Report to	**Audit Committee**
From	**Assistant Director of Digital, Data and Technology**
Risk Reference	**CR3**
Risk Description	**Security and Resilience**
Recommendation	**For analysis and discussion**

Context

In an era where digital transformation is rapidly evolving, the importance of cyber security in local government in the UK cannot be overstated. Local councils and public sector bodies are increasingly reliant on digital infrastructure to provide essential services to citizens. As these services become digitised, we also open further doors to cyber threats. We must ensure that cyber security measures that are protecting the integrity of these services are current and adequate

Recent years have seen a significant increase in cyber-attacks on local government in the UK. For example, the ransomware attack on Redcar and Cleveland Borough Council in 2020 led to substantial disruption of services and considerable financial loss. There was also the attack on St Helens that led to several issues for the council moving forward.

Local governments in the UK are subject to various legal and regulatory requirements concerning cyber security and data protection. The General Data Protection Regulation (GDPR) mandates stringent measures for the protection of personal data. Failure to comply with these regulations can result in substantial fines and legal repercussions.

In addition to GDPR, local governments must adhere to the National Cyber Security Centre's (NCSC) guidelines and frameworks, such as the Cyber Essentials scheme. These frameworks provide a set of best practices for managing cyber security risks and ensuring compliance with legal obligations.

Cyber security is not solely the responsibility of IT departments; it requires a holistic approach involving all levels of an organisation. Bury must foster a culture of cyber resilience, where every employee understands the importance of cyber security and their role in protecting the organisation's assets.

Key Potential Impacts

In the event of a successful Cyber Attack the there are several devastating impacts both in the short and long term and we can learn the depth of these from organisations that have experienced similar events.

Listed below are the impacts that we could experience in the event of a successful cyber-attack – though this is not an extensive list as there are impacts, we can't foresee.

Short Term Impacts

Reputation

In the event of a cyber-attack often the public lose faith in the organisations ability to provide digital services. This has several issues attached to it but as the Council's strategy is to promote a digital first approach that will not only make life easier for residents but also to help make efficiencies desperately needed to meet demand.

If the public lose faith in the ability to use these systems, then this could have a devastating impact on our abilities to deliver these services through a digital medium

Operational

In the event of a successful attack, it will be incredibly difficult to operate safely during and in the immediate aftermath. We would likely be forced to take all services offline while we remedy the issues, and this would mean access to systems like Unit 4 our financial system or iTrent our staff management system would not be available. This could mean depending on the time of the month we might not be able to process staff payment.

Regulatory

The Information Commissioner's Office (ICO) has the authority to impose significant fines on public organisations that fail to protect personal data adequately. Under the General Data Protection Regulation (GDPR), fines can reach up to €20 million or 4% of the organisation's annual global turnover, whichever is higher. For public organisations, this can translate into substantial financial penalties that can impact their operational budget.

The ICO may issue enforcement notices requiring the organisation to take specific actions to comply with data protection laws. These notices may mandate the implementation of improved security measures, staff training, or changes to data handling procedures. Non-compliance with enforcement notices can lead to further legal action and increased penalties.

In extreme cases, where there is evidence of deliberate or reckless behaviour leading to a data breach, criminal prosecution may be pursued against individuals within the organisation. This can result in personal fines, imprisonment, and a criminal record for those found guilty of serious data protection violations.

Public organisations must therefore take proactive steps to safeguard against cyber breaches and ensure compliance with data protection regulations to avoid these severe regulatory punishments.

Financial

Obviously unpinning all of the above is the financial impact that is considerable especially in the event of ransomware attacks

Outside of the actual impact of the event there are secondary impacts that surround our equipment which may need to be replaced and the extra services that may be needed to help re-establish the services

Below are some examples of attacks to UK based organisations and the impact

Case Studies of Financial Impact

1. NHS WannaCry Attack (2017)

One of the most notable cyber attacks in recent history is the WannaCry ransomware attack that targeted the National Health Service (NHS) in May 2017. The attack caused widespread disruption across the NHS, affecting more than a third of NHS trusts and around 8% of GP practices.

Financial Impact:

- The direct costs of the attack were estimated to be around £92 million. This includes the costs associated with IT support, system recovery, and additional staffing to manage the crisis.
- The indirect costs, such as lost productivity and cancelled appointments, were significant. It is estimated that up to 19,000 appointments were cancelled, leading to substantial revenue loss and affecting patient care.

2. TalkTalk Data Breach (2015)

In October 2015, telecommunications company TalkTalk suffered a major data breach that exposed the personal information of approximately 157,000 customers. The attack resulted in significant financial losses and reputational damage.

Financial Impact:

- TalkTalk reported a one-off cost of £42 million directly associated with the breach. This included costs for incident response, customer support, and remediation efforts.
- The company also experienced a loss of £15 million in revenue due to the breach, as the incident led to a loss of customers and a subsequent drop in stock prices.
- In addition to these immediate financial impacts, TalkTalk was fined £400,000 by the Information Commissioner's Office (ICO) for failing to implement adequate security measures to protect customer data.

3. British Airways Data Breach (2018)

British Airways faced a significant data breach in 2018, where approximately 500,000 customers' personal and financial information was compromised due to a sophisticated cyber attack.

Financial Impact:

- British Airways faced an initial penalty of £183 million from the ICO under the GDPR regulations. This fine was later reduced to £20 million, but it still represents one of the largest fines ever imposed by the ICO.

- The airline also incurred substantial costs related to customer compensation, legal fees, and remediation efforts. Industry estimates suggest that the total financial impact of the breach could exceed £100 million.

4. Travelex Ransomware Attack (2019-2020)

Travelex, a foreign exchange company, was hit by a ransomware attack in December 2019 that forced the company to shut down its online services for several weeks.

Financial Impact:

- The attack reportedly cost Travelex around £25 million in direct losses, including costs for IT recovery, lost revenue, and other operational disruptions.
- The incident also had long-term financial repercussions, contributing to the company's financial difficulties and eventual administration in August 2020.

Long term Impacts

There are in addition to the short-term impacts some more longer-term impacts

- Unwillingness for other organisations to share data with us in future working or needing to complete extra tasks before they will work with us reducing opportunities for Bury
- Insurance premiums could be negatively effected
- Lasting public reputational Damage
- Increased scrutiny for years by national bodies

Current Controls

At Bury we have several layers of protection already in place and we are looking to grow our cyber resilience with a constant improvement of our policies and procedures as well as our toolset.

Here is an overview of our controls that are in place currently;

DDaT Revolution

Last year the council made the decision to move away from their traditional IT structure to a more modern DDaT offering. As part of this structure change a dedicated position was formulated to recognise the importance of Cyber Security, therefore we now have a Cyber Security and Compliance Officer whose role is dedicated to working on improving our security.

SOC (Security Operations Centre)

We have a currently a Security Operations Centre that is run by ANS (Though this is set to change see Planned Actions for detail). This is a 24/7/365 operation that monitors threats to our environment and will act on our behalf for certain actions to ensure that we have around the clock protection

Firewalls

Firewalls operate both internally and externally for the organisation that they allow traffic to and from the outside world. We operate “geo-locking” in our firewalls which ensures that traffic coming from other countries is not allowed to connect to our network.

JISC DDOS Protection

This is the protection from denial-of-service attacks where cyber criminals use tactics that bombard the network with traffic to effectively cause the systems to collapse. This is often used as a diversionary tactic rather than the main point of the attack.

Microsoft Security

We employ a full range of security features from Microsoft including their defender solution. We work closely with our partners on this and Microsoft to ensure that we are consistently keeping ourselves in line with best practices

Other examples

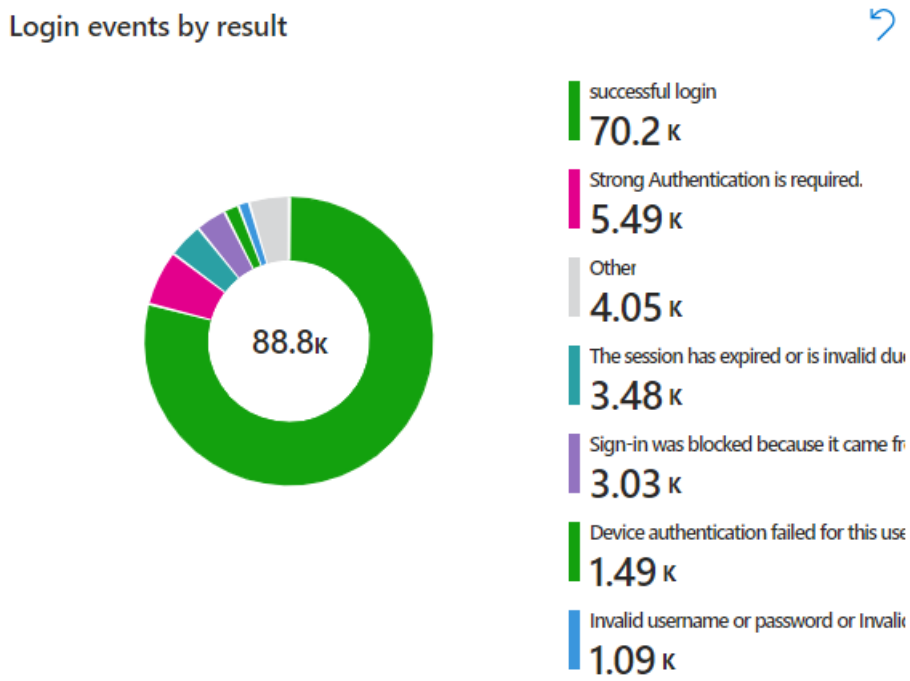
There are other examples of practical ways in which we are working to protect Bury Council:

- Backups – we back up data to the Microsoft cloud
- External flagging – after a spate of phishing attacks we implemented an “external” flag on emails to highlight the email has come from an outside source
- Policies – we have committed to implementing a full ISO27001 compliant policy set work has started on this and will be complete end of Oct with a audit from Salford commencing in Nov
- PSN accreditation – after our initial assessment we will be submitting our remediation at the end of the coming week (w/c 30th Sep)
- Cyber Essentials plus accreditation – the team are working towards attaining this in 2025 with gap analysis being commissioned to help steer us
- Change Control – we’ve implemented change control to ensure we are tracking any changes to systems made by the team

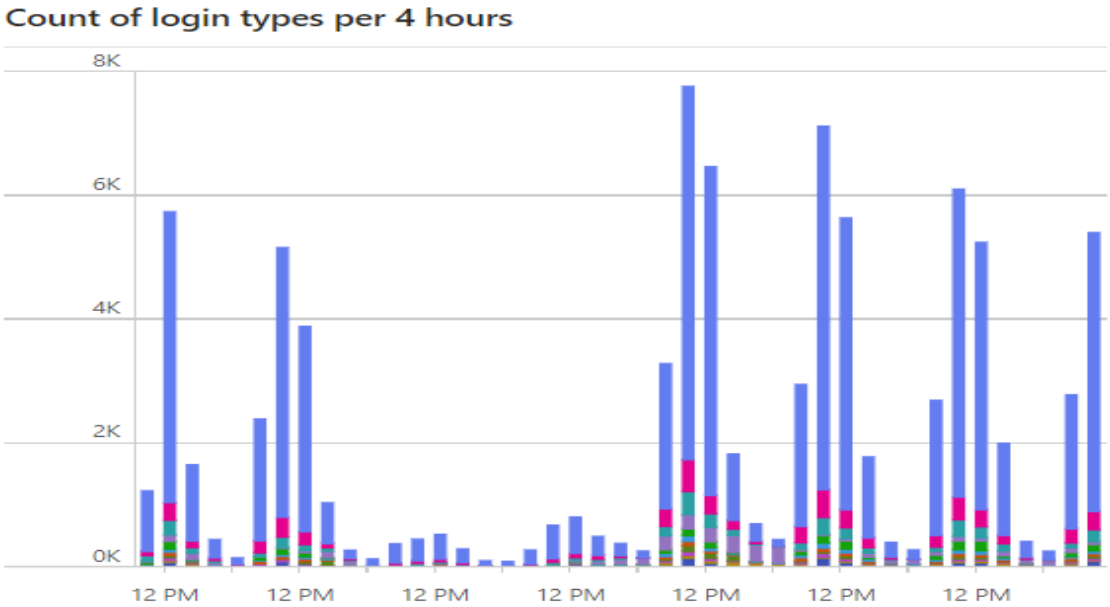
Further examples

Below you will see an example of what the some of our security features do for us and an idea of the volume of information flowing;

The below shows over the last week how many login events there have been. As you can see there are 88k logins in those 7 days alone. You may wonder why this is so high but every time as system is access where the login details are used it is logged an assessed by the system



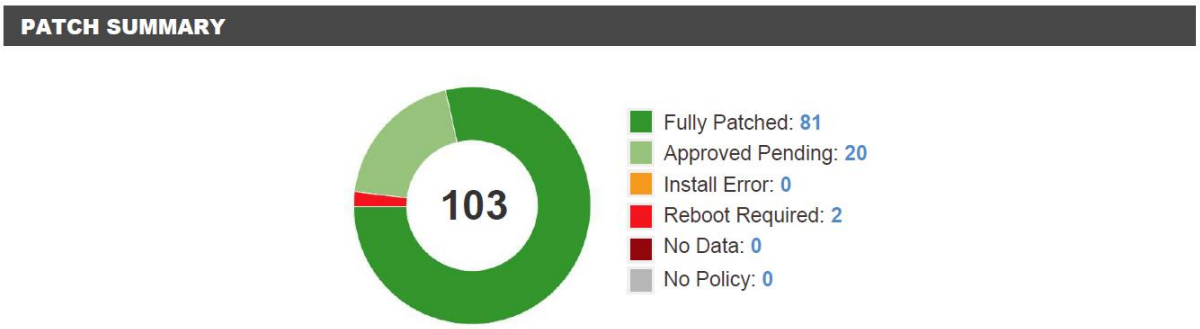
This gives you an idea of how that might be spread across this day



This is the spread of logins we may typically see by application

We also limit the number of admin accounts we have and make sure that we are reviewing them regularly

In addition we regular patch our systems which means that we update them to the latest versions they can be this ensures that any security flaws that come to light are quickly shut down



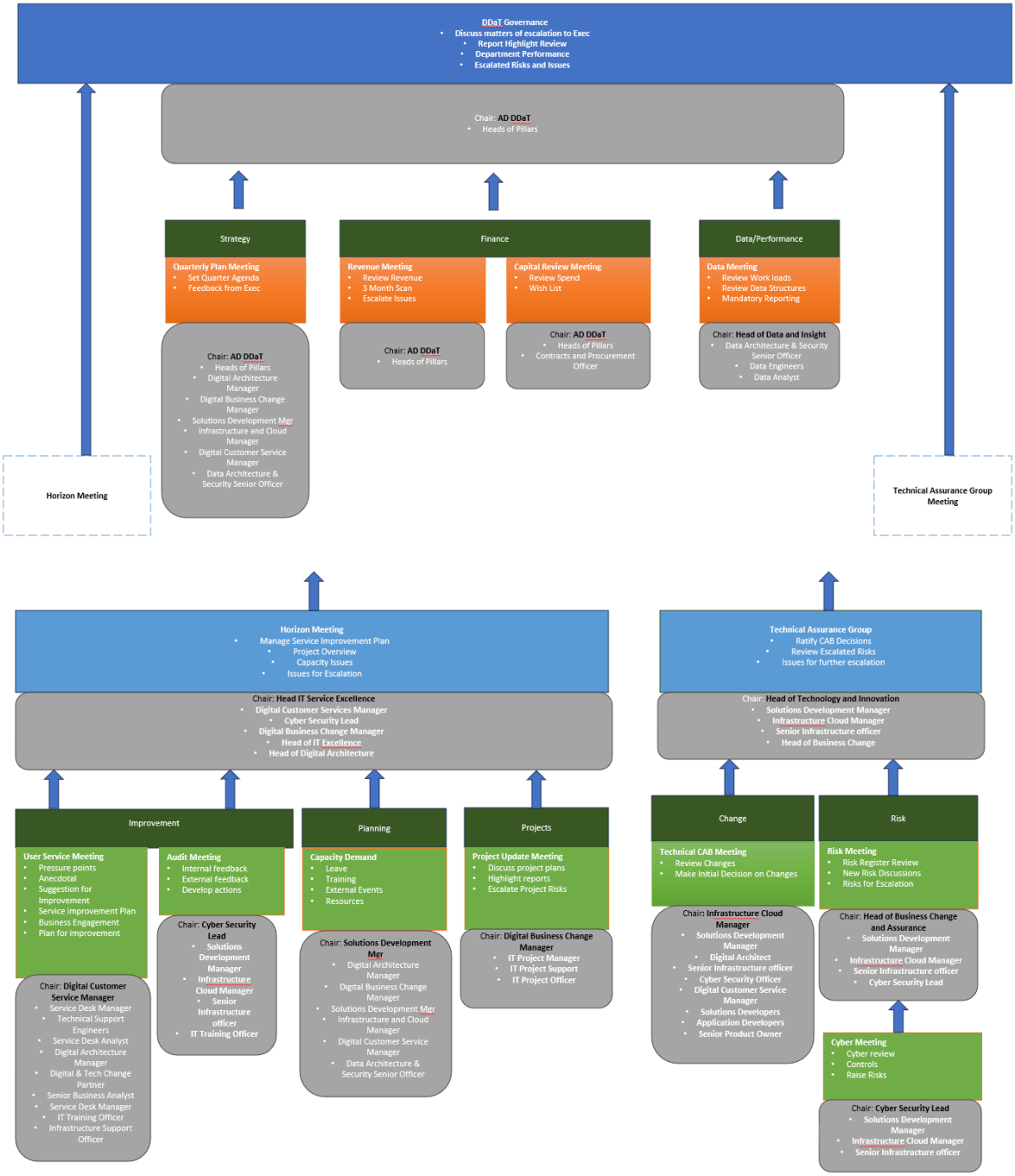
Some patches require a little extra approval as from time to time these can cause issues to the system, so they need to be carefully implemented

Two Factor Authentication

We have enabled two factor authentication on all the systems we can providing and extra layer of protection from attacks on credentials

Governance

One of the most effective ways of protect against cyber attacks is to have good governance within the Digital team. Over the last 6 months we have created a new governance structure which is well on its way to being implemented fully this can be seen below;



Planned Actions

On top of the actions that we already have in place we will be working to expand our skills and toolsets to try and stay ahead of the curve. Below is a list of actions we are currently working on;

Zabbix

Bolstering our current toolset we are implementing a tool called Zabbix that is a open source (free) tool which can improve the monitoring of our network and we will have some more interactive dashboards to make it easy to see issues;

SOC Change

As mentioned we are moving our SOC away from current supplier ANS this is to work with our neighbours Salford Council who have a SOC that they operate. Not only will this provide a significant saving for the council but it fosters a mutually beneficial relationship in which Salford Council who are digital one of the leading organisations will help us to upscale our digital maturity and there can be quick sharing of information and skills.

#Digital Salford

Salford City Council

Desktop Exercises

In addition to our joint SOC we are also going to work with Salford to complete cyber attack simulations referred to as Desktop Exercises. This will involve the team working through a cyber attack simulation to understand where our current knowledge, processes and practices may come up short in a real event.

Immutable Backups

We are currently seeking funds to onboard the council for what are referred to as immutable backups. Currently we back up the data in the cloud but in theory there is a link between our environments we use and the backups. What this means is that potentially a ransomware attack could encrypt our backups in addition the live environment. Immutable back ups sever the link between your environments and the backup so in the event of a ransomware attack our data is safe and cannot be reached by the attack.

Training and Processes

We will be looking to upskill the team constantly to ensure that we have staff trained to deal with situations such as a cyber-attack. We will continue to tighten our processes too in order to keep the environment safe