Report author: Louise Whitworth

Tel: 07891 276168

Report of Director of Resources and Housing

Report to Corporate Governance and Audit Committee

Date: 22nd September 2017

Subject: Annual Information Governance Report – update on Cyber position

Are specific electoral Wards affected? If relevant, name(s) of Ward(s):	☐ Yes	☒ No
Are there implications for equality and diversity and cohesion and integration?	☒ Yes	☐ No
Is the decision eligible for Call-In?	☐ Yes	☒ No
Does the report contain confidential or exempt information? If relevant, Access to Information Procedure Rule number: Appendix number:	☐ Yes	☒ No

Summary of main issues

1. The Public Services Network (PSN) was set up as an assured route for information sharing by central Government, to facilitate shared services and also serve as the assured route for Government Connects Secure Extranet (GCSx) mail. It acts as a compliance regime that serves as both a commitment to a basic level of information security for connecting authorities and also a level of trust between Leeds City Council and other public services.
2. Due to more stringent compliance controls brought in by the Cabinet Office in 2014 the council are presently unable to meet the PSN certification requirements. The Cabinet Office has contacted the Council through the Chief Executive to ensure that the Council brings itself into compliance as soon as possible. The Council's access to the PSN has not been unduly restricted but this would be a likely consequence if prompt action was not taken.
3. In view of this, the Council is currently working with the Cabinet office to meet requirements by the end of September, a deadline set by the Director of Resources and Housing.
4. Multiple streams of work are supported by Project Managers and Professional leads.
5. The 2017 independent audit of controls revealed a large volume of issues, which must now be resolved before the end of September to prevent further escalation.
6. A programme of works continues beyond the September deadline to ensure the future of Leeds City Council compliance.

Recommendations

Corporate Governance and Audit Committee is asked to consider the contents of this report and be assured that considerable effort is being undertaken to rectify the current situation with

regards to the Council's approach to information governance and specifically in this case PSN compliance.

1. Purpose of this report

1.1 To provide Corporate Governance and Audit Committee with an update on the current position on Cyber Assurance and Compliance, specifically compliance to the PSN Assurance standard.

2. Background information

2.1 Leeds City Council recognises the need to protect its information assets from both accidental and malicious loss and damage. Information Governance is taken very seriously by the council and this is evidenced by the on-going work to improve the management and security of our information.

2.2 The report provides Committee Members with an update and answers to questions posed during the annual Information Governance review.

3. Main issues Cyber Assurance and Compliance PSN

The Public Services Network (PSN) was set up as an assured route for information sharing by central Government, to facilitate shared services and also serve as the assured route for (secure) GCSx mail. It acts as a compliance regime that serves as both a commitment to a basic level of information security for connecting authorities and also a level of trust between Leeds City Council and other public services.

3.2. A number of services are accessed via PSN, Blue Badge, Revenues and Benefits and Tell Us Once for Registrars. PSN certification is relied upon as a mechanism to support information sharing, where many of the requirements request that the council present a certificate prior to sharing, or evidence alternative, more time consuming compliance work to be completed. This has had an impact already on sharing with Health as a number of the controls are evidenced by a PSN certificate. For instance, GCSx mail depends upon PSN certification; JARD (Joint Asset Recovery Database) is presented over the PSN network; new ways of working with the Valuation Office Agency; and, the Family Information Service eligibility, which is a new legislative requirement from September 2017, relies on the council having PSN certification.

3.3. Due to more stringent compliance control brought in by the Cabinet Office in 2014 the council are presently unable to meet the PSN certification requirements. The Cabinet Office has placed the council into an 'escalation' process for PSN, a process by which the Cabinet Office seek commitment from the CEO and provide further support in remediation against the controls.

3.4. The council has since received the IT Health Check (ITHC) results for 2017; an annual audit required for PSN compliance. The ITHC report for 2017 details vulnerabilities across the infrastructure. This audit followed the cabinet office' scope requirements for PSN and as such the number of issues the council must address has grown significantly from 2016.

- A significant number of individual vulnerabilities were revealed on a 10% sample of the estate. The sheer size and volume of unknown issues across the estate evidences systemic failure of controls, previously believed to be sufficient.

- The PSN Assurance team mandates that each vulnerability is extrapolated to the estate as a whole and resolved. Those identified as critical or high must be resolved before the authority can be determined compliant.

4. Actions to date

4.1. A PSN Remediation Board has been established with the Head of Information Management and Governance as Senior Responsible Officer (SRO), reporting to CLT and the Senior Information Risk Officer (SIRO) Monthly. The board meets bi-weekly to work through the compliance requirements and close down remediation tasks realised by the ITHC audit. Monthly meetings with the PSN Authority (PSNA) provide them with regular reports about the progress being made by the council. This relationship is strong and supportive.

4.2. A virtual vulnerability management team has been formed, which brings together the various resources tasked with bringing the patching and configuration of the estate to an acceptable level in order to close or remediate the findings from the 2017 ITHC. The team is responsible for the maintenance of the estate on a periodic basis.

4.3. Relationships with business areas have been strengthened and agreement on appropriate and timely downtime gained. The strength of the PSN board and support of Chief Officers has been fundamental in achieving this.

4.4. The application development, training and support team have begun to contact software suppliers to ensure they meet the requirements set by the PSN Authority on Cloud Security Principles. Further work to understand and update contract terms is planned in the medium term.

4.5. The IT procurement process documentation has been refined and being used to incorporate the cloud security principles which will prevent the purchase of sub-standard ICT solutions in future should all services comply and use the appropriate documentation.

4.6. Seven projects have been funded by Essential Services Programme (ESP) budget in order to improve the security position of the Council in the medium term, aiming for completion by April 2018. Those projects are:

- Vulnerability Management
- User Password Policy and Practise
- Technical authentication
- Protective Monitoring
- Mobile Devices Management
- Network Segregation
- Active Directory cleansing and maintenance
- Once complete, the programme of works is expected to significantly improve the Council’s compliance position.

5. Response to WannaCry

5.1. The Leeds City response to the outbreak of the ransomware Trojan, WannaCry on Friday May 12th was a combined effort between the Council and Health services. The Cyber Incident Response Team was formed and met throughout the weekend. ICT service providers for the NHS, updated the team on any incidents within the City region. Out of band activities ensured the infrastructure was protected and updated to prevent infection. Once the Health service activities were managed and controlled, Leeds City Council, despite no incident employed resources to ensure the same within the council boundary.

5.2. Immediate activities included blocking all mail from the NHS domain, however, it was later discovered that the mode of delivery was not email.

5.3. It was also initially understood and broadcast that the prevalence of old, XP devices encouraged the spread so quickly. That is now understood to be inaccurate; the main reason for swift infection was the method of delivery and poor patching and security practises.

5.4. As a result of the WannaCry outbreak, the practise of stopping standard patching during a 'Change freeze' is now accepted to be poor practise and has halted. Only system upgrades will now stop, during change freeze periods.

6. Risk from NHS and Information Sharing

6.1. The NHS is made up of a number of separate entities with different budgets and priorities. The one constant is the Data Security standards in the IGToolkit for health: the standards to which the NHS are held to. Those standards for information security are improving. It is expected in the next two to three years, for NHS standards to consolidate with the requirements for local authority. The risks to Leeds City Council are expected to decrease following the roadmap for security and compliance as we move towards a shared city platform.

7. Security of Mobile Devices

7.1. The security of mobile devices has been highlighted as one of the areas requiring improvement to meet the PSN standard, as such a new method of authentication is being employed as part of the ESP programme of works.

8. Briefing for all members and staff on Cyber

8.1. The request for a briefing on Cyber is noted and will be actioned.

9. Consultation and Engagement

9.1. Consultation on the development of strategies, policies, procedures and standards are extensively undertaken across a broad range of stakeholders including information management professionals, representatives from all Directorates via representatives of Information Management and Technology Teams and Information Management Board members.

10. Equality and Diversity / Cohesion and Integration

10.1. Equalities, diversity, cohesion and integration are all being considered as part of delivering the Information Management Strategy. This refers to the way training is being delivered as well as how policies will impact on staff and partners.

11. Council policies and City Priorities

11.1. The policies support the Information Management Strategy and contain areas of legal requirement. Furthermore, the implementation of the Information Management Strategy will improve the quality of the council's policy framework by ensuring the authenticity, integrity and security of the information contained therein.

11.2. Under the Code of Corporate Governance in Part Five of the council's Constitution, the fourth principle (taking informed and transparent decisions which are subject to effective scrutiny and risk management) requires decision making processes and enables those making decisions to be provided with information that is relevant, timely and gives clear explanation of technical issues and their implications.

12. Legal Implications, Access to Information and Call In

12.1. Delegated authority sits with the Director of Resources and Housing and Senior Information Risk Owner and has been sub-delegated to the Chief Information Officer under the heading "Knowledge and information management" in the Director of Resources and Housing Sub-Delegation Scheme.

12.2. There are no restrictions on access to information contained in this report.

13. Risk Management

13.1. The risk associated with not implementing information governance policies, procedures and practice across the Council leaves the organisation more susceptible to breaches of legislative, regulatory and contractual obligations, affecting the confidence of its citizens, partners, contractors and third parties when handling and storing information.

13.2. Information risk is being systematically addressed by joining up the approach to risk required by information security standards, the need for the senior information risk owner to be clear about the risks he/she is accountable for and the council's standard approach to risk management.

13.3. Further work is being undertaken in conjunction with the Corporate Risk Manager to embed the recording and reporting of information risk monitoring and management. The Information Asset Register project will generate information required and an automated dashboard will be produced to report risk assessments to the SIRO. This will provide the assurance required by the SIRO from the business and will allow risk mitigations to be prioritised.

14. Conclusions

14.1. The work of the previous year, reported to this Committee in April 2017, has been continued.

14.2. The establishment of improved Information Governance in ICT and improved practice and procedures outlined in this report provides a level of assurance to Committee that the range of information risk is being managed both in its scope and through to service delivery. It allows the council to work with partner organisations, third parties and citizens in a clear, transparent, but safe and secure way. It helps to protect the council from enforcement action and mitigate the impact of cyber incidents aimed at attacking and/or bringing down council information systems.

15. Recommendation

15.1. Corporate Governance and Audit Committee is asked to consider the contents of this report and be assured that considerable effort is being undertaken to rectify the current situation with regards to the Council's approach to information governance and specifically in this case PSN compliance.

15.2. The Corporate Governance and Audit Committee is also asked to consider a report back to Committee in January 2018, to further update with regards to PSN and Cyber Compliance

15.3. Background documents: None