City of Westminster

Audit and Performance Committee Report

Meeting:	Audit and Performance Committee
Date:	18 July 2024
Classification:	General Release
Title:	Cyber Security
Wards Affected:	All
Key Decision:	None
Financial Summary:	N/A
Report of:	Gerald Almeroth, Executive Director, Finance and Resources Becky Chapman, Interim Chief Digital and Innovation Officer

1. Executive Summary

At the February committee meeting several questions were raised about cyber security at Westminster City Council. This summary is intended to answer these questions and provide Members with assurance of Westminster's ongoing cyber security operations. The service is continuously developing, and we recognise that there are always improvements to be made. We brought in some expertise to lead the team at the end of April 2023 and have since implemented a significant number of new measures which are outlined below.

2. Recommendations

For committee members to note and feedback as required.

3. Cyber Security Training

Cyber security training is an important part of Westminster's security strategy and equips people with the knowledge and skills needed to protect themselves and the organisation against cyber threats.

A new process has been implemented to improve compliance levels and ensure users receive timely communications about the importance of their training along with additional guidance. Since this has been implemented, compliance levels have substantially increased and currently stands at ~80%. The Cyber Security and Data Protection team will continue efforts to improve this, with oversight provided by the CDIO and Executive Director.

Councillors are provided the opportunity to undertake cyber security training as part of their induction. In addition, a new training platform has been delivered in April that provides Councillors with role specific content that is endorsed by the National Cyber Security Centre (NCSC). It is expected that Councillors will be aligned to staff and undertake this training on a yearly basis. However, as this is not mandated in policy, we are working with colleagues in Governance and Councillor Liaison around how this is managed.

Further developments are being planned, such as providing role specific training for those considered sensitive, high profile or likely to be targeted. The Learning Management System will be enhanced to support bite-size 'Micro-Learning' to allow us to respond more quickly to changes in the threat landscape.

4. Phishing Campaigns

Phishing simulations are a proactive measure that imitates malicious attempts to deceive users into providing sensitive information such as usernames and passwords. Westminster City Council has an ongoing campaign that will perform different phishing simulations to enhance employee awareness and reduce the risk of breaches. Furthermore, the outcomes are an important

indicator of how effective cyber security engagement, and the training programs are in the organisation. By integrating phishing simulations into cyber security operations, Westminster will create a more security-conscious workforce and significantly improve their overall security posture.

Phishing simulations that focused on Councillors were undertaken in 2022, and wider Council staff in 2023. Additional simulations that target specific groups (including Councillors) as well as organisation wide campaigns are being planned in coordination with the Cyber Security and Data Protection communication and engagement strategy. The results of these will help inform and shape our engagement and training activity to improve people's awareness of the increasing risk of malicious attacks.

5. Communications and Engagement

There will be an increase in cyber security engagement efforts as part of a 12-month communication plan. Each month will have a theme with content delivered in different ways to maximise employee engagement and the security impact. This will include:

- Cyber security information portal.
- Regular communications, including Loop Live.
- Bite size videos.
- Local office awareness campaigns, such as posters.
- Lunch and learn presentations.
- Drop-in sessions.

The communications and engagement plan will be linked to both the cyber security training program and phishing campaigns allowing each to inform and be informed by the other.

6. General Cyber Security Developments

Westminster City Council continue to develop security capabilities making the organisation more resilient to the growing threat of cyber-attacks.

This includes enhancements of the protective controls, monitoring, detection, and the ability to respond and recover from a major incident. These include:

- Improvements in the security tooling specifically focused on better coverage of internal and external environments. The systems are better integrated to support a single security control plane. WCC security tools provide:
    - Advanced Anti-Virus, Anti-Malware and Ransomware protection for clients, servers and other infrastructure. Enhanced detection of threats with automated investigation and response to contain risks.
    - Identity security ensures that people accessing WCC services are who they claim to be and are authorised to access the information they are

requesting. Technology such as Multi Factor Authentication is enforced and correlated with patterns of behaviour analysis to identify unusual activity that needs investigation.
    - Protection for our Microsoft 365 environment by verifying the authenticity of external parties communicating with WCC. Files, attachments and links are all analysed in real time to enhance the security in Email, Teams, SharePoint and OneDrive.
    - Ensuring the security posture of WCC's cloud environment through continuous assessment against industry standards and recommendations identified and implemented through continuous improvement plans.
    - Analysing how the organisation is using external cloud services and providing WCC with the ability to control access and enforce data loss prevention controls to secure information.
- Mobilising a 24/7/365 Security Operations Centre with the ability to respond to threats any time of the day or night.
- Reducing the attack surface and moving towards a zero-trust architecture.
- Hardening the environment, including significant supply chain partners.
- Improving the vulnerability processes and reducing our mean time to respond and remediate.
- Managing exposure to improve visibility and remove security blind spots.
- Adopting AI to help identify indicators of compromise or insider threats.
- Improving response capabilities through tabletop exercises.
- Ensuring an industry leading cyber incident response team is available 24/7.

The Cyber Security and Data Protection team analyse risk by calculating the probability and impact of a risk occurring. Using this, the costs of any mitigation strategy are assessed against maintaining the security posture and will inform what technical or procedural controls are required. As the threat landscape changes regularly, this is a topic discussed monthly with the Digital and Innovation management as well as the Executive Director responsible for Cyber Security to ensure the balance is retained.

Cyber security is a priority for Westminster City Council to ensure vital services remain available and information about citizens, residents, businesses and partners remain secure.

7. Security Events

Since the start of the year Westminster City Council have had 442 incidents identified and investigated by our Security Operations Centre. 39 of these required an immediate response actioned within the hour to protect the organisation, 24/7/365.

Most of the attacks target our people. This is predominantly through email, and in the last month, ~114k were blocked for being malicious.

The second largest vector is through attacks trying to compromise user accounts. In the last month there has been over 70k suspicious, attempted logins from overseas with the majority originating from China and Russia. These were all blocked.

Many attacks try to create a sense of importance or urgency. In the last month, 12 emails were sent to specific users disguised as an email from our CEO attempting to redirect funds or obtain sensitive information. These were all detected and blocked.

Finally, securing the supply chain is essential, and where a partner or supplier is compromised, WCC often need to restrict communications between the organisations until they have been secured. Three separate suppliers have been compromised in the last month with connectivity limited to protect the Council.

5. Financial Implications

Within the Digital and Innovation capital budget there is funding identified for the enhancement of our cyber security activity. In 2024/25 the capital budget is £471,000, with £50,000 available for each of the next four financial years. Expenditure will be mapped against emerging need.

6. Legal Implications

N/A

7. Carbon Impact

N/A

8. Equalities Impact

This paper refers to organisation-wide activity, that will apply to everyone in the organisation. Where needed, adjustments will be made for training provision so that is accessible to all.

9. Consultation

N/A

If you have any queries about this Report or wish to inspect any of the Background Papers, please contact:

Gurpreet Muctor, Chief Data and Technology Officer

APPENDICES

- None

BACKGROUND PAPERS

- None