Performance, Finance and Customer Focus Overview and Scrutiny Committee

Date of meeting:	22 February 2023
Title of Report:	**Cyber Attack Briefing**
Lead Member:	Councillor Mark Shayer (Deputy Leader)
Lead Strategic Director:	Andy Ralphs (Strategic Director of Customer and Corporate Services)
Author:	John Finch
Contact Email:	John.Finch@Plymouth.gov.uk
Your Reference:	None
Key Decision:	No
Confidentiality:	Part I - Official

Purpose of Report
To brief the Council on the resilience to a cyber attack

Recommendations and Reasons
To note the update.

Alternative options considered and rejected
None

Relevance to the Corporate Plan and/or the Plymouth Plan
Delivery of the plan is dependent upon accessing IT services

Implications for the Medium Term Financial Plan and Resource Implications:
None

Financial Risks

Dependent upon nature of any attack

Carbon Footprint (Environmental) Implications:
None

Other Implications: e.g. Health and Safety, Risk Management, Child Poverty:

* *When considering these proposals members have a responsibility to ensure they give due regard to the Council's duty to equality of opportunity, eliminate unlawful discrimination and promote good relations between people who share protected characteristics under the Equalities Act and those who do not.* Click here to enter text.

Appendices

**Add rows as required to box below*

Ref.	Title of Appendix	**Exemption Paragraph Number** (if applicable) *If some/all of the information is confidential, you must indicate why it is not for publication by virtue of Part 1of Schedule 12A of the Local Government Act 1972 by ticking the relevant box.*						
		1	**2**	**3**	**4**	**5**	**6**	**7**
A	Briefing report title							
B	Equalities Impact Assessment (if applicable)							

Background papers:

**Add rows as required to box below*

Please list all unpublished, background papers relevant to the decision in the table below. Background papers are <u>unpublished</u> works, relied on to a material extent in preparing the report, which disclose facts or matters on which the report or an important part of the work is based.

Title of any background paper(s)	**Exemption Paragraph Number** (if applicable) *If some/all of the information is confidential, you must indicate why it is not for publication by virtue of Part 1of Schedule 12A of the Local Government Act 1972 by ticking the relevant box.*						
	1	**2**	**3**	**4**	**5**	**6**	**7**

Sign off:

Fin	DJN.22.23.378	Leg	EJ/1114/14.2.23(1)	Mon Off	Click here to enter text.	HR	Click here to enter text.	Assets	Click here to enter text.	Strat Proc	Click here to enter text.
Originating Senior Leadership Team member: Andy Ralphs											
Please confirm the Strategic Director(s) has agreed the report? Yes Date agreed: 17/01/2023											
Cabinet Member approval: *'approved verbally by Councillor Shayer* Date approved: 17/02/2023											

CYBER ATTACK RISK

Performance, Finance and Customer Focus Overview and Scrutiny Committee report

Introduction

The threat from Cyber-attacks is rising within the public sector, with a major focus within central government and the LGA to ensure that Local Authorities reduce their exposure to a cyber-attack, and also have the appropriate business continuity processes in place to reduce the impact if affected by a cyber-attack.

This document sets out the different scenarios that may be faced, and the impact on the Council, which are summarised in the table in Appendix A.

Scenario 1 – Total Loss of IT and Internal telephony

This scenario is the most catastrophic, as all IT systems, both cloud hosted (online) and internally hosted will be compromised with Council staff unable to use them. In addition, all laptops used by staff are compromised and could not be used. This would result in all digital services and telephony being unavailable. Work Mobile phones would be able to be used for telephony and SMS.

This scenario is very unlikely, as the cloud hosted services used by the Council have very advanced protection against cyber-attacks, and recent major cyber-attacks against Local Authorities have not seen cloud hosted services compromised.

In this scenario, the Council would need to reply on paper-based processes to operate until IT services are restored.

In the unlikely event cloud hosted services are compromised, we would rely upon the suppliers to restore them. Experience (from other cyber attacks) shows that most suppliers are well placed to deliver swift and secure restoration.

Scenario 2 - Total loss of internally hosted IT and Skype telephony

This scenario has been experienced by Local authorities that were subject to cyber-attacks, in that they lost access to all services hosted internally, including all laptops, however were still able to access cloud hosted services such as email and document storage.

The Council has several cloud hosted systems such as all of the Microsoft 365 applications, which still could be accessed (via non compromised devices) in the event of this type of outage.

Services that would be unavailable in this scenario include key applications such as CareFirst, telephony using Skype, Financial systems, and Education systems, plus the loss of all corporate laptops used to access any systems unaffected.

In this scenario, it would be possible to operate on a limited basis with staff using devices other than Council devices to access cloud hosted services. This could include personal devices and / or devices loaned from partners but would need to be used offsite from Council premises.

Scenario 3 – Total loss of on-premise IT, client devices still operational

The Council would lose access to all services hosted internally, however were still able to access cloud hosted services such as email and document storage from Council provided laptops.

This scenario needs to be treated the same as scenario 2, as until each laptop has been verified as uncompromised - we would need to assume that devices were compromised initially - therefore the same conditions as scenario 2 would apply.

Scenario 4 – Loss of all client devices

There have been cyber-attacks where all client devices such as laptops and desktops have been compromised, however this has been in conjunction with other major applications also being compromised.

It is possible for a cyber vulnerability to exist only on client devices, with applications on server infrastructure not subject to the same vulnerability, in which case an attacker could compromise all client devices, rendering them inoperable.

In this scenario, it would be possible to operate on a limited basis with staff using devices other than Council devices to access cloud hosted services. This could include personal devices and / or devices loaned from partners.

Scenario 5 – Loss of a key system

This scenario is unlikely due to a cyber-attack, as multiple systems are hosted on the same infrastructure, and it is very rare for a cyber-attack to target a single system as the attackers generally seek to maximise the impact of their attack to leverage greater returns by affecting as many systems as they can.

The impact would depend upon the system(s) affected.

Scenario 6 – Loss of a single building

The Council's infrastructure is replicated across buildings, with the ability for any member of staff to work from any building. This scenario would only materialise if a client device was affected at a specific site and was not able to infect sites. All laptops used by staff would be assumed to out of operation, with the impact being determined by the specific building affected.

Scenario 7 – Loss of network connectivity

There are certain cyber-attacks which target network connectivity, known as Denial of Service (DoS) attacks. This type of attack is generally limited to internet access and can be contained quickly using technical controls, therefore the impact of such an attack is determined as low.

What are we doing to reduce the likelihood of scenarios

The council undertakes an annual IT Health Check, (ITHC) which checks the infrastructure for vulnerabilities. Any identified vulnerabilities are addressed by Delt, which prepare a remedial action plan that is monitored on a regular basis with the Council. Central government are provided with details of the ITHC and will monitor the remedial action plan, issuing a certificate on completion.

The Council has also tasked Delt to prioritise Cyber protection to ensure that all the expected controls are in place to reduce the risk of a cyber-attack. This includes ensuring that robust identity and asset management form the building blocks of an IT infrastructure that will meet future cyber protection architectures.

Delt have produced their own Disaster Recovery plan, which is being tested regularly, last test in December 2022 as a table-top exercise.

Reducing the impact

Corporate Business Continuity Incident Management Plan

A draft Corporate Business Continuity Incident Management Plan has been completed and is with Ruth Harrell as Chair of the Business Continuity Strategic Group (BCSG) to put before CMT for adoption. It is, however, fully usable currently. The key point/mitigation is that the BCSG would convene in whatever format was possible in order to start providing the strategic direction we would need to deal with the event. That group routinely met in October 2022 and will continue to meet every April and October and as required.

Departmental Recovery Plans (DRPs)

All DRPs (42 plans) have been completed. They include specific sections on loss of communications and software with workarounds where possible, in addition to the more traditional scenarios such as a loss of buildings/equipment/personnel.

Personal Business Continuity Plans

The advent of flexible working offers greater resilience in the face of some types of potential attack and puts a responsibility onto individual staff members to consider their personal business continuity requirements. The development of personal business continuity arrangements will be an area of focus in the coming year.

DRP Exercising

The DRP exercising programme is well underway. Currently 20% DRPs have been exercised. By the end of December 2022 the completion rate will be 25-30% and scheduled to be 100% by August 2023. Exercise debrief/assessment sheets are being completed and returned to DRP owners at the conclusion with recommendations such as amendments required/further discussions. Early feedback has stressed the importance, in the early stages following disruption, of the ability to communicate with staff (using personal devices if necessary) to at least regain control, commence discussions about the next stages and to take direction from the BCSG.

General Business Continuity Work Cycle

A 3-year BC work cycle has now been devised to ensure regular reviews of all BC related matters takes place, including BCSG meetings, corporate BC plan updates, communication with plan leads, DRP updates and plan exercising.

New Cloud Storage Facility

An independent (of Microsoft) cloud-based storage system has been identified and ordered to provide resilience to our current S: Drive. The vulnerability of data stored in this drive was identified as a weakness during the completion of the DRPs. The provision of this resilient storage is awaiting suitable (cost effective) proposals back from Delt.

Cyber 360

The Council is taking part in the Local Government Association's Cyber 360 programme at the start of March. The aims of the programme are to build capabilities within councils by coaching and signposting to advice and guidance help councils to better understand what 'good' looks like. The programme is a opportunity for the LGA to learn about various roles and their perspective on the cyber health of the council and to capture any reflections.

A reflective report will be written by the programme team, which will be anonymised, so no comments will be attributable to anyone. The report will not be published publicly, and the council will have a chance to comment before it's finalised.

The report will focus on the

- Strengths - Positive tangible and intangible attributes, within the council's control
- Weaknesses - Internal factors within the council's control that detract from their ability to be as secure as possible.
- Opportunities - Any 'quick wins' or improvements.

Discussion slots have been scheduled with Councillors, management and staff.

Appendix A: Scenario summary

Scenario	Likelihood	Impact	Mitigation
Total loss of IT and internal telephony	Low	Council unable to function digitally	DR Plans for individual departments
Total loss of on premise IT and Skype telephony	Medium	Council has access to cloud hosted services, key applications such as revenues and benefits unavailable. All Laptops unavailable.	DR Plans for individual departments Personal BC plans for staff
Total loss of on-premise IT, client devices still operational	Medium	Council has access to cloud hosted services, key applications such as revenues and benefits unavailable. All Laptops unavailable until verified as uncompromised.	DR Plans for individual departments Personal BC plans for staff
Loss of all client devices	Medium	Council has access to all applications, however staff do not have a device available to access them.	DR Plans for individual departments Personal BC plans for staff
Loss of a key system	Medium	Dependent upon system	DR Plans for key departments relying on key systems
Total loss of a building	Medium	Dependent upon building	DR Plans for individual departments
Network connectivity loss	Medium	Low	Technical controls to identify and stop DoS attacks.