COTSWOLD
DISTRICT COUNCIL

AUDIT COMMITTEEE **24TH JANUARY 2017**

AGENDA ITEM (12)

CYBER-SECURITY UPDATE REPORT

Accountable Member	Audit Committee
Accountable Officer	Tony Oladejo ICT Audit and Compliance Manager 01993 861194 tony.oladejo@2020partnership.uk

Purpose of Report	To present an overview of the current state of risks and considerations relating to cyber attacks
Recommendation(s)	**That the Audit Committee considers the report and makes comment on its content, as necessary**
Reason(s) for Recommendation(s)	To address concerns previously expressed by the Audit Committee relating to the Council's arrangements to prevent cyber attacks.

Ward(s) Affected	Not applicable
Key Decision	No
Recommendation to Council	No

Financial Implications	As detailed in the circulated report
Legal and Human Rights Implications	As detailed in the circulated report
Environmental and Sustainability Implications	Not applicable
Human Resource Implications	Not applicable
Key Risks	Loss of Council assets and personal and sensitive data, non-delivery of essential Council services
Equalities Analysis	No effect on protected groups identified

Related Decisions	None
Background Documents	Cyber-Security Update Report

Appendices	**Appendix 'A'** - Glossary of Terms

Performance Management Follow Up	Performance is monitored by the Group Manager - ICT, Change and Customer Services

Background Information

1. The threat of a cyber-attack has no longer become a case of if, but when it will happen. It is no longer safe to assume our firewalls and security systems will protect us all of the time.

2. In preparation for a Cyber Security incident, we need to follow a Prevent, Detect & Recover multi-layer strategy, with assurances sought for each stage. Our multi-layer strategy aligns with the Cabinet Office's UK National Cyber Security Strategy.

3. The partner Councils: West Oxfordshire District Council, Cotswold District Council, Cheltenham Borough Council and Forest of Dean District Council hold a vast amount of personal and sensitive information. This information is used to pay benefits, protect the vulnerable and assist in delivering essential services. All this information makes the partner Councils key targets for cybercriminals looking for opportunities to steal data, money and cause widespread disruption.

4. With our global economy becoming increasingly cyber dependent, it is critical that we understand the risks to our business. Escalating statistics surrounding cyber security show that the risk to organisations can be catastrophic, and that the response to security has been too fixated on technological aspects of security, as opposed to management, behavioural and cultural aspects:-

- 2.5 million cyber security incidents were reported in 2015;
- 38% increase in the number of security incidents detected in 2015;
- 56% increase in the theft of hard intellectual property;
- the average cost of breaches to business has nearly doubled since 2013;
- £75,000 - £311,000 - average cost of a cyber attack to a Small Medium Entities (SME);
- a 2015 UK Government survey found that 90% of large businesses across all sectors had experienced a malicious IT security breach over the past year;
- Within our IT network, there are approximately five intrusion attempts every 24 hours.

5. Recent Cyber Breaches

Over the last few years, and in recent weeks, cyber security issues have been brought to the world's attention, here are a few headline makers:-

- in November 2012, one of our partner Councils was subject to virus attack to its ICT network which resulted in a disruption to services including on-line Council Tax payments system for several days;
- there was a massive data breach at Yahoo, which resulted in the details of 500 million user accounts being leaked. However, this breach occurred in 2014;
- The World Anti-Doping Agency (Wada) has condemned Russian hackers for leaking confidential and sensitive medical files of star US and British Olympic athletes;
- on 1st November 2015, the New Zealand Nurses Organisation (NZNO) was targeted by a spear-phishing attack that resulted in the organisation disclosing the email addresses of tens of thousands of its members.

6. Impact on Reputation

When discussing the risks in general, one of the hardest areas to quantify is the impact on a company's reputation. The 2014 Information Security Breaches Survey estimated that reputational damage accounts for around 5%-20% of the cost of a cyber-security breach for large businesses. The value of a brand or goodwill can be seriously affected by a data breach, and this can be particularly costly for those companies who sell their products through e-commerce.

7. Cyber-Crime/Cyber-Fraud and Cyber Extortion

7.1 Cyber-Crime/Cyber-Fraud

7.1.1 Cyber-crime involves *'The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities, or other property'.* Cyber-crime is the most common and costly type of cyber-risk suffered by organisations. These types of attacks are highly likely to impact both on enterprise businesses and SMEs and, due to their impact, are high in severity to both parties.

7.1.2 One recent security breach involved Tesco Bank which froze all on-line transactions after fraudulent activity was discovered on 20,000 current accounts. The bank has 7.8 million customer accounts across the UK, of which 136,000 are current accounts.

7.2 Cyber Extortion

7.2.1 Cyber extortion is defined as *'The cost of expert handling for an extortion incident, combined with the amount of the ransom payment'.* It is the act of locking down a network and systems and requesting a ransom in order to release them. Commonly, *'ransomware'* is used to conduct this sort of an attack.

7.2.2 Ransomware is a form of malware that typically encrypts key data belonging to an organisation so that attackers can demand money in exchange for unlocking the data.

7.2.3 A recent and surprising case of cyber extortion was an attack on Lincolnshire City Council where cyber attackers used ransomware to lock staff out of key databases for the duration of a week.

8. Cyber Security and Information Security

8.1 'Cyber security' is a relatively recent term which has become more popular over the last five or six years and relates to security measures in place for information held digitally. This would include measures to protect the Council's network - application systems, databases, computers/devices on the network, and anything beyond the Council's network such as internet connections, mobile networks and Websites. The majority of the Council's Information Security standards relate to cyber security.

8.2 'Information Security' is an established term and relates to the security in place around 'all' the Council's information, irrespective of the manner in which it is stored. This can be held either in electronic or paper format.

8.3 The partner Councils have been working on Information Security since 2004 and have formal policies on Information Security in place. The Councils are now working towards a joint comprehensive Information Security Framework which will be based on ISO 27002, the international standard for Information Security Management.

9. Cyber Security Partners

9.1 The Cabinet Office National Security Secretariat provides coordination on security and intelligence issues of strategic importance across Government bodies. The Secretariat has recently issued the 'UK National Cyber Security Strategy'. The Strategy explains the Government's approach to tackling and managing cyber threats.

9.2 The key objectives are:-

- Defend - the defence against cyber threats, response to incidents and protection of systems;
- Deter- the detection, understanding, investigation and disruption of hostile cyber actions, leading to prosecution;
- Develop - the innovation, research and development of cyber expertise that will meet and overcome future threats.

9.3 The Councils have formally registered with the Zephyr Regional Cyber Crime Unit (RCCU). This provides a forum to receive and share up-to-date cyber threat information and the sharing of best practice.

9.4 ICT constantly reviews cyber security updates and guidance from the Government's National Cyber Security Centre (NCSC). Its remit is to provide support to public and private sector on how to avoid cyber threats.

9.5 As members of the Public Services Network (PSN), the partner Councils are now required to develop their own threat profiles to ensure continued compliance. This is a significant change in approach from PSN with regards to risk management, which will be reflected in our internal processes going forward.

10. Security Measures

10.1 Prevention

Security measures must be taken to protect information from unauthorised modification, destruction, or disclosure whether accidental or intentional. Security measures include a combination of legacy and next generation security, combined with user awareness training provides a prevention layer. Our Prevention measures currently include:-

(i) ICT Policies Framework - the Framework consist of a number of operational Security Policies. Our policies are split into 'User' for example, Password policies, and Internal Operational polices, such as authentication and patching procedures. The objective of these policies is to ensure the highest standards and good practices in ensuring information security is maintained at all times across the partner Councils:-

- all users of the Councils' Information Systems are assured of the confidentiality, integrity and availability of the information used and produced;
- business damage and interruption caused by security incidents are minimised;
- all legislative and regulatory requirements are met;
- the partner Councils' ICT equipment and facilities are used responsibly, securely and with integrity at all times.

(ii) Next Generation Firewalls - deep inspection of network traffic as it traverses the network combined with a live database of known threats on the Internet. These systems are managed centrally allowing a co-ordinated response across all Partner Councils. A threat detected at one firewall is blocked at all firewalls. Not only do we inspect internet traffic, we also inspect name resolution traffic, enabling us to remove suspected threats before our devices even attempt contact.

(iii) Structural Modification - inspecting links and data within documents/emails for malicious code attempting to redirect unsuspecting users. These links can be manipulated before onward delivery.

(iv) Traditional Anti-Virus and Device Lockdown - devices on our network run the latest software with updates installed continuously. Using multiple Anti-Virus engines from multiple vendors provides us additional protection.

(v) Micro segmentation - the ability to logically segment parts of our Server Infrastructure ensuring a single compromised host does not impact the rest of the Infrastructure.

(vi) User Awareness Training - a programme of training highlighting the risks. The key is to ensure management instils a culture that understands cyber risk, teaching staff and users to always question what they receive and whether to open files. The first line of defence is often employee education. Little can be done to prevent an employee's actions that are both deliberate and malicious. Pre-employment/background checks can help to screen out criminal infiltration, but sophisticated automated monitoring of the network (known as protective monitoring) is required to detect and stop malicious actions when they occur.

10.2 Detection

10.2.1 It is not enough to prevent the intrusions. It is important to detect the intrusions as soon as possible. Discovering that we have been compromised is not as bad as being told we were compromised six months earlier.

10.2.2 We currently deploy the following detection methods:-

- Next Generation Firewall tracking - the ability to detect where a file entered our network and which devices it was transmitted to;
- Logging - logging extended into user permissions, for example, if an Administrator user account is created or modified, senior managers in ICT are informed;
- Structural Analysis -implemented, and is partially configured - we have the ability to detect content within documents as they move across our IT infrastructure, for example; a file of bank account numbers can be detected leaving our network;
- We are planning on implementing in early 2017 Scan and Isolate capabilities. This system will constantly scan our IT infrastructure looking for systems that have been compromised and, upon detection, will isolate the offending system until remediation can take place. This will ensure our systems are protected 24/7.

10.3 Recovery

Given we accept it is likely at some point we will be compromised, it is vital to ensure we can recover. Our recovery procedures include the following:-

- Snapshots, Replication and Backups - a full plethora of backup solutions are employed to ensure multiple copies of all our systems are kept and replicated to remote sites;
- Disaster Recovery Plan - we have a Disaster Recovery program in place that will allow us to survive an incident or disaster and to re-establish our normal business operations quickly and efficiently. Our ICT team undertakes rolling Disaster Recovery testing throughout the year. To date, all our Disaster Recovery objectives have been successfully tested, and an appropriate action plan is in place to resolve any issues identified;
- Business Continuity - we have business continuity procedures in place, both at Corporate and services levels. Business continuity plans are maintained and updated throughout the year. Each plan contains the critical information on how the business needs to stay running in spite of adverse events. We identify and prioritise which systems and processes that must be sustained and provide the necessary information for maintaining them.

10.4 Assurance and Compliance

We are subjected to various external compliance requirements in terms of our Cyber and Information security standards.

10.5 Public Services Network Compliance

10.5.1 PSN provides an assured "network of networks" over which the Government can safely share services. The PSN is managed within the Cabinet Office, and a PSN Programme has been designed to oversee and implement elements of the UK Government ICT Strategy.

10.5.2 We must comply with the new PSN connection controls. IT Health Checks are conducted annually for the purpose of ensuring PSN compliance and comprise both external and internal vulnerability tests. The IT Health Check tests must be undertaken by a Government-certified organisation using Government-certified testers. The outcome of the IT Health Check was positive and demonstrated that the Council's cyber security systems were safe and robust.

10.5.3 The external vulnerability test involves the tester attempting to break or hack into the Council's network and all its externally facing systems, including the Council's Website. The internal vulnerability test involves the tester assessing 10 -15% of the Council's servers and a representative sample of PCs, laptops, etc. They run automated checks of their configurations and also attempt to gain access to systems as an unauthorised user.

11. Penetration Testing

We undertake our own independent vulnerability management program. Our penetration testing searches for security vulnerabilities on our systems, network or application. The idea is to locate the weaknesses and eliminate them before an attacker exploits them.

12. Payment Card Industry Data Security Standard

12.1 The Partner Councils take debit and credit card payments and therefore are also required to be compliant with the Payment Card Industry Data Security Standard (PCI DSS). A failure to comply with this standard can result in considerable financial penalties in the event of a disclosure of card details.

12.2 External and internal vulnerability tests of the network are conducted every quarter for compliance with the PCI DSS. The external test must be conducted by PCI-qualified testers and the internal test is conducted by ICT staff using an approved testing tool. The Partner Councils must pass the tests to achieve compliance.

12.3 To date, no compliance issues have been identified.

13. Data Protection Requirements

13.1 As a controller and processor of personal information, each Partner Council must comply with the requirements of the Data Protection Act 1998. The UK Information Commissioner's Office (ICO) issues regular security guidance to ensure that organisations comply with the 7th Data Protection Principle. This requires that '*appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data*'.

13.2 The Information Commissioner has the power to serve a fixed monetary penalty notice of up to £500,000 on an organisation for a significant breach of the Data Protection Act. The majority of monetary penalties issued to other bodies to date have been for breaches of the 7th Principle and have each exceeded £100,000.

13.3 To date, no data protection breaches has been reported.

14. Risk Assessments

14.1 We undertake risk assessments, this involves identifying the various information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data, intellectual property, etc.), followed by identifying the various risks that could affect those assets.

14.2 A risk estimation and evaluation is usually performed, followed by the selection of controls necessary to treat the identified risks. The threat profile and risk assessment will be reviewed periodically as necessary.

14.3 There are a number of processes and controls to mitigate cyber risks:-

- identify key assets at risk and address weaknesses, such as a lack of user education or reliance on third parties;
- create a cyber security aware culture and ensure that this is enforced from the top down;
- implement network access, communications and password policies;
- manage and control user privileges;
- implement monitoring across networks and systems to ensure there are set policies and procedures around these areas;
- ensure proper back-up and data recovery are in place;
- make decisions around which risks to avoid, accept, control or transfer.

15. Conclusion

15.1 We have an assured, secure, Government-accredited network, which is subject to on-going and evolving cyber-attacks which, to date have been successfully rebuffed. The network must continuously evolve with the threats in order to remain secure. It is not possible to secure anything completely, so detection can be as important as prevention.

15.2 A glossary is attached at **Appendix 'A'**.

(END)