CARDIFF COUNCIL
CYNGOR CAERDYDD

CARDIFF
CAERDYDD

AUDIT COMMITTEE: 13th November 2018

CYBER SECURITY GOVERNANCE, RISK MANAGEMENT AND CONTROL
REPORT OF CHIEF DIGITAL OFFICER

AGENDA ITEM: 4.3

Reason for this Report

1. This report has been prepared to provide Audit Committee members with assurances on Cyber Security Governance, Risk Management and Control.

2. The Audit Committee's Terms of Reference sets out its responsibility:

    a. To monitor the effective development and operation of risk management in the Council.
    b. To monitor progress in addressing risk-related issues reported to the committee.

Background

3. Following a Request from Audit Committee, Cyber Security was escalated to the Corporate Risk Register (CRR) in Q4 of 2016/17. As such the risk is reviewed and updated quarterly by ICT as well as being monitored every quarter by Committee and bi-annually by Cabinet.

4. The release of the Cardiff Council's Digital Strategy at the start of the 2018/19 Financial Year laid out the vision for a more connected and modernised Authority that is able to work for Citizens and Employee's in the modern Digital World.

5. The Digital First and Digital by Default approach outlined in the Strategy means the implementation of new technology, applications and ways of working for Staff. New ways of working open up new avenues of risk and, in turn, must be addressed and governed accordingly.

    a. *"We will deliver simple, efficient and attractive Digital Services that Customers will choose to use instead of the traditional contact channels. We refer to this as making our services "Digital First".*

    b. *"Over time we will aim to make appropriate services "Digital by Default", meaning that they will primarily be available digitally."*

6. When referring to "Cyber-Security" we refer to the set of processes and controls created and put in place in order to safeguard the organisation's data, systems and networks from attack.

7. Cyber Security has found itself in the public eye following high-profile cases of Cyber Breaches

    a. **NHS England and Scotland: May 2017** – Over 70,000 devices (including computers, MRI scanners and theatre equipment) affected after an exploit in outdated Windows systems was found. Resulted in non-critical emergencies being turned away and cancelled operations

    b. **British Airways: August 2018** – 380,000 card payments were compromised. Names, addresses, email addresses and credit card details stolen through exploits in the company's website and app. Required customers to cancel cards and resulted in huge reputational damage

    c. **Facebook: September 2018** – Up to 90 million accounts comprised due to exploit in a "Profile View" setting. Users affected included CEO Mark Zuckerberg. This breach could carry huge financial penalties if GDPR regulations have been violated.

8. These high-profile cases clearly illustrate the need for robust Cyber Security measures and controls that stand up to the task of protecting the Council's vital information. By their very nature Cyber-attacks can be indiscriminate in their approach. Attacks are often automated and exploit known vulnerabilities. Attacks can also be targeted against individuals or bodies.

9. In April 2018 the Government released the findings of its Cyber Security Breaches Survey. Of the 1,519 UK Businesses who took part in the survey, 43% experienced a Cyber-Security breach or attack in the last 12 months.

10. Cyber Security breaches have the potential to compromised sensitive information, corrupt data or inflict huge reputational damage as well as the potential for financial penalties to be incurred if laws and regulations are violated (e.g. GDPR).

<u>Issues</u>

Risk Management:

11. Implementing a robust Risk Management Regime is essential in order to establish a uniform means of identifying, managing and monitoring Risk. The principle method is through the Risk Register process.

12. ICT hold an ICT Risk Register which, in turn, feeds in to the Resources Directorate Risk Register (DRR). The ICT Risk Register is divided into two sections, one for general ICT related issues and one specifically for Cyber Security. Both of these feed into the Corporate Risk Register (CRR) where risks are identified as significant.

13. Two ICT risks are currently on the CRR following escalation from the DRR:

    a. ICT Platforms Unsuitable/Outdated
    b. Cyber Security

    Due to the nature of Cyber Attacks (blanket attacks looking at exploiting out-of-date ICT infrastructure) both risks are intrinsically linked and are reviewed closely during Risk Assessments.

Performance Review:

14. Cyber Security Maturity Assessment is regularly reviewed against 10 key risk factors following the National Cyber Security Centre (NCSC) recommended approach. The 10 risk factors as identified by the National Cyber Security Centre are attached as Appendix 1.

    - Network Security
    - User Education and Awareness
    - Malware Prevention
    - Removable Media Controls
    - Secure Configuration
    - Managing User Privileges
    - Incident Management
    - Monitoring
    - Home and Mobile Working
    - Set up a Risk Management Regime

    In addition to this Cardiff Council has added an 11th risk factor called 'Corporate Cloud Security'

15. Following the latest Cyber Security Maturity Assessments, 3 of the 11 areas of Cyber Security underpinning the Corporate Risk have been identified as containing high risks. These generally are explained as:

    a. **Unsecure Configuration** - Unauthorised access and changes, exploitation of software bugs and insecure system configuration.

    b. **Monitoring -** Assessment of how and when systems are being use; detecting and reacting to attacks or accidental user activity.

    c. **Corporate Cloud Security –** A 2016 Internal Audit identified contract, SLA and service management weaknesses in some externally hosted services.

16. The findings and conclusions of the Cyber Security Maturity Assessments resulted in regular monitoring being undertaken to drive risk-based prioritisation and actions. The 3 high risk areas surrounding Secure Configuration, Monitoring and Corporate Cloud Security are escalated to SMT and improvement actions and support were discussed and agreed at SMT level. Cyber security risk is identified as high because of the potential consequences of any breach. Although the likelihood of breach has been reduced due to security mitigations the consequences of the breach remain high so the residual risk remains high.

17. The principle controls put in place for the risk areas are:

    a. **Secure Configuration -** Established secure baseline and compliance standards with centralised policies to secure user environments.

    b. **Monitoring –** Realtime and reactive log analysis with incident reporting to the Information Security Board (ISB) and discussed with the Internal Audit.

    c. **Corporate Cloud Security -** Maturing Data Privacy Impact Assessment and Cloud Impact Assessments process used to assess risks to data and technology solutions and identify mitigations.

Proposed Management Actions in Cyber Security Corporate Risk:

18. ICT and Information Governance (IG) Teams to continue to liaise with FM for physical security assurances and to promote an incident reporting culture.

19. To enhance user education and awareness via Information Governance Seminars for each Directorate.

20. To ensure strong ICT security, monitoring and cloud security controls:

    a. ICT lifecycle and notification targets are being monitored and managed through the 'ICT Platforms' risk actions

    b. Collaboration between ICT and Information Governance to develop and map current ICT system providers in phased development of an Information Asset Register

    c. Privacy Impact Assessments (PIA) and Cloud Impact Assessments (CIA) to be created and reviewed regularly to ensure compliance with the requirements of the GDPR Action Plan. These assessments are managed by the Information Governance Team and act as general security good practise guidance

    d. Governance and management requirements to be formalised for periodic and systematic review of all ICT systems.

Internal Audit

21. An Internal Cyber Security Governance Audit was completed in March 2018 and a set of recommended actions laid out. These recommendations have been taken forward and incorporated into the CRR as Proposed Management Actions

22. The outcome of the Internal Audit identified "User awareness" as one of the key areas, requiring attention. In addition to the Cyber Security measures already in place, the audit identified that these systems require user knowledge in order for the Council's Cyber Security to be as robust as possible.

23. 12 Cyber Security eLearning modules have been purchased and made available to all Council Staff via the Council's training "Academy" e-portal. These are also accompanied with Cyber-security Awareness videos circulated through staff information.

24. These address the key areas such as good password practise, Internet Security, Phishing Attacks and when to consult ICT to seek advice or assistance. Completion reports are then run monthly to identify staff take-up levels and help assist targeting directorates with low take-up.

Other Review Methods

25. ICT performs reviews of the risks to its service, from Cyber Security and all other sources, on a quarterly basis following the council's standard Risk Management Strategy. This escalates risks through the Directorate risk register on onto the Corporate risk register as appropriate. ICT has a Risk Champion that provides an active input to the overall Directorate risk management regime as a critical friend.

26. Risks are monitored regularly via both ICT and Customer and Digital Management Teams. Risks are escalated to the Information Security Board as well as the Resources directorate management meetings and SMT

27. As well as internal review and audits performed by the Internal Audit Teams and a dedicated ICT Security and Compliance Team, the Council is assessed yearly by the Cabinet Office to ensure it is compliant with the Public Services Network (PSN) security requirements. This enables the Council to communicate across government and public sector organisations and exchange data necessary to perform key Council functions. Examples are enabling our Housing Benefits team to access data from the DWP or to access information on Blue Badge service users securely.

28. This assessment includes a qualified 3rd party independent IT Health Check (ITHC) of the Council's internal and external (internet facing) networks, to find and remediate vulnerabilities and weaknesses to cyber-attacks.

Governance and Control

29. The Digital Strategy key principles outline the strategic direction in which new Digital Services are developed and subsequently implemented. The Digital Strategy key principles are attached as Appendix 2.

30. Key principles include:

    Modern, fit-for-purpose technology will be used to ensure efficiency:
    "We aim to use Cloud-based solutions wherever we can in order to reduce reliance on physical hardware."

    Digital Services will be continually monitored, assessed and improved:
    "We will always test Digital Services thoroughly before releasing them for general use. This will include piloting them to assess the customer experience and completing detailed technical testing to check that they fulfil requirements."

31. These principles are underpinned by the Council's comprehensive ICT Security Policy. The policy, in conjunction with the Information and IT Governance Framework, provides direction and guidance to ensure that ICT security is in line with the relevant laws, regulations and business requirements.

32. Key Message from the ICT Security Policy:

    a. "*All new ICT systems being considered must be assessed and approved through the council's Architecture Review Team (ART). A Privacy Impact Assessment (PIA) should be performed for all new systems in line with the Council's procedures which are outlined within contract award and project documentation"*

33. Data Privacy Impact Assessments (DPIA) are also performed by the Information Governance team on each new business change. One of the subsets of DPIA is the Cloud Impact Assessment (CIA) which focuses on the technological impact of using cloud-based systems. These are used less that DPIA but with the advent of the digital agenda these are likely to grow in number with more externally hosted solutions being consumed by the organisation.

Recommendations

34. That the Committee notes the contents of the report

Isabelle Bignall
Chief Digital Officer
13th November 2018

The following Appendix is attached:
Appendix 1: Nation Cyber Security Centre: 10 Steps to Cyber Security.
Appendix 2: Digital Strategy: Key Principles.
Appendix 3: ICT Governance Structure Diagram