London Borough of Enfield

General Purposes Committee

26 November 2020

Subject: **Cyber & Technology Security**
Cabinet Member: **N/A**
Executive Director: **Executive Director Resources**

Key Decision: **N/A**

Purpose of Report

This Cyber Security report sets the current position for the organisation, the progress against the Cyber Security Remediation plan of activities and risks.

Proposal(s)

1. Recognise and accept the risks and findings in this report
2. To recognise and accept progress against the Cyber Security Remediation Programme

Reason for Proposal(s)

3. This report provides the existing assurance levels including the use of industry standard tools and local reporting.
4. Increased remote working and increased cyber threats to public sector organisations.
5. Successful attacks on peer organisations.
6. We have been successful in thwarting these attacks, but as these attacks become more sophisticated and are created and distributed using software rather than individuals, then the capacity and methods to thwart these attacks must change.
7. To ensure that our existing tools and processes are robust we will introduce additional testing programme.
8. To maintain statutory compliance and to remain secure, our processes, products and tools continually need upgrading, replacing and new tools introduced.
9. The whole council needs be aware of the increased risks, remain vigilant

and awareness raised and to know what to do when an issue occurs all supported by training.

Relevance to the Council Plan

10. Managing Cyber Security well contributes to the Council's ability to address the values set out within the Council's plan

Background

11. **The on-going challenge**

Since the July 2020 Cyber Security report, threats worldwide, have continued to increase across all key threats

- Phishing
- Email spoofing
- Ransomware
- Malware
- Distributed Denial of Service

Hackney Council who deliver the same services and use many of the same applications were victim to a ransomware attack in October.

12. **Security Reporting for period**

Incident Reports (1st July 20 to 31st October 20)

Incident Level	Number	Comments
High (severe business impact)	1	Ransomware Attack on Hackney Council – alerted by LB Hackney and National Cyber Security Council – investigation and actions to ensure Enfield Council not impacted.
Medium (potential impact to a business area)	2	Both were investigated, incorrect information being sent via email or to a wrong recipient. These were investigated by Security, Information Governance and if needed be referred to Data Protection none of which had any impact following review
Low (individual impact/advice)	51	Advice, guidance or reporting issues where websites or tools could not be accessed.

Email Security

The council uses specific email monitoring and security tools to monitor incoming and outgoing emails. Since the July report we have undertaken a full review with the supplier that the tools are optimised and reporting and preventing threats entering the systems correctly.

On average we send or receive around 56,000 emails per day and around 48% of those (mainly incoming) are rejected through the filters set within the tools. These include identifying phishing, spam or virus infected emails and incorrect or unsafe email addresses.

While the review provided assurance that the software and processes work well (e.g. no unsafe emails were sent from the council) it did identify that in just one month the software intercepted nearly 200 malware emails alone. In addition, it also provided a series of improvements and remediation that will be incorporated into the Cyber Security Remediation Programme.

Cyber Security Risk Register

Specific cyber risks are mitigated and risks being reduced or removed through the Cyber Security Remediation Programme that is in delivery. The risk register is being reviewed and will be presented in the next report.

13. Current Progress and Achievements since last report

Phishing Simulation and Testing to monitor awareness and reporting

Over 3,700 users targeted with simulated email, around 23% clicked the link, 3% reported it. The outcomes have been used to raise awareness to key stakeholders, all council employees and will now be repeated on a quarterly basis to identify whether improved compliance awareness and reporting is successful.

Multi Factor Authentication implemented

Multifactor Authentication (also known as Two-Step verification) has been introduced across the whole council. The rollout was expected to complete in July, but in agreement with stakeholders was staggered across the period to ensure all users were supported in the changes. The change has been implemented successfully, with barely any calls or issues being raised and is now part of the standard tools used by the organisation.

PCI/DSS Certification

This is the statutory certification that enables the council to receive and issue payments on our network. The certification was achieved on 4th September.

PSN (Public Services Network) Certification

In July we reported that the re-certification process for accessing Public Services Network (the closed private network used by public sector bodies to exchange information securely) had been delayed in agreement with the cabinet office because of the impact of COVID19. We resubmitted our application in September. They have not taken away our certification as the council has no critical vulnerabilities but they have now required the council to undertake further remediation which it expects to complete by the end of this financial year and at which point it will then commence the next certification process.

NHS Toolkit Submission

The annual return that demonstrates to NHS that we are compliant with security and information governance standards to be able to share data with them. This was completed in October.

Cyber Security Remediation Programme

The programme has now been scoped, activities banded and work has commenced on completing the relevant activities.

There are over 100 activities across 9 delivery streams:

Applications and Toolsets (21)
Assurance and Reporting (11)
Business Continuity and Disaster Recovery (9)
Communication and Publicity (12)
Funding and Costs (1)
Governance and Standards (28)
Risk Register (5)
Service Improvement (6)
Staffing and Support (7)

Since commencing the programme, 17 activities are now completed with around 80 more to be completed by the end of March 21.

Reorganisation of Digital Services (Formerly ICT)

Service Management and Governance Service has been created, reporting into the Director of Digital, Data and Technology. The Head of Service, Martin Sanders is now in post, and Security, Information Governance and Service Management and Delivery now sit in a single service. This has enabled the Security and Information Governance Teams to be realigned to increase resources to deliver both the compliance, assurance and maintaining the security of the organisation, but also to be able to deliver against the Cyber Security Remediation Programme. The next stages will be to bring in some specialist

fixed term roles to ensure we have capacity to deal with new and emerging threats.

The reorganisation and the Digital Services strategy will enable the organisation to look to achieve ISO Standards in the year 2022/23.

Maintaining existing standards

- The Change Advisory Board (CAB) review each ICT change against Cyber Security standards
- All ICT projects are reviewed and signed off against security standards before they are approved
- All ICT suppliers must meet Enfield's Security Standards as part of their contractual terms
- Standard Security Risk Assessments are undertaken for any new or changed ICT tools
- Information Governance Board Terms of Reference have been revised to meet the new standards and re-organised service
- A council-wide Security Assurance Board is now in place to cover all security risks including Cyber

14. **Projects to delivered**

Cyber Security Remediation Programme

As noted above, all projects are being delivered under a single holistic programme. The previous separate technology projects failed to deliver a joined up programme.

This programme is targeting the majority of its' delivery by the end of March 21.

However, as the programme has begun delivery, it is becoming clear that Enfield needs to invest in new and replace some applications and toolsets to both maintain its' statutory compliance in light of emerging threats, but to raise its standards to National Cyber Security standards and be able to achieve ISO accreditation in the future.

Main Considerations for the Council

15. Awareness of new and emerging threats. Although the council acted quickly to review and mitigate the risks of the Hackney Council attack, it demonstrated the impact of a Cyber attack on a London Council, closing it's services down entirely and it still continues to recover the situation. The impact of such an attack, are not just reputational, they are financial, impact on jobs and service delivery and ultimately can impact on the ability to deliver frontline services affecting people's lives.

16. The direction of travel on delivery of the Cyber Security Remediation Programme is good and moving fast. It requires council wide engagement and support to ensure that it is delivered, embedded and then improved upon to enable the council to remain assured.

17. To maintain and improve its standards, the council will need to continue to invest in its' applications, infrastructure and toolsets to keep pace with cyber security threats to keep entire council network safe from attack.

18. Failure to implement these changes will result in the organisation being non- compliant with the Public Services Network(PSN) and Payment Card Industry (PCI) meaning that we will not be able to share data with other public sector organisations or take on line payments.

19. In addition, the Council has reviewed the Emergency Planning procedures in the light of the Hackney event so that authority is in place to take action at pace in the event of a cyber attack and there are plans in place to simulate a cyber attack in the new year to test out plans.

Safeguarding Implications

20. Maintaining compliant Cyber Security is essential to all services and in particular services for children, young people and vulnerable adults. This report seeks to demonstrate the existing position for the organisation and its' proposed way forward to maintain compliance and reduce risks.

Public Health Implications

21. Service delivery requires compliant and secure systems, this includes any services delivering public health. This report seeks to demonstrate the existing position for the organisation and its' proposed way forward to maintain compliance and reduce risks.

Equalities Impact of the Proposal

22. There are no impacts from this report

Environmental and Climate Change Considerations

23. This Cyber Security report proposes creation of programme of work within the existing service area and staff without any change on property use or energy consumption or carbon emissions or impact on environmental management.

24. This report does not require or request any funding or approval of contracts.

Risks that may arise if the proposed decision and related work is not taken

25. Non-compliance with Security Standards will prevent the council taking payments or sharing information with other public sector organisations.

26. The increased number of cyber threats will continue to grow as the organisation uses more technology. The impact of COVID alone demonstrates that the increase is something that the organisation has

little control over, so it requires the tools and standards in place to deal with it.

27. Staff cultural awareness of cyber security risks will not be embedded in the organisation.

28. Increased ransomware attacks pose direct risk to the authority's systems.

29. Increased Phishing attacks pose a risk to the organisation.

30. End of life software that is still in use will continue to present a risk.

Risks that may arise if the proposed decision is taken and actions that will be taken to manage these risks

31. Cyber security attacks, in particular those with criminal intent, will remain an ongoing risk, however, these actions set out mitigate this risk for the organisation.

Financial Implications

32. The financial implications of the Cyber Security programme are funded through the existing Digital Services budgets. As new software and requirements emerge from this ongoing strategy this will be addressed via the medium term financial plan and capital programme; this is a high priority spend area for the Council.

Legal Implications

33. None

Workforce Implications

34. None

Property Implications

35. None

Other Implications

36. ICT Implications are covered within the report and within the risks.

Options Considered

37. Do Nothing was not considered as Enfield would lose its' statutory compliance certifications and put its' entire network and services at risk

Conclusions

The council has committed to delivery of a Cyber Security Remediation Programme and implemented a supporting structure to mitigate risks, maintain compliance and keep ahead of emerging threats.

By delivering that programme, it will provide a basis to raise standards to be ready to achieve ISO accreditation on 2022/23 onwards. It requires the entire organisation to understand it's responsibility to comply with, support and raise awareness and to help Digital Services in keeping the organisation compliant, secure and safe.

Report Author: **Martin Sanders**
Head of Service Management and Governance
martin.sanders@enfield.gov.uk
02081320061
Date of report: **17th November 2020**

Background Papers

The following documents have been relied on in the preparation of this report:

None