.

London Borough of Enfield

General Purposes Committee

Meeting Date 23 July 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, proposed plan of activities, risks and proposed remediation.

Proposal(s)

1. Recognise and accept the risks and findings in this report
2. To support the adoption of NCSC standards and compliance for the organisation
3. To note the proposal to address the key risks through a Cyber Security remediation programme from June 2020 and for regular updates to this Committee
4. To agree the movement of SIRO and CISO roles to the Director of Digital, Data and Technology

Reason for Proposal(s)

5. This report provides the existing assurance levels including the use of industry standard tools and local reporting.
6. With increase in remote working there is a worldwide increase in cyber threats to organisations
7. 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.
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.

11. The council will work to National Cyber Security Centre (NSCS) to ensure it is compliant, uses the best tools and advice available and is an active participant in sharing, mitigating and identifying new risks with its' peer organisations.

12. With the appointment of Director of Digital, Data and Technology to move the Senior Information Risk Owner (SIRO) and Chief Information Security Officer (CISO) roles into that posts' responsibilities

Relevance to the Council Plan

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

Background

14. The on-going challenge

Cyber Security threats increasing worldwide, recent report from Mimecast reporting increase over the past 12 months of over 140% in attacks including:

- Phishing
- Email spoofing
- Ransomware
- Over 40% of small and medium sized organisations suffered a cyber security incident in the past year

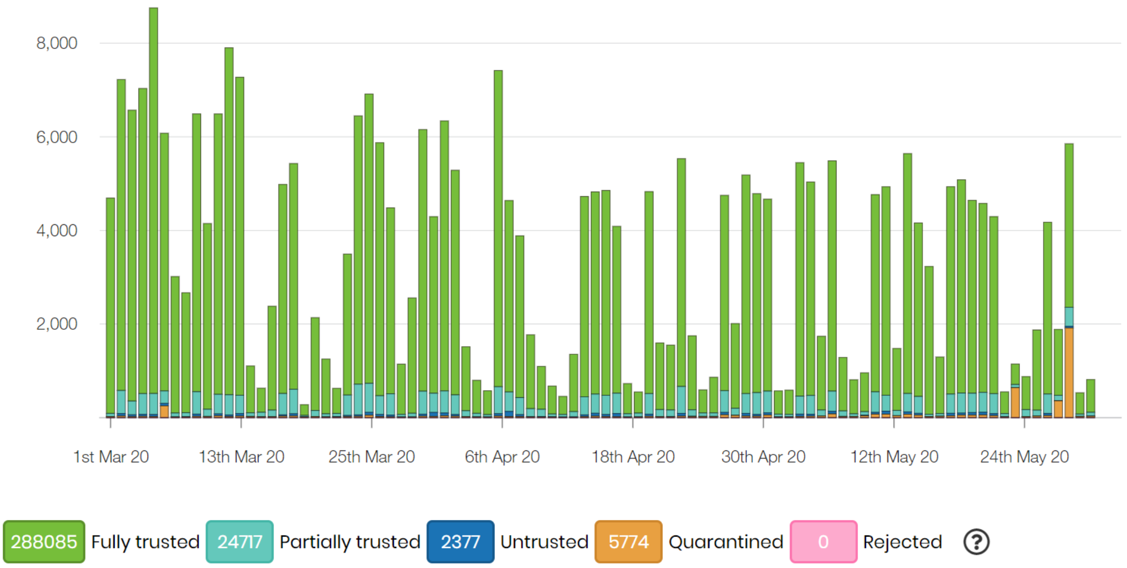
15. Quarterly Security Reporting

Incident Reports

Incident Level	Number	Comments
High (severe business impact)	1	Attempted Financial Fraud through Phishing was detected and reported – payment recovered no loss to council, process amended
Medium (potential impact to a business area)	6	All were investigated, these were generally to do with 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)	44	Advice, guidance or reporting issues where websites or tools could not be accessed.

Email Security – Faking/Spoofing



The table is produced from our Security Monitoring tools and shows looks at emails sent from an enfield.gov.uk address.

The trusted emails are verified from the council, and untrusted and quarantined emails are not. While this demonstrates the value of the tool it also indicates the ongoing and increased levels of attack we are under.

Cyber Security Risk Register

Residual Risk	Cyber Security
3	2
4	
6	4
8	
9	
10	2
12	3
15	1
16	
20	2
25	
Total	12

that

These are specific risks identified all of which are mitigated and risks being reduced or removed through the Cyber Security Remediation Programme will be undertaken in 2020/21.

16. Adopting the National Cyber Security Centre Standards

Report from MHCLG 10th June promoting NCSC standards and tools

The report identified additional key risks and threats resulting from COVID 19 as well as emphasising the existing threats. Some of the increased risks include:

- Increased Vulnerability of Mass Remote Working as staff are using their own internet and are working on their own
- Insufficient staffing to deal with Cyber Threats
- Increased Ransomware attacks from organised criminal groups
- Phishing attacks
- Cyber Enabled Fraud
- Espionage from within organisations
- Disruption from hackers who wish to bring down or disable systems

The NCSC also provided a set of standards and support for the council to use, and we will now work towards implementing in July 2020. These include:

- Reviewing the ICT Supply Chain to ensure it remains secure and robust
- Joining the local Warning, Advice and Reporting (WARP) community to raise and share awareness of current and new threats
- Under the NCSC Cyber Security Survey and use the outputs to feed into our security approach
- Review the existing NCSC Cyber Toolsets to ensure these are all assessed against our current solutions and implemented where required
- Review the benefits to Enfield of joining the Local Digital Declaration used by over 200 public sector organisations including councils, to ensure that Enfield’s Digital and Cyber approach are aligned and it’s profile raised

The output of this review with provided to the Executive Director of Resources and Director of Digital, Data and Technology at the end of July 2020 and we are responding the MHCLG with an outline of our activities in response.

Implementing the standards

As referenced in the Cyber Security Report in March, there is already work being undertaken to address threats raised. The work to address these will be implemented as part of an overall set of activities to implement our standards

- Review the current activities and risks from the March report and progress on proposed activities to address them
- Review the results of the NSCS Review
- The creation of a single Cyber Security Remediation Plan to be used to implement and maintain our standards and address our risks
- A strategic review with Director of Digital, Data and Technology at the end of July
- Increased monthly Cyber Assurance Reporting through dashboard reporting and to the Assurance Board
- Reviewing the Business Continuity testing to include additional tests for Cyber Security attacks such as Ransomware

17. Current Progress and Achievements in last quarter

Increased Training and Awareness

- Developing a programme of Security and Information Governance Awareness for new starters
- New ICT Intranet Page making access to support, reporting of incidents and guidance more accessible
- Specific COVID and Remote Working guidance on Secure Working from home

Permanent Security Team recruited

- These roles have been difficult to fill, leading organisation to rely on contractor staff to support it
- Obtained funding from LGA to provide additional certificated training to the team

COVID 19 – Secure Remote Working solutions

- Increased remote working capacity to cover all staff and members
- Added additional secure tools to support access for all applications (Forticlient)
- Prioritised and brought forward rollout of networking and firewall upgrades
- Social Media/Video Conferencing – securely risk assessed new tools such as Zoom, and introduced secure rollout avoiding issues encountered by other public sector organisations

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

18. Projects to delivered

Multi Factor Authentication

In March we reported that we would be implementing Multifactor Authentication (also known as Two-Step verification). With the increase in remote working this is even more urgent and this has started to be rolled out, with the expectation that it will be completed by the end of July.

This will reduce the risks, such as an attacker learning someone's username or password, since it requires a second level of authentication such as code to your phone.

PSN (Public Services Network) Certification

In March we reported that we were completing the re-certification process for accessing Public Services Network which is the closed private network used by public sector bodies to exchange information securely. The council's IT systems are complex and require continuous updating, patching and vulnerability management throughout the year to maintain compliance to the PSN certification.

While Enfield has no critical vulnerabilities there is on going work being completed to address the remaining lower level ones. This activity has been delayed in agreement with the Cabinet Office to enable organisations to focus on addressing the new threats from COVID19.

The work on the certification has continued and is expected to complete by the end of September 2020.

ICT Security, Information Governance and Data Protection Dashboard

Development of a new dashboard feeding from the security tools and systems to present a holistic view of all reporting by the end of September 2020.

Test Scripting for Security

To review existing testing processes, to enable testing of cyber security threats including Phishing, Ransomware and use of tools to undertake Penetration Testing. This to be completed by September 2020.

Business Continuity Cyber Security Testing

To incorporate Cyber Security tests into the Annual ICT Business Continuity Testing, this includes simulation of Cyber threats including Ransomware and Phishing attacks.

This is intended to by undertaken in November 2020.

Main Considerations for the Council

19. Adopting of NCSC standards recommended nationally with a support network of peer organisations is an industry standard specifically used in the Public Sector. This will help compare against peers and enable us to raise standards without the additional costs normally associated with third parties setting standards.

20. Address the key risks through a Cyber Security remediation programme from June 2020 ensures that all aspects needed to address risks, including toolsets, testing, processes, training and on going performance monitoring are captured in a single programme, rather than as separate projects.

21. To agree the movement of SIRO and CISO roles to the Director of Digital, Data and Technology, ensures that the both recognition and responsibility for risks and the tools and resources to address them sit under one Director.

22. As stated in March, the proposed approach is adopted by leading ICT organisations building on the existing security and compliance approach, but recognising that the increasing volumes and types of cyber security threats require an approach that increases and makes use of industry standard tools to protect an organisation of our size and type.

23. 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.

24. In addition, the existing software and infrastructure will be unable to keep pace with cyber security threats making the entire council network vulnerable to attack.

Safeguarding Implications

25. 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

26. 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

27. There are no impacts from this report

Environmental and Climate Change Considerations

28. 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.

29. 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

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

31. 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.

32. Security risk awareness among staff is low

33. Increased ransomware attacks pose direct risk to the authority’s systems

34. Increased Phishing attacks pose a risk to the organisation

35. End of life software that is still in use

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

36. None

Financial Implications

37. None

Legal Implications

38. None

Workforce Implications

39. None

Property Implications

40. None

Other Implications

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

Options Considered

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

43. Increase staff resources without changing its' approach to tools and software. The increasing number and nature of security threats cannot be resolved by increased staffing alone, new products that identify, isolate and resolve risks are also required.

Conclusions

Along with all local authorities, there continue to be an increasing number of and more sophisticated set of Cyber Security threats, that will continue to grow. By implementing a programme to remediate and mitigate those risks and adopting a set of National Cyber Security standards, the organisation will be able to monitor and reduce the impact of those risks.

Report Author:	**Martin Sanders** **Service Management and Governance Manager** **martin.sanders@enfield.gov.uk** **02081320061**
Date of report:	**1st July 2020**

Appendices

Key Threats:

- **Phishing:**

  Scammers will convince users to click on misleading links to provide sensitive information or company data, or even download content to their computer or server.

- **Malware:**

  If a victim of phishing does end up initiating a download, there's a good chance that the program received is harmful or malicious and comes in various forms, tasked with anything from spying on the system to manipulating its code.

- **Distributed Denial of Service (DDoS):**

Floods the server with requests from multiple sources, leading it to become overwhelmed to the point of slowing down substantially or even crashing.

- **Brute Force or Password Attacks:**

  These threats involve an attacker attempting to gain access to a network by using a program to ascertain a working password.

- **Ransomware:**

  This is a type of malware that, when opened, encrypts the system so that no one can use it anymore. The computer or server affected will remain locked until a hefty ransom is paid to get the encryption key to unlock the system.

<u>Security Controls in place:</u>

- **Email protection:**
  Mimecast includes - email protection and back up of email in the cloud to protect from phishing and malware

- **Mobile Device Management: (Mobile phones)**
  Lookout - mobile security to protect from phishing, malware and ransomware. The increasing volume of mobile devices require additional licences.

- **Microsoft Azure Cloud:**
  Microsoft Security Centre: Azure disk Encryption: Azure Cloud APP Security: Advance Treat Protection: Backup and Site Recovery: AZURE Key Vault: AZURE PIM: Threat Intelligence (Dark Trace): Making use of treat feeds to detect malicious intrusion and data exfiltration to command and control servers. These all protect from Distributed Denial of Service, Ransomware, Brute Force or Password Attacks as well as provide Disaster Recovery protection. However, as threats increased and the amount security applications increase, we require more resource to operate them

- **Managed Clients – Device Endpoint Protection (e.g. laptops, desktops, servers)**
  System Centre Configuration manager: Microsoft Defender: Threat Analytics: Windows 10 Enterprise Security. These protect against all the above risks. These products regularly become outdated as threats change and need replacement and updating more frequently than we have existing budget and resources to do.

- **Hybrid Security Solutions (e.g. Working from Home, 3rd Party sites, on site connectivity)**
  Firewalls: Directs Access VPN: Fortinet VPN: Express Route (Direct Connection to Azure): Log Management: Pen Testing: Vulnerability Scanning. These protect from Distributed Denial of Service (DDoS) and Brute Force or Password Attacks. Products such as Direct Access and Remote Desktop Access that we use to work from home become out of date and therefore stop working with our protection and have to be replaced.

List of Security controls in place to address known threats and compliance requirements

Area	Tools	Outstanding Risks	Phishing	Mal-ware	DDoS	Brute Force	Ransom-ware	Compliance
Email protection	Mimecast	The license type has limitations that would not allow archiving and investigations beyond 30 days	Y	Y			Y	Y
Mobile Device Management	Lookout - mobile security	The number of licences is insufficient for the estate.	Y	Y			Y	Y
Microsoft Azure Cloud	Microsoft Security Centre	No. of applications increased and need more Computing, Storage and FTE resources to monitor alerts			Y	Y	Y	
Managed Clients – Device EndPoint Protection	System Centre Configuration manager: Microsoft Defender & MDM	These products become outdated quickly and need replacement and updating frequently	Y	Y	Y	Y	Y	Y
Hybrid Security Solutions	Firewalls, Direct Access, VPN, Fortinet, Proxy	Direct Access/ Remote Desktop Access that we use to work from home become out of date and stop working with our protection and have to be replaced			Y	Y	Y	Y
Vulnerability management	Tenable.io	Initial phase of review						Y
Protective Monitoring / Complian	Caretower Managed Service via McAfee SIEM	All LBE kit should be onboarded for monitoring but are not now. A resource is (Appliances and FTE)						Y

ce (e.g. PSN)		required to on-board all LBE Kit						
Multifactor Authentication	Microsoft MFA	This has not been rolled out to all users				Y		Y
Geolocation locking	Microsoft Azure Security	Access from countries we do not do business with increase the risk						

Background Papers

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

None