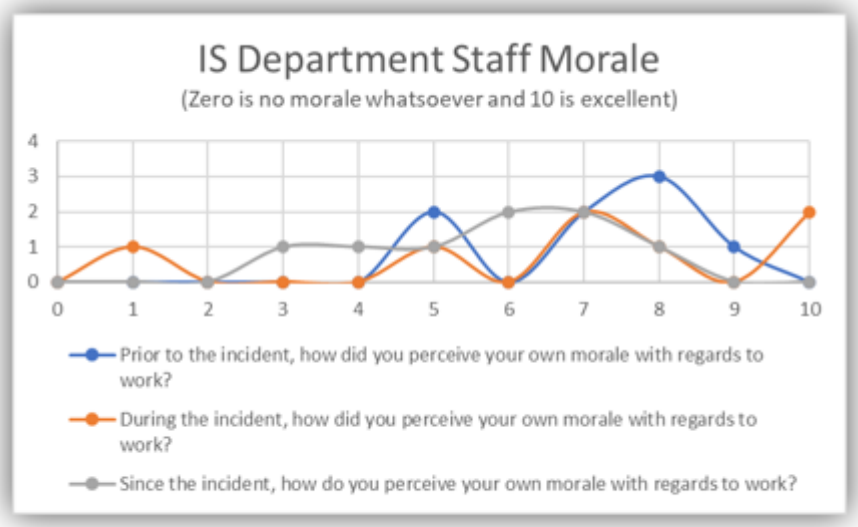


Figure 1. Value and recognition



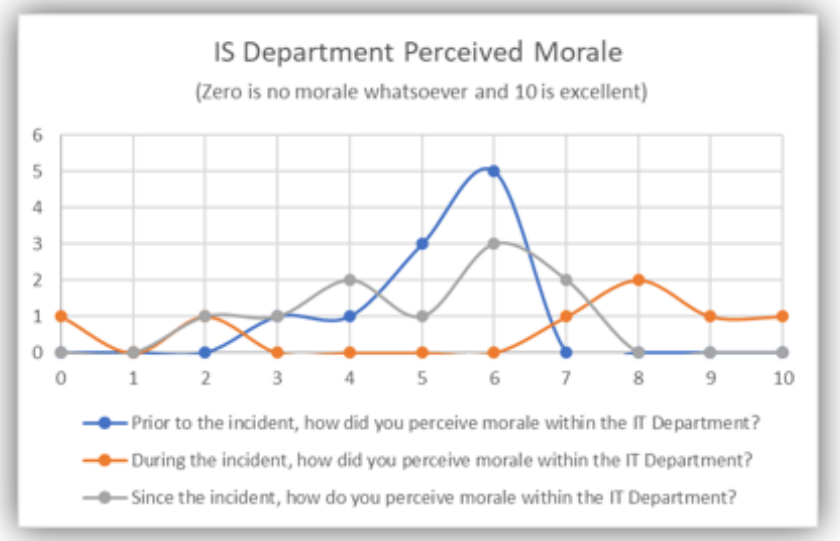


Figure 2. Perceived Morale within the IS Department

Figure 4. Workload Management

100% of interviewees responded that they felt respected in their workplace.

Though 60% stated that stress within the working environment was affecting their life outside of the organisation.

80% of respondents felt that the organisation cared about them.

50% of those interviewed knew what the organisation's expectations of them.

The final question is referred to as the employee Net Promoter Score (eNPS). It derives from the customer Net Promoter Score, which was developed by Fred Reichheld, Bain & Company and Satmetrix in 1996 as a measure of customer loyalty and satisfaction. The method was modified in 2001 as a way of measuring employee satisfaction and loyalty.

Answers from the eNPS are broken down into three categories:

- 0-6 = "Critics" or "Detractors"
- 7-8 = "Passives"
- 9-10 = "Ambassadors" or "Promoters"

The score is calculated by subtracting the percentage of "Critics" or "Detractors" away from the percentage of "Ambassadors" or "Promoters". The score can therefore range anywhere from -100 to 100. The resulting scores can be interpreted thus:

- Poor (-100 – 0)
- Good (0 – 29)
- Great (30 – 69)
- Excellent (70 – 100)

While the method does have its flaws and critics, the eNPS is a recognised metric which can be used as a benchmark against which SEPA can monitor its employee satisfaction. SEPA's score from the people interviewed came out at 30% (Great). SEPA had zero "Critics" or "Detractors".

8. Training

Evidence collected within the interviews identified that senior managers had attended external cyber resilience training. Throughout the autumn of 2020 , mandatory cyber training was also provided and completed by 1252 staff with 70 remaining outstanding.

A common juxtaposition was identified in that IS staff lamented a lack of formal training while senior managers indicated there was budget for training and that the IS department received the majority of this budget . However, a key strategic element of training that was received involved the engagement with best in class external contractors to engage with SEPA staff to facilitate knowledge transfer and practical learning.

SEPA has a formal technical training budget for IS staff. In recent years there has been a heavy emphasis on training to support the move to the cloud. New training for systems testers, training for web developers on Umbraco and the largest area of training has been on agile methodologies – the digital first approach with over 40 IS staff being trained

All parties provided very similar interpretations of the process for requesting training courses. Where the confusion or any misunderstanding creeps in is with regards to the interpretation of the employee identifying the necessary training. Those who identified a lack of training believed the process to be that they would identify the training that they needed as part of the Personal Development Program, their line manager would then pass that to the Learning and Development Department who identified the course and requested budget from the Director of IS.

Those who received training identified the actual course, from a training provider run at set scheduled times. They submitted that to line manager or the Learning and Development Department who requested budget.

There was some trepidation in how staff felt with regards to how well trained and qualified they are to use and support the new infrastructure, given some of the significant shifts and updates to it, however all identified that they had either undergone or were scheduled for training.

Ongoing and continuous technical training is an integral part of cyber prevention. Indicative prices for training referred to during interviews seemed to be in-line with industry norms. There are however cheaper and even free methods to get relevant training. These may include buying course bundles or subscribing to training providers with catalogues of courses available which employees can dip into and out of during the year. Exams and accreditations may cost extra however the courses in themselves would represent a significant method of upskilling, filling demand/need and improving morale.

R9: Identify training bundles and offer them to staff as opposed to the current identification of courses in isolation.

Management response:

Technical training will be an important part of our recovery. This will be accessed by staff to maintain current skills and develop new skills. Prior to the incident we had signed up to the Microsoft Enterprise Skills Initiative (ESI) training programme. We will continue to build on this and will train further staff as required.

In addition when introducing a new technology platform or developing a new service, we will use a blended approach working with external contractors alongside our existing staff to facilitate knowledge transfer and practical learning.

Owner: [redacted]

Deadline Date: [redacted]

Ongoing and continuous all-staff training is an integral part of cyber prevention. Mandatory cyber training was available to all SEPA staff in the lead up to the attack. This training was reinforced by the organisation during the roll out of MS Teams.

Given the ongoing elevated risk of cyber crime and the recent experiences of a cyber-attack on the organisation, it is critical that cyber specific support, advice and direction continues to be given to all staff.

R10: Appropriate ongoing and regular cyber prevention training for all staff should be re-introduced.

Management Response:

As part of our recent roll out of the [redacted] products all staff were required to go through a mandatory 'onboarding' session where cyber training was given to staff.

SEPA will reintroduce 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.

Owner: [redacted]

Deadline date: [redacted]

9. Assurance: Reviews, Audits & Measures

Within SEPA, [redacted] a vulnerability management solution, was purchased and installed to support attainment of the Cyber Essentials Plus Accreditation Within SEPA [redacted] the VMS was deployed as per manufacturer's instructions, on a [redacted] basis dedicated members of staff administer its output. Where vulnerabilities were identified they were passed to the relevant individual with priority afforded to remediating the critical and high vulnerabilities through, for example, patching.

SEPA has also undertaken a number of external reviews/audits and penetration testing.

When asked about an assurance process for reviewing systems that were being implemented or updated to ensure SEPA met certain cyber security criteria (such as encryption of data in transit and at rest, user function separation, or user access and action auditing), there appeared to be a view from respondents referencing this function as either Change Advisory Board (CAB) process or a Governance Department issue.

No respondent was able to identify a defined standard or framework against which the systems were measured. It was highlighted that Information Systems were not consulted on IT associated purchases until a request to install was received.

[redacted]

The procurement of all systems and devices should adhere to strict controls around SEPA's security posture, organisational capacity to deliver, etc.

R11: Introduce a clear mechanism and policy regarding the purchase and introduction of any equipment that requires connectivity to the network or software installation. Any such equipment should be reviewed by both the Governance Department and the IS department prior to any decision to purchase it. This will ensure that licensing cost, compatibility, supportability, and conformity are considered, and an appropriate lifecycle planned. This should include the decommissioning of the device and the weeding and migration of data.

Management Response:

We will only introduce software, systems and IT equipment that has been approved by Agency Management Team. These will go through our change Control Board and be evaluated to ensure compliance with our security and governance standards prior to installation/connectivity to our network.
We will review and introduce best practice approaches such as maturity assessments to aid with decommissioning of systems.

Owner: [redacted]

Deadline date: [redacted]

10. Action/Mitigation Plans & Progress

Previous incidents had been quickly contained and were recovered from quickly and easily. Despite these incidents, nobody expected a cyber-attack; mostly because nobody thought that SEPA would be targeted.

Based on the experience of the previous incidents, everybody interviewed indicated that prior to the incident they believed, given the technology that was in place, they were well positioned to repel a cyber-attack; with many citing comparisons with other Public Sector organisations.

Supporting initial beliefs regarding preparedness for incidents, interviewees did believe that protection mechanisms in place prior to the incident were sufficient and were able to list a wide variety of technologies in place at the time of the incident to detect and prevent threats. These included:

- [redacted] endpoint protection
- [redacted] email filtering
- [redacted] IDS
- [redacted] system logging capability
- Configuration of the VDI environment
- Firewalls
- Automated patch management processes
- VPN accebackss controls

- [redacted] Professional Vulnerability Management
- User phishing training

SEPA had in place web filtering and DNS. This was provided by a third party contractor as part of their [redacted] contract. This contract was the preferred route for [redacted] to access network connectivity. It was put in place as a security enhancement above the previous in place in house services. [redacted]

These technologies are still relevant to protect the organisation post incident and despite the shift in technology stacks as a result of it. Many highlighted how these technologies have, or are being, augmented by additional protection mechanisms afforded by:

[redacted]

Since the incident significant progress has been made. Most notably amongst these was the recovery of user's emails.

At the time of interviews, a total of 103 priorities were identified that required completion before June 2021, and each of the priorities had dependencies.

Since the attack on SEPA the workload placed on IS is now is greater than it was prior to the incident. Criminal enterprises may target the same victim multiple times. It is important that this workload is constantly managed to avoid mistakes, misconfigurations, and vulnerabilities.

R12: Review the workload and priorities, making them ambitious, realistic and attainable.

Management response:

Our future workload priorities will be developed and approved through SEPA's Annual Operating Plan.

This will be considered in conjunction with recommendation 8 where we will review the ongoing resourcing requirements of the IS function.

Owner: [redacted]

Deadline date: [redacted]

R13: Produce a process for the implementation and verification of each system/service before it goes live and before the next priority is tackled. This should tie in with security standards, and documentation to ensure the systems fully and correctly implemented and to avoid repeating past omissions.

Management response:

In line with recommendation 11 we will only introduce software, systems and IT equipment that has been approved by Agency Management Team. These will be verified by our Change Control Board to ensure compliance with our security and governance standards prior to *go live*.

Owner: [redacted]

Deadline Date: [redacted]