# Birmingham City Council

# Report to Cabinet

**9th February 2021**

| | |
|---|---|
| **Subject:** | **Update on the delivery of the Birmingham City Council Information and Communications Technology and Digital Strategy (2016-2021)** |
| **Report of:** | **Director, Digital & Customer Services** |
| **Relevant Cabinet Member:** | **Cllr Brigid Jones - Deputy Leader** |
| **Relevant O &S Chair(s):** | **Cllr Carl Rice, Chair, Co-ordinating Overview & Scrutiny** |
| **Report author:** | **Dr Peter Bishop**<br>Director, Digital & Customer Services<br>Tel: 0121 675 5762 Mobile: 07864 926819<br>Email: peter.bishop@birmingham.gov.uk |

| | | |
|---|---|---|
| Are specific wards affected?<br>If yes, name(s) of ward(s): Birmingham City Wards | ☐ Yes | ☒ No – All wards affected |
| Is this a key decision?<br>If relevant, add Forward Plan Reference: ref 008382/2021 | ☒ Yes | ☐ No |
| Is the decision eligible for call-in? | ☒ Yes | ☐ No |
| Does the report contain confidential or exempt information?<br>Information relating to the financial or business affairs of any particular person (including the authority holding the information). | ☒ Yes | ☐ No |

## 1 Executive Summary

1.1 The purpose of this report is to update Cabinet on the implementation of the delivery of the Council's Information & Communications Technology and Digital Strategy (IT&D Strategy 2016-2021) and in particular to our Cyber Security and to secure further funding for the implementation of the Cyber Security Strategy (Appendix A).

1.2 The report builds on the progress made since the previous update to Cabinet on 5th June 2020, with a specific review of our Cyber Security Strategy to ensure we continue to adapt best practise to protect the delivery of our services for the Citizens of Birmingham. Our Cyber Security investment does need to keep pace with the changing threat landscape.

1.3 The report will provide Cabinet with an update on the current security position, achievements made to date, recommendations for further funding and an overview of the new Cyber Security Strategy.

## 2 Recommendations

2.1 That Cabinet:-

2.2 Approves the Cyber Security Strategy (Appendix A) and specifically option 1 from Section 4.4 and delegates authority to the Deputy Leader, the Chief Financial Officer and the Director Digital and Customer Services to implement.

2.3 Notes the additional funding requirement for the ICT & Digital Strategy of £12,428,695 (In section 9.3 Option 1) to fund the implementation of the Cyber Security Strategy. This is made up of £12.003m revenue funding, following a contribution of £1.1m from the net controllable ICT service budget, and £0.425m of capital funding, after a contribution of £1.775m from the technical refresh programme. This requirement will form part of the standard budget setting process with the financial plan that will go to cabinet in February for approval.

2.4 Authorises the City Solicitor to negotiate, execute, seal and complete all necessary agreements and documentation to give effect to the above recommendations.

2.5 Notes that Cabinet will receive a performance report of the implementation of the Cyber Security Strategy as part of the yearly update to Cabinet as part of the ICT & Digital Strategy performance report.

2.6 Recommend that the performance of the Cyber Security Strategy will be reported and monitored by the Councils Audit Committee.

## 3 Background

3.1 Cyber-based crime presents a significant threat to UK business, local and national government. Local government is particularly prone to attack as the diversity of systems and services provide many opportunities for cyber criminals to disrupt council services. The Covid-19 pandemic has seen an increase in cyber-attacks further stressing the need for the Council to be proactive in managing the risks involved.

3.2 The LGA highlights the importance of cyber security as an integral part of local government's wider work to digitalise services and improve productivity. It states that "With councils making more local public services available digitally, getting more of their workforce online and planning greater collaboration and integration work with partner organisations, reviewing and reinforcing current cyber security arrangements is a key priority for local authorities.

A cyber incident can be very disruptive, leading to the loss of data, as well as disruption to the running of council services".

Note:https://www.local.gov.uk/our-support/efficiency-and-incomegeneration/digital/cyber-security)

3.3 The cyber security threat landscape for local councils, is always evolving and there have been a number of successful cyber-attacks on councils in the UK.

Note: https://www.localgov.co.uk/Cyber-attacks

Councils that have had cyber-attacks have had a severe impact on their services to citizens. Example service impacts have been online citizen services, payroll, housing, social care services, planning and Council Tax. These attacks have cost those local authorities millions of pounds to recover and involved significant disruption.

3.4 In a report by Big Brother Watch based on responses from 395 local authorities the following observations were made. Note: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/02/Cyber-attacks-in-local-authorities.pdf

3.4.1 UK local authorities were subjected to at least 98 million cyber-attacks between 2013-2018.

3.4.2 114 (29%) councils experienced at least one cyber security incident in an actual security breach,

3.4.3 25 councils experienced one or more cyber security incidents that resulted in the loss or breach of data. UK local councils faced 263 million cyber-attacks in first half of 2019. The report went on to say: "The unrelenting cyberattacks that UK councils experienced in 2019 will not abate in 2020. Due to the IT staff limitations that these councils often deal with, they would be wise to invest in automated security analytics solutions that can identify and mitigate the cyberattacks that human personnel would never be able to keep up with".

Note: https://www.localgov.co.uk/Councils-hit-by-800-cyber-attacks-an-hour/4826

3.5 The National Cyber Security Centre (NCSC) in their March 2020 cyber breach survey reported that the number of security threats has not diminished and that cyber-attacks have evolved and become more frequent. The Birmingham 2022 Commonwealth Games will also bring additional scrutiny to the Council and the Council's systems. Increased cyber-attacks were common during the 2018 Commonwealth Games in Australia.

3.6 The COVID-19 pandemic has also led to an increase of Cyber-attacks by 40 percent.

Note: https://securityboulevard.com/2020/11/40-increase-in-ransomware-attacks-in-q3-2020/

This has re-focused the threats of Cyber-attacks for the following:

- Ransomware
- Phishing
- Remote Working

The Council needs to adapt to this changing threat landscape, and this is clearly noted in the Councils Strategic Risk Register.

3.7 The ICT & Digital strategy's overarching principles to "Simplify, Standardise and Share" ensures that the council maximises the benefits from investment in new technology and digital services by:

- **Simplify** – the way we operate, in order to add value and drive up efficiency.
- **Standardise** – the way we operate, emulating the best and enabling agility.
- **Share** – collaborate, innovate and inform.

These design principles will ensure that we:

- Consolidate services and applications.
- Re-use and rationalise.
- Share with and learn from partners, internally and externally.
- Don't reinvent - learn from others and share.

3.8 The ICT & Digital Strategy and other portfolio documents form a Governance and Assurance framework for the design and implementation of ICT and will help ensure that there is an evidence-based approach to the choice of technologies the Council can use. In October 2016 Cabinet approved the Council's ICT & Digital Strategy, which formed a new framework for ICT service operation around 6 key themes:

1. Integrated ICT and Digital Services - to deliver a reliable, flexible, integrated, secure, accessible and well managed service.

2. Digital facilitation - to enable our stakeholders to participate and fully contribute to the growth of the Digital Economy and Digital Society and create a Digital Culture.

3. Insight - to become more data centric – so we can create the capability to turn information into insight.

4. Commissioning - to deliver 'Value for Money' services through the commissioning of excellent ICT and Digital Services.

5. Governance - to deliver the effective management of ICT and Digital Services.

6. Innovation - to be innovative; to make changes to what's established, by introducing new methods, ideas, and solutions.

3.9 To date, the following has been delivered to improve the current cyber security posture and security capabilities. These activities and future investments are supporting the management of security risks and evolving security threats.

- Firewall upgrade,
- DDOS prevention upgrade,
- Internal vulnerability scanning,
- Bring Your Own Device (BYOD) introduced with correct security controls,
- Microsoft Advanced Threat Protection for email has been procured as part of Office365 renewal,
- Secure Remote Working,
- Projects and IT&D strategic programme support,
- Cyber awareness and training,
- Red Team assessments (independent advanced penetration tests) to establish a security baseline,
- Remote collaboration using MS teams and securing Zoom access,
- Increased Cyber security communications,
- Application Platform Modernisation (APM) program has contributed to the provision of new secure infrastructure.

3.10 As a result of this work, the transition back to the Council of the ICT Services, and the rapidly changing threat landscape, the development of a new Cyber Security Strategy, Roadmap and Business Case was commissioned.

3.11 The objective of the Cyber Security Strategy is to improve the Council's Security position through technical and human responses (leveraging technology and security improvements, further testing and actions to address external assessment findings, cyber security awareness and training e.g. Monthly phishing exercises). The key focus areas as referenced in Cyber Security Strategy (Appendix A):

3.11.1 Security Education and Engagement:

- Increase cyber education and user awareness communications to all BCC staff, to be vigilant of phishing emails and remote working threats.
- Target communication to the Council departments to be vigilant of fraudulent payments.
- Build strategic partnerships within the Council directorates and external organisations (Commonwealth games, National Cyber Security Centre), sharing of lessons learnt in the public sector.

3.11.2 Development of the Cyber Security Team .

- Security was managed previously by Capita, with support from the central Capita security teams. The transition back to the Council reduced the security resources available to support the cyber services required to protect the Council and require:
  - Increase resources in the team to proactively manage the increased threat level.
  - Additional capability, capacity and resource in order to inform, educate and support the key Council objectives.

3.11.3 Policy and reporting:

- Reviewed security policies and processes, including Incident response plan.
- Reviewed backup strategy for ransomware resilience.
- Increased monthly security reporting to Information Assurance and IT Strategy boards.

3.11.4 Development of the wider ICT & Digital strategy requires the need for additional security and technology controls to ensure full security protection of the Council and its customers.

## 4 Options considered and Recommended Proposal

4.1 Throughout the COVID19 pandemic, officers have been seeking to find a best value approach to improve the Cyber Security position of the Council, as detailed in the Cyber Security Strategy (Appendix A). The following options have been considered:

4.2 **Do nothing** - On presentation of the ICT & Digital Strategy in 2016, Cabinet recognised that it would be possible to continue without delivering the ICT & Digital Strategy. However as ICT is a key enabler for the Council Delivery Plan, not delivering the key areas of the ICT & Digital Strategy, would negatively impact on its success. The Council has also seen significant improvements in its efficiency and effectiveness as the strategy has been implemented.

4.3 **Deliver** the ICT & Digital Strategy - As the Council has already approved the strategy and the associated technical refresh programme, and ICT is a key enabler for the future the work needs to continue and delivery the Strategy and its associated projects. However, Cyber Security investment does need to keep pace with the changing threat landscape.

4.4 The following options for Cyber Security were reviewed and option 1 is recommended**:**

- **Option 1:** Strategic risk will be addressed though the ALL funded strategy roadmap activities. Significantly improve and strengthen Council Security posture,
- **Option 2** : The Council will have sufficient capabilities to defend a cyber-attack(s). Reduced resources, detection, respond and recover capabilities in the event of a major cyber-attack,
- **Option 3**: The Council will have technologies in place but significantly reduced capabilities to defend a major cyber-attack(s). Inadequate resources, detection, respond and recover capabilities in the event of a cyber-attack(s).

## 5 Impact for local people and service customers

5.1 The recommendations within this report would provide the public with the reassurance that the Council IT systems, infrastructure, data and customer data is protected with a view to sustain Council business with minimal interruption of service.

## 6 Consultation

6.1 External consultation: The Cyber Security Strategy (Appendix A) was drafted to build on the existing work that has been completed, build in feedback from the various external assessment activities the Council has undertaken e.g. LGA Rand Report, NHS Toolkit etc., and advice from National Cyber Security Centre (NCSC) and Industry peers.

6.2 Internal Consultation: Council Leadership Team, Director of Finance, Legal, HR and Procurement.

6.3 The Leader and Deputy Leader have been consulted regarding the contents of this report.

6.4 The Cabinet Member for Finances and Resources, the Chair of Resources Overview and Scrutiny Committee, the Chair of Co-ordinating Scrutiny Committee, the Leader of the Conservative Party, the member with responsibility for ICT matters from the Conservative Party, Leader Liberal Democrat Party and the member with responsibility for ICT matters from the Liberal Democrat Party and the Green Party have been consulted regarding the contents of this report.

6.5 Birmingham Children’s Trust and Birmingham 2022 Commonwealth Games have also been consulted.

## 7 Risk Management

7.1 Strategic risks are reviewed monthly and reported to Audit Committee three times per year, of which Cyber Security has been allocated a high risk level.

7.2 In terms of the service, there are a range of risks being managed as the strategic outcomes are delivered through the strategy. These are:

7.2.1 The digital skills and culture change needs of the Council may demand far more effort than planned for and funded within the programme but are essential to deliver the new ways of thinking and working necessary to exploit the opportunities enabled by the new technologies being implemented.

7.2.2 Lack of suitably qualified and available skills at the time they are needed to implement the new technologies being delivered.

## 8 Legal Implications

8.1 The Council is under a duty under Section 3 of the Local Government Act 1999 to make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness

8.2 The City Council will carry out this work under the General Powers of Competence Section 1 of the Localism Act 2011.

## 9 Financial Implications

9.1 Consultations have taken place with the Director of Finance. There are financial implications for the Council to consider in relation to fund the recommended option, detailed within the Exempt Report (Appendix C).

9.2 The funding requirement will form part of the standard budget setting process with the financial plan that will go to cabinet in February for approval.

9.3 Currently Cyber Security has a controllable net budget of £0.308m that is forecasted to be fully spent in 2020/21. The original ICT investment for Cyber Security was very limited and does not adequately meet the changing threat landscape.

The following financial options have been considered:

9.4 **Option 1:** Strategic risk will be addressed though the ALL funded strategy roadmap activities. Significantly improve and strengthen Council Security posture.

9.4.1 Funding totalling £12.428m is required over the next four financial years up to and including 2024/25.

9.4.2 This is made up of £12.003m revenue funding, following a contribution of £1.1m from the net controllable ICT service budget, and £0.425m of capital funding, after a contribution of £1.775m from the technical refresh programme.

9.5 **Option 2:** The Council will have sufficient capabilities to defend a cyber-attack(s). Reduced resources, detection, respond and recover capabilities in the event of a major cyber-attack.

9.5.1 This requires funding totalling £10.128m. This is made up of £9.703m revenue funding following a contribution of £0.813m from the net controllable ICT service budget, and £0.425m of capital funding, after a contribution of £1.775m from the technical refresh programme.

9.6 **Option 3:** The Council will have technologies in place but significantly reduced capabilities to defend a major cyber-attack(s). Inadequate resources, detection, respond and recover capabilities in the event of a cyber-attack(s)

9.6.1 This requires funding of £5.837m, all of which is revenue monies, following a contribution of £0.678m from the net controllable ICT service budget.

9.7 All capital monies can be funded by a contribution from reallocation of the technical refresh programme. The government has announced as part of the latest spending review additional funding to be assigned to Cyber Security for Local Government. The Council will bid for this funding when the applications are made available.

## 10 Procurement Implications

10.1 Each software, hardware or service required to deliver the Cyber Security Strategy will be covered via an individual Procurement Strategy. Each strategy will detail the procurement approach, route to market and evaluation criteria, and will follow agreed governance arrangements. To help inform the Procurement Strategies early and active market engagement will take place to;

- Allow for innovative solutions to be explored with market leaders
- Leverage expertise within the marketplace to inform procurement decisions
- Create interest and competition within the market, and
- Ensure a robust market tested approach for each procurement

10.2 The level and type of market engagement will be established on a case by a case basis.

## 11 HR Implications

11.1 There are no immediate HR implications. Any recruitment opportunities will be carried out in line with Birmingham City Councils Recruitment and Selection Policy and Procedure.

## 12 Public Sector Equality Duty

12.1 An Equality Analysis was completed during the development of the ICT & Strategy (2016-2021). There has been no change to that analysis.

## 13 Appendices

- Appendix A - Cyber Security Strategy
- Appendix B - Equality Impact Analysis (EA001412)
- Appendix C - Exempt Report

## 14 Background Documents

- Report to Cabinet 18th October 2016 - Birmingham City Council Information & Communications Technology & Digital Strategy (2016 - 2021)
- Report to Cabinet 18th October 2016 - Birmingham City Council Strategic ICT & Digital Investment Programme (2016 - 2021) ICT and Digital Strategy (2016 – 2021)
- Report to Cabinet of 27th March 2018 - Outcome of final stage negotiations between BCC and Capita - proposed IT and Digital Service Transition Roadmap to 2020/21, with associated investments and benefits (appendix 2 gives a summary of performance against the strategy)
- Report to Cabinet of 14th May 2019 - Update on the delivery of the Birmingham City Council Information and Communications Technology and Digital Strategy (2016-2021)
- Report to Cabinet 5th June 2020 – Update on the delivery of the Birmingham City Council Information and Communications Technology and Digital Strategy (2016-2021)