Audit, Governance and Standards Committee

29 July 2021

Update on Cyber Security Risks

Report by Steve O'Connor, Assistant Director Digital & IT

Relevant Portfolio Holder: Tim Cobbett, Portfolio Holder for Communities and Engagement

Purpose of Report

The cyber security risk is held on the Corporate Risk Register, C&C Risk 57. This paper sets out how the cyber security risks are managed.

The paper provides an overview of the mitigations in place in respect to governance, technology, policy and procedures and staff.

Recommendation(s)

The Committee is asked to RESOLVE that:

1. To note that measures are in place to mitigate the cyber security risks to the Council.

2. Despite the measures set out in this paper it is impossible to fully mitigate the risk of a disruptive cyber attack on the Council given the evolving nature of the threat. Therefore being prepared to manage and recover from an attack is a vital part of the risk mitigation.

Benefits to the Community:

The impact of a cyber security attack, such as a ransomware attack, on the Council would be significant. Services to residents would be severely disrupted and the work of the Council as whole would be impacted. The importance of managing the ever growing cyber security risk is critical to successful operation of the Council and the delivery of services to residents.

Key Points

A. Cyber Security risks continue to evolve and grow and it is critical to the delivery of Council services in our communities that this risk is actively managed. The threat of an attack is high and malicious activity and code are in constant circulation and ever changing. The Council intercepts and blocks malicious activity every day.

B. Without the steps set out in this paper the Council would almost certainly have been severely impacted by cyber attacks with the resulting disruption and loss of services to residents. Malicious activity and attempts to break into networks are endemic across the internet, the threat is ever present. The threats continue to change and evolve and therefore the Council response must continue to adapt. Continued investment in cyber security defences, planning and awareness are vital.

C. The paper sets out how cyber security risks are managed, focusing on four aspects of the mitigations in place, covering;
1. Governance
2. Policies and Procedures
3. Technology
4. Staff Awareness

D. The prevalence of the ongoing cyber security risk to organisations and the ever changing nature of the threats means that it is impossible to provide complete assurance that the Council will not be impacted by a cyber security incident. It is therefore a vital part of our risk mitigation to lessen the impact by being prepared for a major cyber security incident and that the Council is able to recover from such an attack.

Context

1. Over recent months there have been a number of high profile cyber incidents that have been widely reported in the media, ranging from Manchester United through to an attack a lot closer to home in Hackney Council.

2. The highly disruptive attack on Hackney Council in October 2020 has been reported as an example of a ransomware attack. Ransomware is malicious code that encrypts data making it unusable. The attacker will then offer the decryption keys for a ransom. This type of attack is increasingly common and highly disruptive.

3. Recovering from an attack of this nature is complex and time consuming. To reduce further damage you need to effectively shut down your IT network and services. For systems that have been impacted by the ransomware they then need to be rebuilt from scratch using backups. This can take weeks. In some cases if the backups have been impacted or a system is not backed up it can be impossible to restore the service. In Hackney work continues 8 months after the attack to recover services, and this work will continue for some time. The impact of the attack has been felt across the Council.

4. Cyber Security has been and continues to be a priority for the Digital & IT Shared Service. This paper sets out how Cyber Security risks are managed. It will cover:
   a. Governance
   b. Policy and procedure
   c. Technology
   d. Staff

5. **Governance:** The Digital & IT Security Board, chaired by the AD for Digital and IT meets monthly to review the overall cyber security position. This Board is the operational board overseeing the evolving risk position and the policies and procedures including the Acceptable Use Policy for all users of the Council’s IT services. The Security Board reports into the Corporate Information Governance Group chaired by the Council’s Monitoring Officer.

6. The Council has clearly defined roles managing the cyber risks. These include the Data Protection Officer, a technical Cyber team and an independent Cyber security expert and assessor who works with the Digital & IT Team and is part of the Digital & IT Security Board. This role provides expert advice and independent assessment of risk. The Council is well connected into the WARP[1] structure and alerts and advice through the National Cyber Security Centre (NCSC). The Digital & IT Team conducts regular testing to look for security weaknesses as well as regular cyber security audits.

7. The Council has a range of external scrutiny and standards it must adhere to in relation to IT Security. The Council meets the Public Sector Network (PSN) code of connection and this is reviewed and updated every year. The Council must also align with the NHS Data Security and Protection Toolkit which assesses the Council's information governance arrangement including cyber security measures. The Council meets the NCSC Cyber Essentials standards. The Cyber security risks and mitigations are reviewed regularly by audit. These external checks and audits are underpinned by regular scanning and testing including running the NCSC exercise in a box testing our measures and procedures with real world scenarios.

8. **Policies and Procedures:** Underpinning the Governance are a range of policies and procedures. These cover operational running of the IT services including:
   a. A strong patching regime that keeps our servers and devices security patched.
   b. Password and Access control policies
   c. Strong starter/leaver process ensuring the access to the network is removed for leavers.
   d. Acceptable Use Policy
   e. Data breach and cyber incident procedures
   f. Backup procedures
   g. Business Continuity plans

9. **Technology:** The cyber threat to the Council is constant and every day our technology is identifying, blocking and removing malicious code from entering our network. The Digital & IT Service uses a layered approach to prevent a successful cyber attack impacting the Council. In the first instance our technology seeks to prevent any malicious code from entering the network, through a range of measures from firewalls to filtering of emails to remove spam and malware. Anti virus software is deployed across the network. Secondly, specialist cyber security monitoring is in place continually scanning for any unusual behavior across the network. This is monitored by a 24/7 Cyber Security Operations Centre. The shared service arrangements with Sutton Council make this level of security investment possible.

10. Underpinning our defences are a range of technology policies and procedures, including ensuring all our devices are up to date with their patching to remove known vulnerabilities. Access to our services and network is controlled and monitored, for example we use 2 factor authentication to prevent unauthorised access.

[1] WARPs founded in 2003 are a community of peer cyber security leads from the broader public sector in London, councils, police, NHS, Fire & Rescue and some of the major universities with whom data is exchanged. WARPs run on a regional basis and share threat and alert data between each other.

11. The Council has also deployed the NCSC recommended set of tools to provide further assurance and protection. These include further early warning services that enable NCSC to rapidly notify organisations of malicious software. The tools also include further web and mail check services to help prevent email spoofing, spam and phishing.

12. The measures set out above are largely focused on reducing the likelihood of a successful cyber attack impacting the Council. It is not, however, possible to guarantee that a successful attack will not happen. It is therefore critical that we are prepared for any Cyber incident and have measures in place to reduce the impact of a successful cyber attack. Backups of our systems are a key part of our protection. We back up all of our systems and conduct regular testing of our ability to restore data from backup.

13. **Staff Awareness -** The actions of people on the Council network represent the highest risk of cyber incidents occurring. Although a range of the technology defences are in place to prevent threats getting through to users of the network, these technologies cannot stop everything due to the ever evolving nature of the threat. For example some phishing emails (malicious emails designed to look genuine) are almost impossible to block. There are also zero day threats, which are new types of attack that for a short time the technology cannot prevent. It is therefore vital that all users of the network are vigilant and trained in how to spot suspicious activity.

14. All staff have a responsibility to safeguard council information. All staff receive mandatory information governance and cyber security training on an annual basis. This is supplemented by regularly published security advice and guidance, including alerting staff to any new threats. All users of the Council network must agree to the Acceptable Use Policy which sets out the policies and procedures they must adhere to.

15. It is not possible to provide 100% assurance in regards to the Cyber security risk. The threat is always evolving, with new exploits being discovered everyday. We must therefore plan for when a cyber incident occurs not if it occurs.

16. The Council has business continuity plans in service areas for disruption to IT services. These plans will continue to be reviewed, updated and tested on a regular basis to ensure they address the ever changing threat.

Financial Context

17. The council is operating in an increasingly challenging financial environment. Kingston faced a number of financial challenges in the medium to longer term - even before the COVID-19 outbreak, which has further added to these challenges. The economic and financial consequences of the pandemic, growing demand for services, and limited government grant funding make it difficult to find adequate funds to meet the borough's needs.

18. The future of local government finance faces a significant level of uncertainty. The impact of the Fair Funding Review and a future review of business rates is currently unknown, and the lasting effects of COVID-19 on our residents, local businesses and the Council itself remain uncertain.

19. Despite these challenges the council has a drive and commitment to ensure it is doing the best for residents and communities

Resource Implications

20. A disruptive cyber attack would have resource implications, diverting Council officers to the response and implementing business continuity plans.

Legal Implications

21. None

Health Implications

22. A disruptive cyber attack on the Council could impact social care services.

23. A disruptive cyber attack could have mental health implications, including increased stress and workload for Council Officers.

Background papers

None

Author of report - Steve O’Connor, Assistant Director of Digital and IT