CYNGOR CAERDYDD
CARDIFF COUNCIL

DEMOCRATIC SERVICES COMMITTEE: 22 November 2022

REPORT OF THE HEAD OF ICT

CYBER SECURITY - PASSWORDS, MULTI FACTOR AUTHENTICATION (MFA) AND MOBILE DEVICE PROTECTION

Reason for this Report

1. The purpose of this report is to update the Democratic Services Committee on some of the Cyber Security controls in place around Cardiff Council systems and data.

Background

2. The aim of Cyber Security is to protect the **Confidentiality, Integrity and Availability** of council data and services. Particularly as the council's network contains highly sensitive data about citizens and staff, relevant under UK Data Protection legislation.

3. Cardiff has many regulatory & compliance obligations that require the organisation to implement a range of security controls, these include:
   - the UK Data Protection Act (2018) legislation,
   - Compliance & Memorandum of Understanding (MOU) obligations such as PSN and Cyber Essentials with Central Government departments. Examples of this include :
     - access to DWP data for Housing services the council can offer and impacting vulnerable citizens
     - access to health data for social care systems impacting vulnerable adults and children
     - access to the Electoral Registration services impacting the council's ability to perform elections
   - contractual obligations such as PCI Compliance for handling card payments.

Current controls

Passwords

4. One of the most obvious examples of cyber security controls is the use of passwords. The current password policy within Cardiff Council is as follows:

    - The password is at least nine characters long.
    - The password must contain at least 1 character from each of the following:
        - Letters - English uppercase characters (A - Z) OR English lowercase characters (a - z)
        - Numbers (0 - 9)
        - Non-alphanumeric Characters (For example: !, $, #, {, @ or %)
    - The password is required to be changed every 60 days.

Multi-Factor Authentication

5. An enhancement to the use of passwords is the use of Multi-Factor Authentication (MFA). This can also be called 2-step verification (2SV) or two-factor authentication (2FA). Multi-factor Authentication (MFA) is an authentication method that requires a user to provide two or more verification factors to gain access to a resource such as an application or an account.

6. For Cardiff staff, we use this when accessing online services from Microsoft, held in Office 365. This requires the additional authentication from a Multi-Factor Authentication device, either via an smartphone App approval, App code or confirmation via telephone call.

7. These services, that would previously have only been accessible from inside the internal network, are hosted directly in the cloud and so can now be accessed from anywhere in the world including from high threat nation states, or may allow remote connectivity to on-premise services, and as such require this additional level of security for authentication.

8. However, if the access comes from a known physical council location, i.e. a council office-based worker, then MFA is not required. In these cases the security is considered provided via physical building access controls.

9. Unfortunately, Microsoft applications which should share a single MFA authentication request between applications occasionally fails to replicate in a timely fashion, and this can mean multiple MFA prompts are asked for which we are aware can be an annoyance.

Mobile Device protection

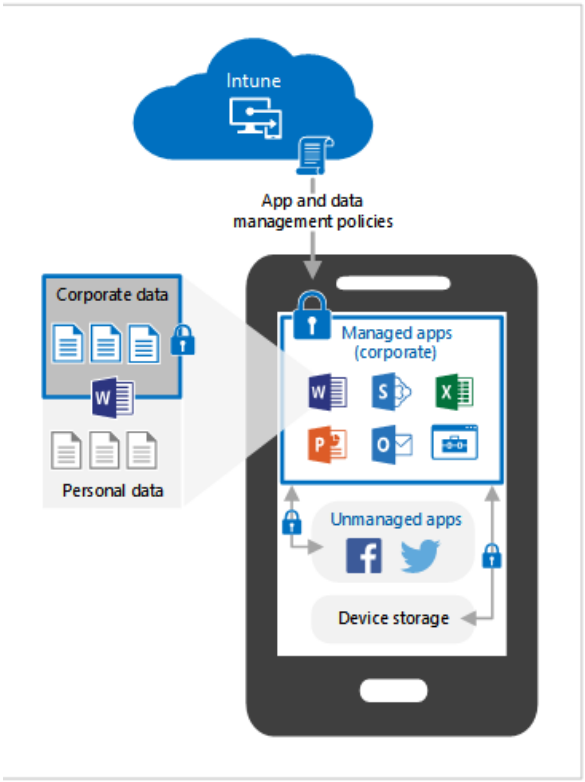
10. Access to council email and data can be performed from both personally and corporately purchased mobile devices, with both operating in the same way. This is both a convenience in terms of not having to carry multiple phones but also a cost saver for the organisation. Access to this council provided email can be managed securely via either:

- Mobile Device Management (MDM). MDM requires taking full control over of a mobile device, which is highly restrictive and takes excessive management. Realistically this not something staff would want to have happen on their personal devices, and for this reason MDM is not used.

- A Mobile Application Management (MAM) – this separates the storage and access of data into a separate secure container, away from the insecure unmanaged portion of the phone (whether corporately or personally purchased makes no difference).

  When using any council provided services on a mobile device, for example email or Word, access between managed and unmanaged storage areas is blocked. This is so that Council data cannot be copied out of the 'managed area' or app, and pasted into an insecure 'unmanaged' area or app. You can copy into a managed application though, for example by taking a photo and adding to a council email.

  Unlike the unmanaged element of the phone where there can be no control over security policies, these corporately provided apps have a PIN for access as well requiring MFA authentication every 7 days, so this provides a high level of security to the authentication process. The below diagram may help visualise this MAM solution:



- The MAM solution enables personal devices to be used without direct control by Cardiff Council but ensures council data is not incorrectly stored in breach of the council's obligations.

Issues & Risks

Passwords

11. Guidance from the ICO recommends that we "*take appropriate technical and organisational measures to prevent unauthorised processing of personal data*" and consider that:
    - "*password length - you should set a suitable minimum password length (this should be no less than 10 characters)"*
    - *"special characters - you should allow the use of special characters"*
    - *"password 'deny lists' - do not allow your users to use a common, weak password. Screen passwords against a password 'deny list' of the most commonly used passwords*"

    Passwords in online services | ICO

12. Guidance from Microsoft and the National Cyber Security Centre (NCSC) is similar and ultimately recommends that password are longer (Three random words - NCSC.GOV.UK), but do not expire until suspected of being breached, and that weak passwords are blocked from being chosen by using a deny list to prevent common, guessable passwords being used.

13. The use of automated responses to "Risky Sign-ins", for example due to brute force attack attempts, or impossible travel where logins originate from 2 different countries, is also recommended to reduce overall Cyber Threats.

14. After review ICT feel the current settings are generally adequate, however the additional protection offered by enhanced security such as those provided by Microsoft E5 service with extra protection from "Risky Sign-ins" would increase Cyber Security and potentially improve user experience, but this would come at a significant additional ongoing cost.

    Multi-Factor Authentication

15. Guidance from the ICO recommends that "*You should implement two-factor or multifactor authentication wherever it is possible to do so - to take the most common example, a password and a one-time token generator. This will be more important where the personal data that can be accessed is of a sensitive nature, or could cause significant harm if it were compromised*" (Passwords in online services | ICO)

16. Guidance from the NCSC recommends that MFA is used wherever possible: "*As long as passwords are used for authentication, there will always be a chance that users and administrators will choose machine-guessable passwords and be susceptible to social engineering. Therefore:*
    - *Organisations should choose Cloud and Internet-connected services that offer a form of multi-factor authentication.*
    - *All users, including administrators, should use multi-factor authentication when using Cloud and Internet-connected services. This is particularly important when authenticating to services that hold sensitive or private data.*

- *Administrators should, wherever possible, be required to use multi-factor authentication.*
- *Organisations should consider carefully the use of services which only allow for single-factor authentication."*

(Multi-factor authentication for online services - NCSC.GOV.UK)

17. It is worth being clear that any breach of data that occurs will always be forensically attributable back to the account/user – therefore without MFA to safeguard sign-in attempts with an extra factor this will mean that all data breaches could be incorrectly attributed to the user and could also lead to personal consequences and fines under data protection legislation.

18. A review of other similar organisations was performed in September 2022, and this found that:

    - A UK Government department (national agency), which uses Google services, has a policy of requiring MFA every day.
    - Welsh Government upgraded to Microsoft E5 services and has implemented MFA with extra protection from "Risky Sign-ins" to allow lower risk user and sign-in attempts to occur without needing MFA unless a high risk sign-in occurs. However, the majority of data is held within their private network and this can only be accessed via VPN which requires MFA every time (every day).
    - Welsh Assembly - upgraded to Microsoft E5 services and has implemented MFA with extra protection from "Risky Sign-ins" to allow lower risk user and sign-in attempts to occur and only prompt every 14 days.
    - Newport Council has a policy of requiring MFA every day, and following a recent issue limit logins to UK geographical locations.
    - Vale of Glamorgan Council upgraded to Microsoft E5 services and is currently implementing MFA with extra protection from "Risky Sign-ins" to allow low risk user and sign-in attempts to occur
    - Caerphilly Council upgraded to Microsoft E5 services and is implementing MFA with extra protection from "Risky Sign-ins" to allow low risk user and sign-in attempts to occur and only prompt every 90 days

19. The current setting of requiring MFA every 7 days which is used by Cardiff can only be set globally and cannot be altered to provide different values for different groups of staff.

20. After review, with the current security tools in use, ICT feel the current setting is both adequate to meet Cyber Security needs, as well as Regulatory, Compliance and Contractual obligations. We recognise that security and good user experience is sometimes a difficult balance to achieve.

21. However, the additional protection offered by the enhanced Microsoft E5 service with extra protection from "Risky Sign-ins" would increase Cyber Security options and potentially improve user experience. This software will profile normal behaviour and be able to automatically detect unusual, abnormal or risky sign-ins and, allowing MFA prompts to happen less often in normal

circumstances (e.g., monthly) but when a risky sign-in occurs immediately prompt for MFA.

22. This is under consideration but with additional costs of circa £430k p.a. this is not an easy decision with the current financial position.

Mobile Device protection

23. MAM is the most suitable end user experience available, and more cost effective than an alternative MDM approach where the council will most likely have to purchase corporate devices for staff who currently use their personal devices at no cost to the council.

24. When using MAM, copying and pasting council data from a managed app to the unmanaged phone or other apps, e.g., Twitter, Facebook, WhatsApp & Google services, is blocked. This is to enforce necessary data protection controls so that insecure & unencrypted mobile devices cannot become the source of a data breach, regulatory fine and reputational damage. For example Greater Manchester Police were fined £150,000 for the loss of an unencrypted device - Encryption and data storage | ICO

25. After review ICT feel the current settings are adequate to meet Cyber Security needs, as well as Regulatory, Compliance and Contractual obligations, particularly for Data Protection.

26. Where data needs to be copied and pasted out of a council system ICT recommends that this should be done on a council managed device, available to all Members from Member Services, this ensures that no unmanaged device or application can intercept council data.

Impact of not meeting our ICT Security obligations

27. Failure to meet our Cyber Essentials & PSN obligations could lead to the withdrawal of services such as DWP provided data affecting Housing services the council can offer and impacting vulnerable citizens; or access to health data for social care systems impacting vulnerable adults and children; or access to the Electoral Registration services impacting the council's ability to perform elections.

28. Failure to meet our UK Data Protection legislative obligations could lead to a data breaches, corporate sanctions and/or significant fine up to £17.5 million per breach under the UK GDPR, as well as cause significant reputational damage. If the breach is a cyber attack this could lead to loss of council services for months or years (A very valuable watch or read from Copeland council - Video - Covid and Copeland Cyber Lessons | UKAuthority / PDF - Copeland Council Case Study - Response and Recovery from a major Cyber Attack) significantly affecting citizens in Cardiff.

Financial Implications

29. There are no direct financial implications arising from this information report. However, failure to meet UK Data Protection legislative obligations could lead to a data breaches, corporate sanctions and/or significant fine up to £17.5 million per breach under the UK GDPR.

Legal Implications

30. A key principle of the UK GDPR is that data controllers must process personal data securely, by means of 'appropriate technical and organisational measures', referred to as 'the security principle'. More fully, Article (5) (1) (f) of the UK GDPR requires the Council, as the Data Controller, to have appropriate organisational and technical measures in place to ensure the security of personal data. It states data should be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

31. The UK GDPR does not define the security measures that must be in place, but the level of security must be 'appropriate' to the risks presented by the processing carried out. This must be considered in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of the processing carried out, having regard to factors such as:
    - the nature and extent of the organisation's premises and computer systems;
    - the number of staff and the extent of their access to personal data; and
    - any personal data held or used by a data processor acting on our behalf.

32. The Council must be able to demonstrate its compliance with the security principle (under Article (5) (2) of UK GDPR, 'the accountability principle').

RECOMMENDATION

33. The Democratic Services Committee is recommended to note the report and the impact of failing to meet our ICT security obligations.

PHILIP BEAR
HEAD of ICT
22 November 2022

Background papers:

Password & Authentication guidance links

- Passwords in online services | ICO
- Three random words - NCSC.GOV.UK
- Multi-factor authentication for online services - NCSC.GOV.UK

Encryption guidance link

- Encryption and data storage | ICO

Copeland council Ransomware case study links

- Video - Covid and Copeland Cyber Lessons | UKAuthority
- PDF - Copeland Council Case Study - Response and Recovery from a major Cyber