Southend-on-Sea Borough Council

Report of the Executive Director (Transformation) to

Audit Committee

on 20 October 2021

Report prepared by: Brad Warren, Head of IT Security and Compliance

Agenda Item No.

Cyber Security Update

A Part 1 Public Agenda Item

1. Purpose of Report

1.1 To report to the Audit Committee the Council's current position in respect of cyber security given the Council's reliance on ICT to be able to function effectively, including remote working in response to the Covid-19 pandemic, and the difficulties that have been encountered by other local authorities recently.

2. Recommendations

2.1 The Audit Committee notes the report outlining the actions taken to enhance the security of the Council's ICT environment, the challenges being encountered and the work that is being done to address these.

3. Background

3.1 Southend ICT take cyber security seriously. Since the new ICT team was formalised in 2020, a key focus area has been addressing and reducing cyber risk. Local authorities and government bodies are constantly under attack and appropriate counter and protective measures need to be taken.

3.2 The underlying architecture needs to be secure by design, and that means adopting an approach that ensures any new technology fulfils this need. The overarching Smart Strategy principles reference secure by design and underpins our approach to cyber security:

3.3 **Secure by Design**: our new solutions are designed with security in mind, to ensure that security has been built into them from the ground up.

- We are very aware that cyber security is a moving target and will constantly strive to update and manage our focus on keeping the Council safe and secured.
- We will build a more resilient environment by applying security in layers.
- Trust is given but must be verified will be applied to all solutions. All suppliers will be required to adhere to our security policies.
- We regard security as everyone's responsibility, educating all users appropriately.
- We collaborate within trusted partnerships regarding security threat intelligence.

- We will identify all key business systems and ensure these reside in our disaster recovery facility.

3.3 The vast legacy estate made this more challenging and more urgent. While the risk can never be eliminated, the team has made significant progress since the initial review and assessment. NIST (National Institute of Standards and Technology) is utilised as a standard to align and measure against. This is also supported by the NCSC's approach.

4. Council Security Strategy, Programme and Cyber Risk Position

4.1 During the early days of the pandemic, ICT Security (hereinafter referred to as ICT) conducted a review and assessment of the capabilities, policies, technology and processes in place at Southend. The cyber security programme at the Council was introduced through Q2 and Q3 2020. The Cyber Security Strategy, approved by the Good Governance Group and published in October 2020, outlines the key elements of the security programme, capability, priorities and a view of the Southend cyber risk position. The cyber risk position informs our Corporate Risk CR5 which is reviewed and reported a priority risk within the Corporate Risk Register.

4.2 Cyber security has been prioritised within the ICT programme of work, with investments approved in the previous and current financial periods. Starting in April 2020 with the formation of the security function, several improvements, efficiencies and risk reduction strategies have been identified and delivered including the following:

- Implementation of all National Cyber Security Centre (NCSC) Active Cyber Defence services.
- Refreshed all Information Security and supporting policies to align with new ways of working and technology.
- Provided regular communications, guidance and training through multiple channels in support of changing culture and awareness related to Cyber, including role and technology specific skills sessions.
- Enhanced identity, device and application security within Microsoft Azure and Office 365 eg. Multi Factor Authentication (MFA).
- Implemented secure device configuration in line with NCSC and Microsoft baselines and recommendations for all end user devices eg. Laptops and Desktops.
- Standardised all end user and mobile devices with cloud-based device management for increased resilience.
- Rolled out of enhanced email encryption for all users – integrated to Microsoft's Office as standard.
- Provided cloud-based OneDrive storage for increased data governance, security and resilience.
- Formalised and continuously improving our Cyber Operations capabilities, including training and certification to industry recognised standards.
- Trained key members of ICT Operations and Security in accordance with NCSC accredited Cyber Incident Planning and Response curriculum.
- Actively participated in initiatives and knowledge sharing with our local WARP and Essex Online Partnership Cyber Working Group.

- Contributed to the research and beta stage testing of MHCLG Cyber Health Framework initiative.
- Have developed and started to use tried and tested Vendor and Supplier Assessment process to address cyber and data security risks in our supply chain.
- Are working closely with Resilience and Emergency Planning Leads to ensure our cyber incident response preparedness is formalised, exercised and communicated effectively.
- Cyber security briefings for Members and for the Digital Champions community. This has led to better engagement with those cohorts and extending our proficiency and awareness out into many more areas of the Council.
- ICT communications often include key reminders related to cyber security and we will continue to raise awareness of issues that may impact on our technology and that we know many of us use in a personal capacity. A recent example being the critical security updates to Apple's products.

5. Current Threat Landscape: Council Insights

5.1 Although ICT have invested and uplifted our cyber security capabilities, the reality of the cyber security threat landscape is that organisations such as Southend will be under constant attack. The team observe such attacks on our users and systems on a significant scale and frequency, some are very persistent and targeted. Even with continual maintenance, improvement and adjustment to our security programme and controls the likelihood of a successful cyber-attack remains, and we therefore also must focus on more than simply defence, but on overall organisational resilience. There are several areas where we particularly apply our focus:

5.2 **Ransomware** continues to be a major threat to local authorities (and wider public and private sector). With local authorities such as Redcar and Cleveland and Hackney being crippled by cyber incidents in the last year and many private companies also suffering attacks we are on constant alert to this threat. In recent weeks more information has been released including a case study issued by MHCLG RED on the Redcar and Cleveland cyber-attack. ICT Cyber and Emergency Planning leads have reviewed the case study, attended briefings and carried out our own gap analysis resulting in a separate report to CMT - due for presentation in October '21.

5.2.1 **Ransomware Insights**: Not only have the Council ICT team significantly uplifted technical countermeasures through the adoption of advanced threat protection across cloud and end user computing but have introduced technology to help identify and contain the impacts of Ransomware. Should the council be unfortunate enough to be impacted by any ransomware that evades detection and prevention technologies this would significantly reduce the potential impacts through loss of data due to encryption. Importantly this further mitigates risks of Ransomware to our legacy infrastructure and data.

5.3 Attacks targeting **Remote and Home Workers** accessing cloud services eg. Office 365 remain on the increase. ICT continue to educate all Council staff, update our technology for everybody, and gain greater visibility and protection using cyber security technologies invested in and deployed in the last few months.

5.3.1 **Insights**: The team recently observed more than 20,000 thwarted and unsuccessful attempts across a 30-day period that can be attributed to malicious sources and with a fingerprint of known attack tools and techniques. Many are identified by alerts which the team then investigate further. This aids in checking controls and mitigation which are in place. The ability to identify risky activity, identities, devices and applications has been critical in contributing to the positive cyber operations so far.

5.4 **Email Phishing** (emails, SMS and telephone scams) continues to be the most prevalent vector of attack. The team have very good insight into the number of attempted phishing emails which are quarantined and blocked ('zapped') within the systems, however like all organisations some will always slip the net, and these continue to be identified. The team regularly engage with users around spotting and reporting phishing and other suspicious email and have simplified the reporting processes along the way.

5.4.1 Worldwide, there are **Massive Data Breaches** reported on almost a daily basis, each of which feeds the dark web market of identities and stolen passwords. Raising awareness of the risks that weak and re-used passwords present both to Council and to Council employees is critical for this reason. The team will continue to share good practice and use technologies that help to reduce the burden on users to choose and use passwords as the only line of defence by adding layers of security – an example of this is the introduction of Multi-Factor Authentication, Conditional Access and application Single Sign On facilities.

5.4.2 **Insights**: the ICT team were able to tap into publicly available intelligence sources which show that around 20% of current Council users email addresses, and other credentials in some cases, are contained within breach data sets that an attacker could use to target the council.

5.4.3 This can be partly attributed to people using their Council email address to communicate or register with organisations that have suffered a major data breach. This is not unusual, cannot be undone, but having knowledge of the extent and detail allows the team to understand the targeting and anatomy of attacks that focus on the Council. This knowledge is used to inform the view of prioritising investigative or proactive actions targeting people or groups eg. Councillors, Senior Executives and Officers in areas of higher risk.

5.4.4 The team also observe attacks which originate from our suppliers and partners across the borough, and where we can, we notify or alert them to the potential that they have a cyber security issue and offer support and guidance towards the appropriate police, NCSC and other agencies that can assist them.

6. Exercising, Assurance and Compliance

6.1 **Phishing**: ICT have been able to enhance internal capability which allows the team to carry out advanced phishing attack simulations. Not only does this test resilience to the attack vector of a particular malicious email, but also allows the team to provide instant tailored learning opportunities to those people who may require them.

6.1.1 In the most recent exercise including over 2400 staff the team received over 300 reports of the simulated phishing email (with over 200 of those in the first hours of delivery). 3% of recipients opened the malicious attachment and would have been compromised in a real attack. All of those who were susceptible in this exercise have been automatically delivered additional learning and awareness material. This exercise reflects the efforts that have been made to increase awareness of the threats and how to report them with the reporting rates rising significantly. It is crucial to note we are all too aware that it only takes one person, and one click to trigger a potential security breach and so early reporting provides ICT with the best chance to identify and contain / remove threats from the systems. We will continue to educate, raise awareness and exercise all our staff and members.

6.2 Independent Maturity Assessment: PWC have recently completed a maturity assessment against a wide range of controls aligned to the NIST Framework the key findings of which have been shared with ICT and incorporated into strategy, plans and the ICT investment case where necessary.

6.3 Remote Working and DR and Recovery Audits 2020: Internal audit carried out fieldwork with assistance from PWC to assess the processes, controls and operation of these areas. Action plans were put in place which align to ICTs prioritised programme of work across cyber security and ICT Infrastructure and Operations. The team continue to work towards improvement and remediation activities in those action plans agreed.

6.3.1 NHS Data Security and Protection (DSP) Toolkit Compliance: ICT have recently submitted evidence of compliance in line with requirements to NHS DSP Toolkit standards due to the information shared and processed in relation to use and interfaces with NHS data and systems. ICT have met the required standards for 12 monthly certifications.

6.4 We have continued our work with the Business Continuity and Emergency Planning teams, both around the assessment of our risk, in particular the Redcar & Cleveland cyber case study, and our Cyber Incident Response Plans.

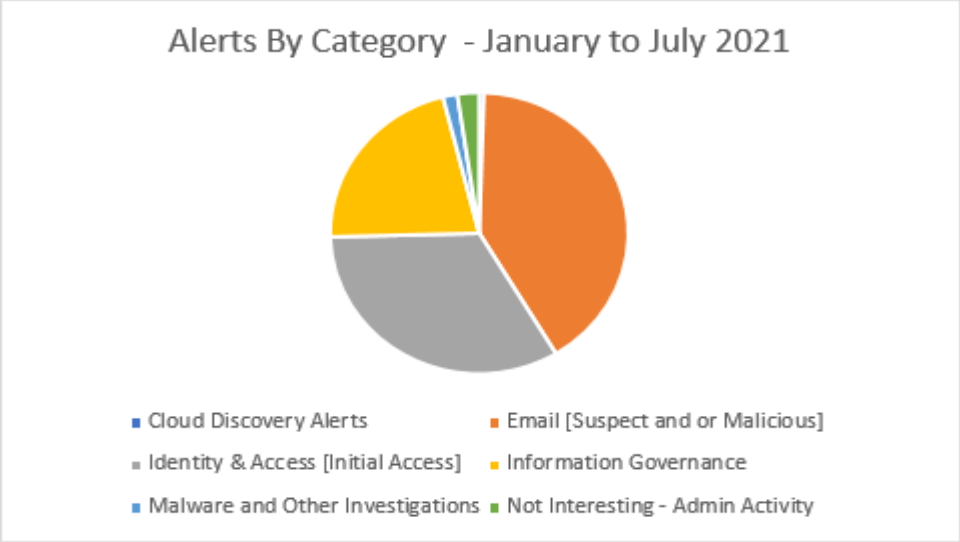
6.5 Much progress has been made internally, and also in conjunction with the wider Essex Resilience Forum and Essex Online Partnership cyber frameworks for coordination and information sharing across these cohorts. Plans are being discussed to exercise plans at all levels, and we will update as and when we have committed timelines for these to take place.

7. Cyber Security Operations

7.1 As covered elsewhere the team have seen in excess of 20,000 attacks against our cloud identities each month, plus hundreds of emails monthly that are blocked due to the email containing malware and/or other threats e.g. Phishing emails with links to malicious sites. These emails are received 24/7 and although some of the threats, alerts and investigations are automatically processed, the majority require analysis by the team.

7.2 Over the 6 months of January to July the team responded to 2172 alerts and incidents* across a broad range of attack vectors and categories, although the majority fall across three categories:

- Phishing attacks
- Identity and Access attacks
- Data handling/access related alerts



7.3 Typically, these are high volume and following investigation non-impacting, but all have potential to quickly escalate into a Major Incident or Cyber Incident Response. Because of this the team plan and prepare for the worst-case scenario.

7.4 We have been working with our technology partner Bullwall to develop and implement our Ransomware Containment solution. This has been challenging as the Council are using some of the most sophisticated end user computing and security products as a result of our MS Enterprise Agreement. This has led to greater opportunity but also far greater challenge for all parties. We are about to go live, having completed final testing and assurance. The outcome being we have greater protection across Council data on the premises, in the cloud and protecting some of our most valuable assets including backups and application environments.

8. Device Modernisation and Stability

8.1 We continue to make great progress in the programme of laptop replacements which allow us to both refresh the hardware and deliver a more secure and resilient working environment and an end to our legacy Windows 7 security risks.

8.2 As of this update over 1900 laptops have been replaced. As these new devices are issued, they are now enrolled into industry standard configuration, protection and advanced threat protection and management through our E5 Security capabilities. These are fully integrated into the Ransomware Containment scope and can be isolated in a fraction of a second when threats are identified.

8.3 Through this work we also identified some users of old mobile devices and apps who have been assisted with updates and provided with new devices in some cases to ensure they now support modern security protocols and MFA.

9. Conclusion

9.1 Much has been done to strengthen the cyber security position of the Council over the past year, but much remains to be done and will be tackled on an ongoing basis.

10. Reasons for Recommendations

10.1 The Audit Committee needs to be aware of the Council's position in respect of cyber security arrangements to assist with enabling it to effectively discharge its responsibilities and to ensure that adequate progress is being made to address the issues arising from the challenges being faced and the work being done to address them.

11. Corporate Implications

11.1 Contribution to the Southend 2050 Road Map

The ICT environment is a significant part of the architecture required for the Council to function and be able to deliver the Southend 2050 Road Map.

11.2 Financial Implications

The ICT environment is highly complex and multi-faceted that requires significant ongoing investment by the Council to enable the delivery of the Council's duties, responsibilities, ambition and outcomes and to protect that environment from threats that exist in the external ICT environment within which the Council has to operate.

11.3 Legal Implications

The Council needs to ensure that it complies with Data Protection legislative requirements and the cyber security and other arrangements are deigned to support this objective.

11.4 People Implications

All Council officers and Members have a role to play in keeping the Council's IT environment as secure as possible and regular information is shared with them to remind them of this.

11.5 Property implications

The ICT equipment operated by the Council needs to be kept appropriately secure and arrangements are in place to deliver this, although most of the risks being faced do not arise from physical security, but cyber security.

11.6 Consultation

The report has been discussed and agreed with key officers at the Council.

11.7 Equalities and Diversity Implications

There is nothing to raise at this time.

11.8 Risk Assessment

The risk arising from cyber security is included on the corporate risk register and there is a risk register maintained specifically in respect of the issue.

11.9 Value for Money

The investment the Council makes in the ICT environment, architecture, infrastructure and security is reviewed by the Investment Board to assess the business case for the investment being made, including the delivery of value for money.

11.10 Community Safety Implications

There is nothing to raise at this time.

11.11 Environmental Impact

There is nothing to raise at this time.