Sandwell
Metropolitan Borough Council

Agenda Item 13

REPORT TO
AUDIT AND RISK ASSURANCE COMMITTEE

08 November 2018

Subject:	Cyber Security Strategic Risk Update
Director:	Executive Director – Resources
Contribution towards Vision 2030:	
Contact Officer(s):	Sue Knowles Head of ICT & Revenues and Benefits sue_knowles@sandwell.gov.uk Andy Saunders ICT Service Manager Andy_saunders@sandwell.gov.uk

DECISION RECOMMENDATIONS
That Audit and Risk Assurance Committee: 1. Review and comment upon the report.

1 PURPOSE OF THE REPORT

1.1 To update members of the Committee on the council's strategic risk related to cyber and information security.

2 IMPLICATIONS FOR SANDWELL'S VISION

2.1 Effective risk management is a key element of good corporate governance and is essential to the overall performance of the council in meeting its 2030 Vision.

2.2 Good risk management will ensure that resources are used efficiently and effectively in the delivery of the Sandwell 2030 Vision and that assets and resources are protected against risk in the most efficient way. Cyber and information security is essential to ensure the protection of sensitive personal information used across all service areas.

3 BACKGROUND AND MAIN CONSIDERATIONS

3.1 As cyber-attacks are increasing across public and private sector organisations worldwide, there is a growing risk that they will become overwhelmed by the number of threats they have to address. The consequences of a successful attack on the Council could be severe, such as the leaking of sensitive personal information or leaving high-profile individuals and departments open to being blackmailed.

3.2 It is important to understand what is meant by the term "Cyber Security". A well-defined explanation provided by the UK National Cyber Security Centre (NCSC) is:

"The protection of internet connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so".

3.3 A perhaps more meaningful definition is provided in the recently published National Audit Office good practice:

"The activity required to protect an organisation's computers, networks, software and data from unintended or unauthorised access, change or destruction via the internet or other communications systems or technologies. Effective cyber security relies on people and management processes as well as technical controls".

3.4 Cyber security is part of the wider activity of information security. Information security is a broad term that encompasses electronic, physical and behavioural threats to an organisation's systems and data, covering people and processes. Data can of course be stored both electronically and physically (e.g. on paper).

3.5 Both definitions equally demonstrate that effective cyber and information security is not just about having the right technology but also having the right people and processes in place. Effective management is not just the responsibility of the ICT Service. It requires much wider corporate governance.

3.6 Sandwell is dependent on a range of computer and information systems necessary to fulfil its service objectives and realise its 2030 Vision. A compromise to any one of these systems would have a significant impact upon the services it delivers and, as stated in the above definitions, lead to further reputational loss or financial sanction by regulatory authorities. Breaches can also lead to the need to pay financial compensation to affected individuals.

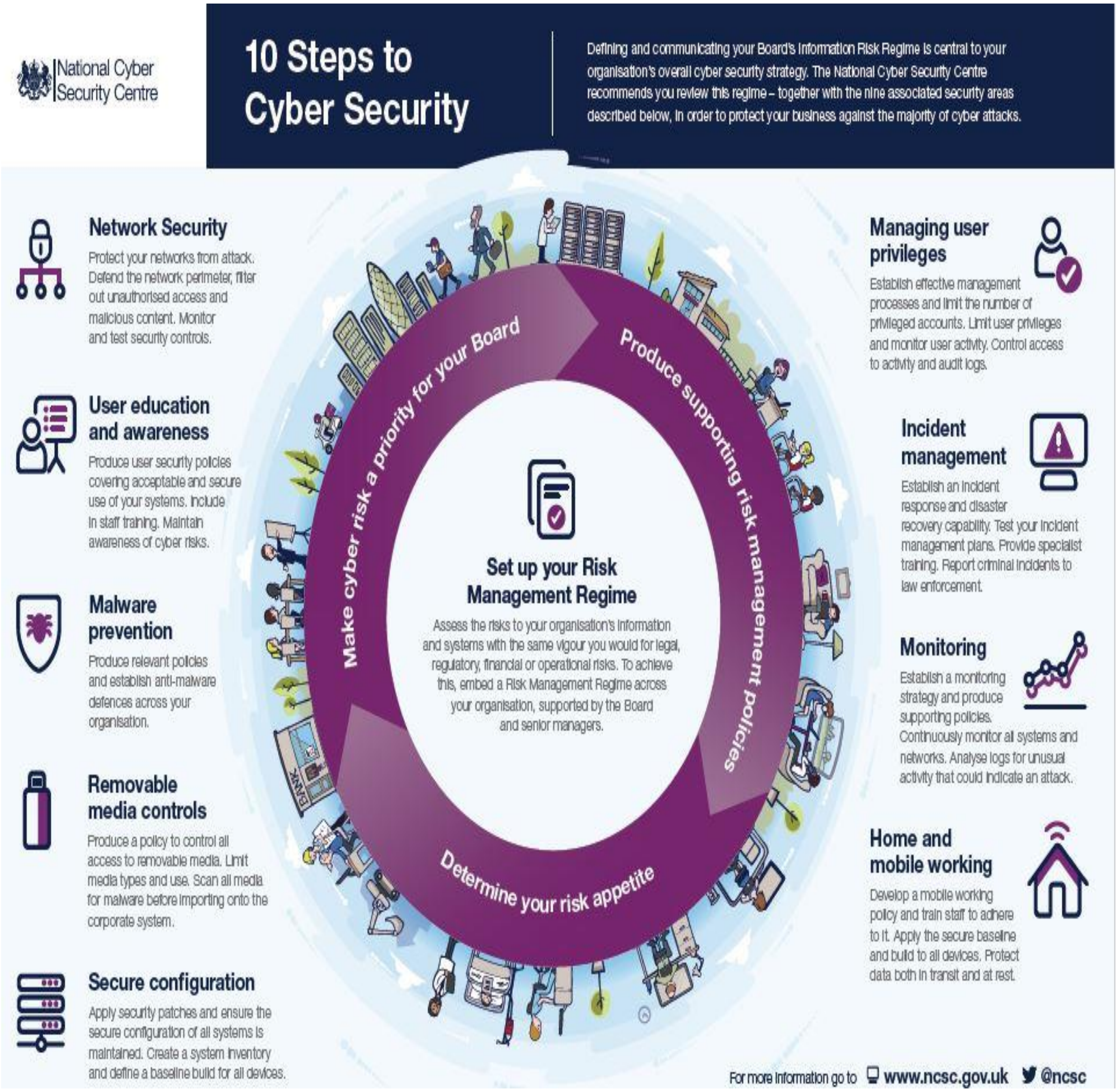
3.7 Formal certification programmes such as Cyber Essentials Plus can assist organisations in ensuring there are adequate and effective controls within their Cyber Security infrastructure and processes.

3.8 The National Audit Office has produced a good practice guide for Audit Committees advising them of the issues that should be considered around this topic. This is included as an appendix to this report. The guide states that public bodies must have confidence in the confidentiality, integrity and availability of their data. Any personal data collected, stored and processed by public bodies are also subject to specific legal and regulatory requirements such as the General Data Protection Regulations. The guide has been attached as an appendix to this report.

3.9 The guide is structured around a set of 10 high level questions as outlined below. These are referred to as the "10 steps to cybersecurity" which have been identified by the NCSC as the baseline which organisations should meet in order to demonstrate a good level of security.

For each of these we have carried out an assessment of the Council's current position and identified key remedial actions.

This provides, in simple terms, 10 areas to focus on in order to achieve effective cyber security and information security protection. The diagram below outlines the high-level structure of the 10 steps.



National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Set up your Risk Management Regime
Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Make cyber risk a priority for your Board

Produce supporting risk management policies

Determine your risk appetite

Managing user privileges
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

4 THE CURRENT POSITION

4.1 It should be noted that due to the sensitive nature of this subject, some of the information presented in this report is high level to eliminate any possibility of weaknesses being exploited.

Good practice guide - high level areas to monitor

Question	Sandwell's Current Position
Has the organisation implemented a formal regime or structured approach to Cyber Security which guides its activities and expenditure	We have a suite of organisational policies and procedures which outline to employees of the council the appropriate ways of managing information and computer systems. Formal certification of cyber security controls is being addressed by the adoption of Cyber Essentials Plus and the adherence to the "Ten Steps to Cyber Security" which is a recognised national standard for managing Cyber Security as produced by the National Cyber Security Centre.
How has management decided what risk it will tolerate and how does it manage that risk	Cyber security is managed by the ICT Service and monitored by its Management Board reporting to the Head of ICT & Revenues and Benefits. The Head of ICT & Revenues and Benefits in turn reports to the Executive Director of Resources who updates Management Board and Elected Members. Cyber Security is included in the corporate risk register. Risk is managed and monitored by the Audit and Risk Assurance Committee.
Has the organisation identified and deployed the capability it needs in this area	The Council has an Information Management Unit within the Resources Directorate and has a dedicated Cyber and Information Security Lead within the ICT Service. This lead officer is provided with the skills and awareness to manage the cyber threat and ensure that necessary processes and technologies are in place to respond to a threat.

	Policies exist, corporately, to manage workforce behaviour related to cyber and information security risk. The procurement of an e-learning software tool is underway. This will allow us to roll out training to all staff quickly, timely and effectively. It will be used to provide regular awareness and updates on good practice. The tool also includes “testing” to ensure adequate knowledge is embedded in our workforce.

Good practice guide - more detailed areas to explore

Information Risk Management Regime	Robust governance is provided via Corporate policies. Our Cyber Security Lead has close links with other local authorities across the West Midlands and Black Country, National Cyber Security Centre and the Central Information Sharing Partnership.
Secure Configuration	It is essential that the ICT Service manages the network and computing infrastructure with security that is intrinsic from the start of any technology project. Patching and updates to systems is an ongoing activity of work due to the high volume and frequency of these being issued by our technology vendors.
Network Security	The Council has strong and robust network perimeter security (firewalls etc) which has been updated recently using industry standard technology. We test this independently every year by using an accredited security / penetration testing company. Any gaps identified are collated into a Remedial Action Plan and managed through to completion. Our last test was undertaken in August 2018.

Managing User Privileges	Users can be an area of weakness with security compliance. With over 4,500 end user accounts this is a significant challenge to manage. Administrator accounts are minimised and password controls implemented to ensure accounts cannot be easily compromised. We are working with HR to review and improve processes when a member of staff moves within the Council or leaves. It is essential that accounts are shut down promptly and new accounts, with the right access privileges set up promptly.
User Education and Awareness	Policies related to information security are approved and available to the workforce. These are due to be reviewed and updated. A new e-learning tool (as noted above) is being procured. In addition, there will be training for Elected members via Members Development plan.
Incident Management	Cyber security incidents are managed by the ICT Service Desk and responded to accordingly. A specific Cyber Incident Response Plan is currently being developed in conjunction with the Council's Resilience Unit.
Malware Protection	Technology is built into our infrastructure to ensure malware and antivirus is scanned for and trapped before it propagates across our systems and network.
Monitoring	Our perimeter network systems can monitor attempted attacks which emanate from across the world. We are looking at how we can best use this massive quantity of data to ensure we are able to respond to threats before they become real. Systems create vast quantities of logs detailing all activities on systems. In

	the event of an incident, these could be used to create evidence.
Removable Media Controls	By default, we do not allow removable media e.g. USB memory sticks as they are inherently prone to security risks. Where there is a robust business case for use, access is permitted but only to a standard encrypted device. CDs and DVDs are now less commonly used but any computing devices which already have them will be locked down to prevent loss of data or infiltration of malware (this is any software intentionally designed to cause harm or damage to a computer, server or network which once implanted or introduced is then known as computer viruses).
Home and Mobile Working	As we work more digitally, agile working will increase and become the norm. Anyone using Citrix services can be assured of adequate security protection and mobile users such as Windows 10 can only connect to our network and information systems by approved secure connections. We are also able to manage other mobile devices such as ‘phones remotely to allow appropriate access to emails and other services such as Microsoft Office 365 (email, file storage etc)

4.1 Strategic risk – 42a – Cyber security is presently rated as amber as a result of the control measures noted above. It is anticipated that the risk will always be present on our register given the global profile of and new developments in cyber security – however through robust management we will continue to manage this risk at a level which is tolerable without imposing overly restrictive working practices or significant financial burden on the council. Where gaps in controls are identified the appropriate investment required to manage the risk to an acceptable level will be necessary.

4.2 The ICT Service recognises the opportunity for collaboration with its wider West Midlands Combined Authority and West Midlands authority partners.

While there has been no formal joined up strategy agreed across the region for Cyber Security presently, all ICT Managers across the region take this seriously.

During the monthly calls that take place, there is an agenda item where Cyber is discussed and knowledge sharing, collaboration, together with life experiences and advice is given.

In addition, each council does undertake a similar approach by adopting the same national security guidance, adopting the GDPR principles and having nominated individuals in their structures responsible for security.

Until there is an appetite from our WMCA partnering organisations to look at a combined strategy, we will continue to discuss at our monthly meetings together with collaboration and sharing of advice.

We have also recently started dialogue with our neighbouring Black Country partners to initiate a proactive Cyber Security working group with all Local Authority leads to see if there is an appetite to develop a combined Black Country strategy.

4.3 In addition, there is a plethora of other external advice and guidance available from key ICT vendors such as Microsoft, Oracle and our security technology partners. All offer useful intelligence and guidance which we use to ensure our defences are robust and secure.

4.4 Cyber security is relevant to the entire council including, not just its workforce, but Elected Members too. For Members, cyber security is being addressed via the Member development programme aligning it to the need to comply with the GDPR.

5 CONSULTATION (CUSTOMERS AND OTHER STAKEHOLDERS)

5.1 No specific consultation has been necessary for this report as no decision is required.

6 ALTERNATIVE OPTIONS

6.1 This report does not require a decision and therefore, alternative options do not need to be considered.

7 STRATEGIC RESOURCE IMPLICATIONS

Cyber Security is currently funded from within the ICT Service’s budget. Requirements for specific investments and improvements are subject to separate individual bids as required.

8 LEGAL AND GOVERNANCE CONSIDERATIONS

8.1 Compliance with the General Data Protection Regulation is mandatory for all organisations processing personal data. Cyber and information security is an essential component in ensuring compliance with GDPR and specifically the principle of ensuring information is “kept safe and secure”.

9 EQUALITY IMPACT ASSESSMENT

9.1 As a decision is not being sought in this report, it is not necessary to undertake an Equality Impact Assessment.

10 DATA PROTECTION IMPACT ASSESSMENT

10.1 As a decision is not being sought in this report, it is not necessary to undertake a Data Protection Impact Assessment.

11 CRIME AND DISORDER AND RISK ASSESSMENT

11.1 There are no crime and disorder risks arising from this report.

12 SUSTAINABILITY OF PROPOSALS

12.1 There are no direct sustainability issues arising from this report.

13 HEALTH AND WELLBEING IMPLICATIONS

13.1 There are no direct health and wellbeing implications from this report.

14 IMPACT ON ANY COUNCIL MANAGED PROPERTY OR LAND

14.1 There is no direct impact on any council managed property or land from this report.

15 CONCLUSIONS AND SUMMARY OF REASONS FOR THE RECOMMENDATIONS

15.1 The purpose of the report is to update the Audit and Risk Assurance Committee with regards to Cyber and Information security.

16 BACKGROUND PAPERS

16.1 National Audit Office Good practice guide – Cyber and information security.

APPENDICES:

National Audit Office Cyber security and information risk guidance for Audit Committees

Darren Carter
Executive Director – Resources and s151 Officer