Preston City Council

“Cyber Security”

Report by the Task and Finish Group

January 2018 – March 2018

Contents Page

Appendices

Web links / Background Documents:

Presentation – Cyber Security

Cyber Crime and Cyber Security Chart

Preston Cyber Security Audit Report

Preston Cyber Security Policy

Preston Cyber Security Risk Register

Minutes of Meetings:

31 January 2018

Chair’s Foreword and Acknowledgements

This topic was a priority for Members following the security breach at the NHS in 2017. Members identified the need to scrutinize the Council’s cyber security, looking at the comparable level of risk, the measures we have in place to prevent a similar breach, and what are we doing to keep one step ahead of potential attacks. In this regard I feel we have succeeded in our task.

I feel the Task and Finish Group learned a great deal from this study and as Chair I was very impressed with the excellent level of security despite the Council’s budgetary constraints.

I would like to thank all members of the Task and Finish Group and officers who contributed to this study.

Councillor Lynne Wallace

The members who contributed to this study were:

Councillor Wallace

Councillor Desai

Councillor Mrs Abram

Councillor Borrow

Councillor N Cartwright

Councillor Mullen

Councillor Rollo

Councillor Saksena

Councillor Mrs S Whittam

Recommendations to Cabinet

1. That the Corporate Governance Group conducts a feasibility study into the prohibition of all personal removable media devices and allow only approved encrypted removable media devices;
2. Subsequent to (1), approve any policy amendments required following the outcome of the study at (1);
3. Ensure mandatory cyber security training for all staff and councillors via Mipod, including 1-2-1 training, tailored to individual requirements and devices (e.g. visual differences on IPads).
4. Support the introduction of self-service password changes;
5. To improve corporate cyber security, ask CMT to introduce a management checklist covering a range of measures (e.g. prompts, reminders, vigilance, visual checks, a clear desk policy regarding password security), including homeworkers.
6. To approve the renewal of a 12 month contract for the spoof phishing email service, subject to budgetary implications.
7. That the Cyber Security policy be updated as appropriate to reflect the increased security measures.

1.1. **Background / Aims of this study**

This scrutiny topic arose from Members' concerns regarding the security breach at the NHS in 2017; what is the comparable level of risk, what measures PCC have in place to prevent a similar breach, and what are we doing to keep one step ahead of potential attacks.

Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

New trends in cybercrime are emerging all the time, with estimated costs to the global economy running to billions of pounds.

The risk of a cybersecurity breach is extremely high for all organisations. Preston City Council take all cyber threats seriously and have a range of hardware and software controls in place to minimise risk and protect data. We are also endeavouring to raise cyber security awareness amongst our user base with tests and training in an effort to help stop security incidents.

1.2 **Scope of the Study**

The Task and Finish Group wanted to gather detailed evidence from PCC ICT Services, in the form of relevant information (e.g. Council policies, ICT audit, and Government guidance) and an interview with the Head of ICT Services.

1.3 **Presentation and Interview with the Head of ICT Services – 31.1.18**

Sharon Thornton, Head of ICT Services gave a presentation on Cyber Security, assisted by Andy Heywood, Deputy Head of ICT Services / ICT Infrastructure Team Leader.

She outlined the potential threats to the Council's cyber security such as malware, ransomware, data breach/theft, denial of service attacks and phishing. She explained that it was not possible achieve 100% protection; the Council can do as much as possible to protect itself and mitigate risk to an acceptable degree. You can never remove all risk.

She referred to the NHS cyber security attack 'Wannacry' in 2017. At the time of the breach, the service was still running the unsupported operating system Microsoft Windows XP. The Council moved away from XP before its unsupported date and is currently running Windows 7.

Ms Thornton gave details of the level of protection and infrastructure security measures in place at Preston City Council, as follows:

- Firewalls with Denial of Service and Vulnerability Protection

- Next Generation Advanced Threat Protection

- Effective Password Management

- Effective Patch Management

- Pro-active network monitoring

- Dashboard Log management system

- Mobile Device Management Software

- Secure remote working gateway

- Strict Access Control - meaning that staff only had access to the software they require to perform their jobs

- Regular (weekly) network scans and annual PSN health check (next one due in March)

- Backups and DR site

She referred to a recent IT audit (carried out by Salford Internal Audit Services) in which Preston City Council were awarded a 'Satisfactory' Level of Assurance (i.e. one level below the maximum score). She highlighted the Action Plan arising from the Audit, which included actions relating to the risk register, log alerts, and denial of service attacks (which had now been completed). The only outstanding actions related to personal USB pen drives, which was to specify that only ‘official encrypted USB pen drives’ were to be used and ‘USB ports to be configured to only allow these devices’, and self-serve password resets. These actions had been agreed by the Corporate Governance Group and a timescale set to investigate suitable options for the Council (30.4.2018 and 30.6.18 respectively).

Ms Thornton explained that currently removable media are allowed for presentations etc. at meetings but are immediately scanned for malware. They do not connect to the network. The high residual risk cited in the Risk Register reflects the danger of potential loss or theft of data (i.e. if not encrypted). If the action agreed for investigation were to be implemented, this would require an amendment to the existing cyber security policy.

Ms Thornton informed members of a spoof ‘phishing’ email service commissioned over the last year to test fraud and security awareness at the Council. She receives a monthly report regarding who has undertaken subsequent training etc. Mr Heywood explained that, globally, hundreds of organisations would often be targeted by a single phishing source. The source would be identified and blocked within 24 hours. The Task and Finish Group expressed concern about phishing. It was suggested that a message or banner be placed at the footer of Council emails (e.g. with PCC logo etc.) to remind employees and councillors about the danger of phishing to raise awareness.

The Task and Finish Group discussed 'social engineering' – i.e. fraud where someone poses as the account holder to get a password changed. If a member of staff needs to change their password, they are unable to use their headsets and so a call is logged by a colleague, usually in the same office so it can be verified as genuine. Currently guidance from the Cabinet Office stipulates that passwords should be changed every 90 days. However, Mr Heywood indicated that a 16 character or more password (e.g. a phrase) is the most secure. It is hoped that the position will be updated soon.

Other issues discussed included the Council's Mobile Device Management software 'Airwatch' which enables ICT to lockdown IPad and smart phones, and remote wipe in case of loss or theft. One member suggested an amendment to the policy – page 26 paragraph 5.5 – to include a reminder that the Windows Key and 'L' will lock a desktop PC.

Regarding the forthcoming General Data Protection Regulation (GDPR), Ms Thornton indicated that she was liaising with Caron Parmenter and Trish Ashcroft regarding new procedures.

Councillor Mullen highlighted the danger of third party apps (e.g. ones used on social media such as Facebook) having the ability to harvest personal data. He requested that this information could be included in the policy to raise awareness for employees.

The Chair thanked the attendees for the presentation and interview. She summarised the key issues which recommendations could be made, i.e.

- External Audit Action Plan - action regarding removable media devices and change of policy

- Threat posed by phishing emails – mandatory training for staff and councillors via Mipod (NB: take into account slight differences on IPads)

- Password changes – self-service / automated

- Ask CMT / Cabinet to look at the value of renewing the contract for the spoof phishing email service

- Corporate security – monitoring by middle managers of security risks such as having passwords on employees' desks

Members requested that the Head of ICT Services email any other additional information relevant to the study such as the link to Cabinet Office guidance, information supplied to the auditor, phishing report details etc.

3.2 Additional Information provided after the meeting

Further to the Cyber Security Task and Finish Group on 31st Jan, additional information provided by Sharon Thornton was as follows:

Phishing Test Report

The statistics in respect of the phishing test are:

When we did the baseline test (i.e. everyone in the Council received the same scam email) 49% of the user base failed by clicking the link within the email. During Month 1 – the figure had dropped to 8% and the Month 10 report shows that 5% of the user base is ‘phish prone’.

Evidential Documents

The Task and Finish Group were provided with copy of documents evidence requested by and provided to Jim Kilburn, Principal Computer Auditor, Internal Audit Services, Salford City Council, which were:

- News Alerts to staff reporting results of phishing tests and reminders to attend training
- Screenshot of 45 minute Infosec security video training
- Logged New User Call and New User Form
- Mipod Cyber Security Modules
- Screenshot of relevant policies available on Cityspace

Ms Thornton also provided the PSN Health Check report (containing confidential and restricted information) from last year.

Another report is due in March this year.

Website for information on the Public Services Network (PSN)
https://www.gov.uk/government/groups/public-services-network

Website for CESG National Cyber Security Centre - https://www.ncsc.gov.uk/

3.0 Corporate Management Team Commentary

This study demonstrates that the Council are taking the issue of cyber-security very seriously. The phishing test in particular shows that measures which are being put in place are having a positive effect on protecting the Council from cyber threats and improving awareness and responses by staff and Members. But we cannot be complacent, and the recommendations in this study, when actioned, will put the Council in an even stronger position. The study group should be congratulated for a focussed study which makes clear recommendations.

Appendix A

SCRUTINY WORK PLAN STUDY TOPICS SCOPING 2017/18

Cyber Security

Key background information

Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

New trends in cybercrime are emerging all the time, with estimated costs to the global economy running to billions of pounds.

The risk of a cybersecurity breach is extremely high for all organisations. Preston City Council take all Cyber threats seriously and have a range of hardware and software controls in place to minimise risk and protect data. We are also endeavouring to raise cyber security awareness amongst our user base with tests and training in an effort to help stop security incidents.

This scrutiny topic arose from Members’ concerns regarding the security breach at the NHS in 2017; what is the comparable level of risk, what measures PCC are place to prevent a similar breach, and what are we doing to keep one step ahead of potential attacks.

Key people to hear from

ICT Staff

External Visit

N/A

Lead Officer

S. Thornton, Head of ICT Services

Panel size

9 (5, 3, 1)

Time estimate

2 meetings

Resources

ICT Staff

Target Audience

Members and Officers

Management Team comment

CMT support this piece of work

Response by the Cabinet

Minute CA111 – 18.4.18

Summary

Councillor Mrs Wallace, Chair of the Cyber Security Task and Fish Group attended the meeting and presented the Work Plan Study report. She outlined the scope of the study, investigations and interviews undertaken and the recommendations made by the Task and Finish Group. Councillor Mrs Wallace thanked the Members and Officers involved in the Study. Cabinet endorsed the recommendations and acknowledged the efforts of the Councillor Mrs Wallace and the work of the Cyber Security Task and Finish Group.

Decision Taken

That Cabinet

i) Endorsed the report by the Cyber Security Task and Finish Group; and

ii) Endorsed the recommendations detailed within the report.