Appendix 2

South Lakeland District Council Cyber Security Update

Author: Ben Wright, Head of Shared ICT and Lead Digital Specialist

Date: 5th July 2019

This paper is intended to complement the audit updates included in this overall report.

Introduction

1. Firstly I want to confirm that we in the Shared ICT service and staff around the council, take Cyber Security very seriously indeed. It is a rapidly changing environment, fortunately the controls we have in place and have had in place for many years, are robust and can adapt to the changing world of Cyber Security.

2. As well as the Cyber Security Audit reported on in this report, South Lakeland and other councils in the country, took part in a Cyber Security Stocktake. This was a simple questionnaire really focusing on the governance of Cyber Security rather than the deep technical solution.

3. The outcome of the stocktake highlighted some gaps, however these gaps were in line with the gaps highlighted in the Audit and as such we are dealing with both by doing the same work and we are tracking that work in this audit report.

Update

1. It should be noted that we achieved reasonable assurance in the audit and it was acknowledged that our technical controls are very good. This is backed up by the fact that each year we are subjected to a rigorous IT Security Health Check. This Health Check is performed by highlight skilled IT security professionals that put our defences through their paces. They do this to highlight to us any weaknesses that could be improved and provide guidance as to how that can be achieved. This process does not end there, in order to pass the annual Health Check, the issues are monitored and only when we have resolved to an acceptable level does South Lakeland receive confirmation that it's network is Public Sector Network approved.

2. In addition to the annual health check described above, we perform quarterly security scanning of devices connected to our network, this scanning allows us to keep up to date with any known security issues and resolve as the arise, doing this makes the annual check more effective

because we can focus on the really hard to find things rather than the simple things that are fixed as a matter of course.

3. The work required as part of the audit recommendations and the cyber security stocktake is about joining up the technical controls and the wider governance of Information and cyber security. We work closely with Information Governance colleagues and together we continually improve the frameworks, policies and procedures we have in place.

4. A key requirement on the ICT Service is to improve the level of documentation we have, this will confirm that we are operating in line with the corporate requirements and ensure that everyone knows what we do and why.

5. We also work closely with colleagues involved in Disaster Recovery and Business Continuity planning, a key focus over the next few months is to create a Cyber Incident response plan and do some testing of that plan to confirm how it would operate for real.

6. To help us achieve what we need to do, we have a member of staff within the Shared ICT Service who is developing the documentation and procedures that we need, we are not starting from scratch putting systems in place, more documenting what we already do so that it can be reviewed more readily, we can also use it to ensure any new staff within the team are fully aware of what is in place and what is required.

7. As this process develops, I see it as an every improving situation whereby we review and incrementally improve as technology and knowledge in this area develops.

8. Below, you will find information on the security controls we have in place to protect the council IT infrastructure.

I hope this paper and the information below goes some way to help assure the Audit Committee and others that South Lakeland DC is taking the threat of Cyber Attack very seriously indeed and we are taking the necessary steps to continually improve the work we do to keep the data and systems the council operates secure.

Without giving away any restricted information away, below is a list of the protective controls we have in place to protect the council from Cyber Attacks, viruses and malware.

- Scanning of all e-mails for viruses/malware/spam inbound to the council from external sources. This scanning/filtering takes place in two places
    - In the cloud, prior to the e-mails being received by the council
    - After receipt by the council using a different scanning engine

- Scanning of all e-mails for viruses/malware/spam outbound from the council to external destinations. This scanning/filtering takes place in two places
    - Before sending by the council
    - In the cloud, prior to the e-mails being sent to the recipient

- E-Mails configured to be encrypted during transmission, this also provides protection to limit e-mails being received where the source of the e-mail has been tampered with.

- Antivirus/malware protection software installed on all Servers, computers, laptops, phones and tablet devices.

- Central Firewall configured to project the council network from the internet in the following ways:

    - Data passing through the firewall from the corporate network to the internet is scanned for viruses/malware
    - Prohibited websites are blocked with no access provided from corporate devices, this list of sites is managed by the firewall manufacturer who are a global organisation and are seen as market leaders in Unified Threat Management. The list of blocked sites is updated automatically on a regular basis
    - Firewall detects and protects against unknown attacks using dynamic analysis and provides automated mitigation to stop such attacks the logic used is updated regularly by the firewall supplier who are seen as market leaders in Unified Threat Management.
    - No direct access to the council network from any external networks, all traffic inbound from external networks is filtered by components installed in cordoned off networks known as a Demilitarized Zone, these areas are designed to protect the corporate network from external attack

- Corporate Network Password controls are configured as standard as follows:
    - Passwords configured to require changing every 42 days
    - Not permitted to use any password from the previous 20 passwords
    - Accounts set to lock out after a defined number of invalid attempts

- Annual IT Health Check performed by 'Check' accredited and approved individuals
    - This is where ethical hacking takes place on our network and any gaps in the configuration are highlighted and resolved by implementing coordinated changes described and documented in a remediation plan

- The Annual check is complemented by the following:
    - Quarterly security scanning of devices on the network for all known vulnerabilities
    - Comprehensive patch management of desktops and servers where software is updated regularly

- Phones and Tablets
    - Only corporate devices used to access the corporate network and data
    - All devices protected by Antivirus and Malware protection
    - All devices encrypted
    - Devices automatically wipe after a defined number of incorrect password attempts
    - Password requirements enforced to be as strong as those defined on the corporate network
    - Connectivity from phones/tablets to the corporate network is via the corporate firewall so all data is scanned in transit
    - Data from the devices destined to the internet rather than internal corporate network is scanned by a separate product
    - Apps installed on corporate phones/tablets are subjected to analysis which highlights potential risks. Any apps highlighted above a configured risk rating are automatically blocked

- Remote VPN Connectivity
    - Remote connectivity from Laptops is provided to staff, part of the configuration is the checking for Security Certificates installed onto corporate devices, without these certificates connection to the corporate network is not permitted even if a username and password is known.

- Staff educated not to connect non-corporate devices to corporate equipment