London Borough of Enfield

[Committee Name]
General Purposes Committee - Cyber & Technology Security
Meeting Date 04 August 2021

Subject: **[ ]**
Cabinet Member: **[ ]**
Executive Director: **[ ]**

Key Decision: **[ ]**

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.

The council continues to improve its' Cyber Security position, implementing new tools, improving its' processes and monitoring threats, but with increasing and emerging threats that means the speed of progress is slower than originally planned.

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. Resources required to maintain security
7. Cyber Security Strategy being drafted
8. To ensure that our existing tools and processes are robust we will introduce additional testing programme.

9. To maintain statutory compliance and to remain secure, our processes, products and tools continually need upgrading, replacing and new tools introduced.

10. 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

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

Background

12. The on-going challenge

Since the November 2020 Cyber Security report, threats have continued to increase across all areas

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

13. Key Global and National Security Threats identified

By working closely with National Cyber Security Centre (NCSC) and their teams, we are made aware of threats and advice on how to deal with them.

Some key incidents you may have been aware of via the press that they have advised on.

SolarWinds Network attack was a global attack on a provider of network monitoring. By early intervention, we were able to follow the NCSC guidance and work with suppliers to apply security patches to all our servers and our network was not compromised. NCSC have since advised that they believe this to be a state sponsored cyber attack.

Microsoft Exchange Servers which handle email, were attacked globally, those servers impacted in our infrastructure applied security updates and continue to do so in line with guidance from NCSC and Microsoft themselves. This is seen as a cyber attack by unknown actors.

PrintNightmare was a vulnerability exploited on Windows Servers that enabled an attack to take control of a system, and Microsoft released updates that were applied to remedy this.

In all the above, while the council were not impacted directly, the work involved to implement these changes caused by the increasing level of threat at a global and national level.

14. Update on risks affecting Local Authorities

In the last report that was presented in November, the impact of the cyber attack on Hackney Council was raised. Working with peer organisations and National Cyber Security Centre and looking at the impact and lessons learned, we continue to review and where necessary make changes to deal with the risks identified.

The types of attack suffered by Hackney, and other council's such as Redcar and Cleveland have an initial impact on services, but also the time and cost taken to recover services.

15. Security Reporting for period January to June 21

16. Incident Reports

Incidents are captured where a specific issue has been identified that requires investigation. These can be reported by individuals, captured by teams and suppliers looking after the council's information security or through working closely with peer organisations who will raise the alert.

In line with the increasing volumes of threats being detected using our own tools, our close working with National Cyber Security Centre and on-going raising of awareness, there has been increased number of incidents identified, an increase of around 100% compared to the previous reporting period. In particular using tools and reporting to identifying vulnerabilities and attacks such as Phishing has meant a significant increase in Critical/High Incidents being identified.

Table 1	**Open**	**Closed**	**Total**
Critical/High (severe business impact)	**7**	**21**	**28**
Medium (potential impact to a business area)	**12**	**52**	**64**
Low (individual impact/advice)	**7**	**84**	**91**
Total	**26**	**157**	**183**

Of the 28 Critical/High Incidents these were classified under the following:

Table 2

Identified/Reported by	Number	Types	How reported
Digital Services	21	Phishing Vulnerabilities Firewall Intrusion Malware Cyber Attack Data Privacy	NCSC Reporting Tools Alerts Self-Reporting
People	3	Phishing Data Breach	Self-Reporting
Place	1	Phishing	Self-Reporting
Resources	3	Phishing	Self-Reporting
Total	28		

17. Email Security

The council uses specific email tools and processes to monitor email traffic which both assist in intercepting and removing attacks such as malware, phishing and information that is inappropriate.

Tools that quarantine emails, that may need to be reviewed are also in place, along with the requirement to categorise emails according to the information and recipient. A new tool is being rolled currently to improve the categorisation further.

Between January 2021 and June 2021, the council received 6.8m emails of which 0.8m (12%) were rejected using the tools and processes now in place. Examples of the rejections included Virus detection, invalid addresses, incorrect categorisation markers, anti-spoofing tools. The levels of rejection can vary daily, depending on whether there are co-ordinated attacks on the council email.

18. Cyber Security Risk Register

Cyber security risks help to identify the risk of a cyber attack or data breach on the organisation,

Risks are identified as part of both our day to day monitoring of Cyber Security, awareness of threats and risks raised through groups such NCSC, our suppliers, our tools and through internal processes, such as compliance monitoring and audits.

Of the 285 risks identified to date, 158 have been closed the remaining 127 remain open as follows:

Table 3

Risk Level	Open
Critical/High	86
Medium	28
Low	13
Total	**127**
Risk Type	**Open**
Cyber Security	41
GDPR	5
Multiple	75
NHS N3	1
NHS N4	1
PSN CoCo	4
Total	**127**

Many of these risks are being addressed through the Cyber Remediation Programme that is in delivery which has assisted in closing risks to date. Some risks remain open as we tolerate them, but it is the risks that we can treat that we are working on. To accelerate the closing of these risks, we will engage additional professional services in 2021 to close those we can treat.

19. Current Progress since last report

20. Mandatory Cyber and GDPR Training developed and introduced

A revised set of training modules which records confirmation that staff have undertaken training annually has been developed and rolled out from April 2021. This will be reported on annually and those that fail to undertake reported back via Information Governance Board for action to be taken. This will be reinforced by raised awareness sessions and workshops across the organisation which will cover Information Governance and Cyber Security.

21. Phishing Simulation and Testing to monitor awareness and reporting

New tools have been acquired to enable this to be carried out more regularly and will enable targeting of specific groups of staff, or to simulate specific types of attack. The recent exercise targeted over 2,700 staff. The number of people clicking on the link increased from 23% to 38%, but the number reporting it

increased from 2% to 5%. We are now able to target specific teams and individuals so we can provide clearer feedback and this will feed into the awareness raising and training that will be undertaken this year.

22. Multi Factor Authentication implemented

Multifactor Authentication was completed for some remaining areas of the council that had been overlooked. This was completed through the ongoing pandemic, ensuring that security was significantly increased, but without any impact on staff. No calls were made at all to the service desk.

23. PCI/DSS Certification

This is to ensure our on going ability to take payments. Our next step of certification is due for conclusion by the end of September 2021. To ensure we achieve this, we are supplementing our team by using professional services to complete this.

24. PSN (Public Services Network) Certification

This is to ensure that we can continue to connect to and share data with other public services. The PSN certification work is due for completion at the end of July and we are also supplementing our team with a professional service to ensure this is completed.

25. 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 by June 2021.

26. Cyber Security Remediation Programme

This programme continues to be delivered. The original plan was expected to be mainly delivered by the end of March 2021, however there have been some delays in delivery of both some of the tools and recruiting staff to implement these changes.

The programme was developed and split into 100 small projects or tasks to be completed and with the increasing numbers of risks and incidents being identified, this has now increased the number to 123. 38 are completed, 54 are in delivery and 31 are to be started. As a result, the plan delivery dates are being adjusted, additional staff are being recruited and professional services have been procured to assist in delivery. In addition, the Digital Services Portfolio Programme agreed in February 2021, will help to provide programme resources to implement many of the new applications and toolsets identified in the

programme. The revised timeframe for the completion of the plan is currently anticipated to be within the current financial year.

27. Testing our Disaster Recovery

In addition to introducing specific testing of our processes to deal with Cyber Security incidents, a Disaster Recovery exercise was undertaken in April 2021 to simulate a failure of systems and need to recover these. The findings of this exercise will be used to implement a Disaster Recovery test by the end of September 2021 for key systems and this will also reflect the requirement to test Business Continuity plans for services using those systems. To assist with this, a professional services supplier will be engaged to undertake this.

A further annual testing plan will be developed as part of the overall Cyber Security Remediation Plan.

28. Maintaining existing standards

The following governance remains in place

- The Change Advisory Board (CAB) reviews and each change against Cyber Security standards
- Information Governance Board reviews Security Reporting at each board
- Security Assurance Panel reviews a Cyber Security Assurance
- 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 tools, applications or infrastructure

Further steps have been added

- Strategic Portfolio Governance now includes Cyber Security and Information Governance as part of its' initial review and sign off
- Internal Audit reports on use of Cloud computing and Cyber Security were undertaken in early 2021, and the findings used to implement further improvements to the process
- Digital Services Contract and Supplier Process has been updated to ensure that suppliers must demonstrate adherence to our standards both during the contract award and through the lifecycle of the contract

29. Reshaping Cyber Security Delivery

Building on the progress over the past 12 months, we intend to reshape the existing service by implementing even more focussed service and support and delivery. That will include changes in reporting lines and resources needed to deliver a Cyber Security service that meets the need of the organisation.

Main Considerations for the Council

30. Awareness of new and emerging global and national threats with increasing numbers that are identified and prevented. The impact on the services delivered by the council if these managed to breach the council's defences would be critical, both impact on service delivery and availability, financial impact and reputation.

31. The direction of travel on delivery of the Cyber Security Remediation Plan remains in a positive direction, but has slowed down due to availability of resources and the increasing number of tasks reflecting the increased threats. While council wide engagement and support is in place, the requirement to bring in both additional resources and professional services is recognised to ensure that it is delivered, embedded and then improved upon to enable the council to remain assured. The revised delivery date of the programme being adjusted to the end of the financial year is noted.

32. 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. The Digital Services Portfolio has specific remediation activities now included to assist in delivering these.

33. The organisation has statutory requirements be compliant with the Public Services Network (PSN), Payment Card Industry (PCI) and NHS Digital Toolkit, to enable it to share data with other public sector organisations or take on line payments.

34. The requirement to undertake increased testing of processes and disaster recovery is resource intensive and requires additional professional services to provide assistance to undertake this regularly.

35. An exercise to review Digital Services Security compared to peer organisations has commenced, indications are that other organisations have increased their capacity significantly and that review is expected to be completed by the end of August 2021.

Safeguarding Implications

36. 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

37. 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

38. There are no impacts from this report

Environmental and Climate Change Considerations

39. 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.

40. 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

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

42. 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.

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

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

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

46. 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

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

Financial Implications

48. 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

49. None

Workforce Implications

50. None

Property Implications

51. None

Other Implications

52. Digital Services implications are covered within the report and within the risks.

Options Considered

53. 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.

In the first six months of 2021, the number of incidents identified increased by 100%. This demonstrates that we are improving reporting and resolving more incidents, but reflects the increasing volumes of cyber threats and attacks locally and globally. We have improved our processes, monitoring and raised awareness and are working closely with the National Cyber Security Centre, our suppliers and peer organisations to mitigate and resolve threats, vulnerabilities and risks as they are identified.

We have a very clear programme of activities heading in the right direction, but the speed of progress needs to increase. This will be done by increasing resources and using professional services to deliver specific parts of the programme.

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: **4th August 2021**

Background Papers

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

None