Literature Review: The Use of Multi-factor Authentication in Frontline Staff

July 2024

Contents

Literature Review: The Use of Multi-factor Authentication in Frontline Staff 1
Introduction..... 3
Why is MFA needed? 3
Who is using MFA? 3
The BSF 3
Healthcare Service: NHS 4
Healthcare Service: AHS 4
Healthcare Service: PHSA 5
Rollout & Challenges 5
Summary 5
References 6

Introduction

Multi-factor Authentication (MFA) is the process in which two or more different authentication factors are required to unlock a device or sign into an account. This literature review investigates the benefits of MFA, who is currently using it, how it has been implemented in other institutions and the risks associated with using it. The conclusion outlines suggestions for BSF and how we could use MFA within our organization.

Why is MFA needed?

Passwords are an easy target for cyber criminals, they can be accessed through phishing or password spray attacks, where the criminal try's several different passwords on the same account until they are successful. If a cyber criminal were to gain access to an account password, they would still require an additional piece of information to fully gain access if MFA was enabled. MFA is an added layer of security providing additional protection to accounts or devices.

Sensitive patient data is handled every day in the Healthcare industry, this data is mostly stored within electronic healthcare records (EHR), online patient portals and cloud-based applications. Although having the data stored in these formats is beneficial for improving patient outcomes, there is a risk that this data could be subjected to a cyber attack. The Healthcare industry is one of the most targeted industries for cyber attacks due to the type of data stored. Attackers can sell patient medical information on the black-market for a large amount of money due to the sensitivity of the data.

Data breaches are expensive to recover from, depending on the severity and scale of the attack. According to [1], the average total cost of a breach was $4.45 million USD in 2023. In 2023 the data breach cost to the healthcare industry was $10.93 million USD, making them the highest costing industry for 13 years in a row.

Who is using MFA?

The BSF

In 2023 The BSF implemented DUO authentication for leadership positions and critical knowledge positions such as IT, Finance, Payroll, etc. There are approximately 100 staff members currently utilizing this MFA method within BSF.

MFA was used within Heart Home Network (HHN) prior to merging with the wider BSF organization. When IT merge was completed in October 2022, MFA was no longer used by HHN staff.

The BSF is looking into rolling out MFA amongst frontline staff. If this is to be implemented, there should be a policy reflecting this change and guidance available for staff.

Healthcare Service: NHS

The National Health Service (NHS) is one of the largest healthcare organisations in the world, with a workforce of around 1.5 million full-time staff. They have been the recipient of countless cyber attacks throughout the years where attackers have gained access to and leaked patient level data and confidential information.

According to the NHS England Policy, DAPB0086: Data Security and Protection Toolkit, MFA was enforced across the organization in October 2023 [2]. This applies to Commissioning Support Units (CSUs), Integrated Care Boards (ICBs), NHS Trusts and Foundation Trusts, and areas of the Department of Health and Social Care.

Although the NHS has not enforced a specific type of MFA, they have advised that organizations should follow government guidelines and national cyber security guidelines.

Healthcare Service: AHS

Alberta Health Services (AHS) published guidance around using MFA in April 2023 in order to improve security across the organization. The guidance explains how to install the Microsoft Authenticator and includes details on how to use this when MFA is required, [3].

Although there appears to be no public policies available outlining who is expected to use MFA, it is clear that many frontline staff will be required to use it in order to access applications used in their work. Within the guidance it is stated that AHS is expanding the use of MFA to many applications, these include:

- Microsoft Outlook
- Project Portfolio Management (PPM)
- CompassionNet
- MyLearning Link
- iExpense
- My AHS
- eSummit
- Unified Access Portal (UAP)
- Learning Evaluation Support System (LESS)
- Insite
- Connection (CliC)
- ServiceNow
- SharePoint
- CapitalCare Staffnet

Healthcare Service: PHSA

The Provincial Health Services Authority in BC published guidance around using MFA in March 2023. The guidance explains how to set up MFA with the Microsoft Authenticator and how to connect work emails to the authenticator [4]. There is no publicly available policy surrounding this guidance, this could either be enforced across the organization or suggested.

Rollout & Challenges

It is important to ensure that the rollout does not disrupt care or other day-to-day operations. Preparation is just as important as the implementation; users should be notified that MFA is being introduced to the organization and be made aware of the importance of using it.

An opt-in or phased approach would be the best way to deploy MFA throughout the organization, this ensures that staff are not overwhelmed by the rollout and can acclimate to using MFA.

The solution chosen must be easy to use by all frontline staff, if the MFA selected is complex to use and understand, frontline staff may not be willing to implement it. It is recommended that the implementation should be a collaboration between IT and frontline staff in order to create a more secure and sustainable healthcare environment [5].

Many organizations are using the Microsoft Authenticator for MFA implementation as it is a free solution and links easily with any Microsoft account, which is applicable to all staff within BSF. The authentication app can be downloaded onto any smartphone and the user will then be able to approve any account sign-ins through their device.

Summary

Although there is little literature available around the use of MFA in continuing care organizations, many healthcare organizations appear to have implemented it over recent years. The enforcement of this seems to vary in the guidance available, some organizations have made the use of MFA a requirement whilst others only suggest that their staff use it. Nonetheless, the use of MFA will overall improve security and better defend the organization against cyber attacks.

References

[1] I. Security, "Cost of a Data Breach Report," 2023. [Online]. Available: https://www.ibm.com/downloads/cas/E3G5JMBP.

[2] NHS, "Multi-factor authentication (MFA) policy," October 2023. [Online]. Available: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/multi-factor-authentication-mfa-policy/nhs-england-multi-factor-authentication-policy.

[3] AHS, 17 04 2024. [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwixxerP4KuHAxXiHDQIHTHqDe4QFnoECBsQAQ&url=https%3A%2F%2Fwww.albertahealthservices.ca%2Fassets%2Finfo%2Fit%2Fif-it-iam-multi-factor-authentication-user-guide.pdf&usg=AO.

[4] PHSA, "How to set up Multi-Factor Authentication (MFA) and Self-Service Password Reset (SSPR)," 2023. [Online]. Available: https://webassets.phsa.ca/citrix/Microsoft%20Token%20Registration%20Instruction.pdf.

[5] HealthTech, "The Benefits of Multifactor Authentication in Healthcare," December 2018. [Online]. Available: https://healthtechmagazine.net/article/2018/12/benefits-multifactor-authentication-healthcare-perfcon.