Implementing A Mandatory Password Change Policy at an Academic Medical Institution

Michael W. Brogan, PhD[1], Ching-Ping Lin[2], Rakesh Pai[3], Ira J. Kalet, PhD[1,2]
[1]UW Medicine Information Technology Services, Seattle, Washington
[2]Biomedical and Health Informatics, University of Washington, Seattle, Washington
[3]Mhalsa Technologies, Inc., Overland Park, Kansas

Abstract

UW Medicine implemented a new policy requiring users to change passwords at least once every 120 days. In the first two password change cycles, many users did not take action upon notification, and their passwords expired, causing high help desk loads. Compliance and support loads improved in subsequent cycles. We conclude that policy changes requiring user behavior modification should be seen as a cultural change, and the implementation strategy should consider socio-technical factors.

Introduction

UW Medicine instituted a mandatory 120-day password change policy, both to support HIPAA requirements to safeguard passwords and to comply with Washington State Information Technology security standards. This policy required both changes in user behavior and a new technical infrastructure.

Setting

UW Medicine Information Technology Services supports approximately 17,600 users in an account and password synchronization system serving six enterprise clinical systems as well as the primary network logon. Historically, users received an assigned password that was rarely changed unless there was a security incident.

Methods

The new password change infrastructure included three primary components: an email notification system that warned users of their impending expiration date five times over 14 days; a web-based self-service password portal; and a system that identified expired passwords and replaced them with system generated passwords.

Initially, 16,500 users were required to comply with the password change policy. To manage help desk loads, we randomly assigned users to groups representing fourteen days over a four-week period. On their assigned day, the system began sending email notifications to users indicating that their password would expire in two weeks. Notifications included instructions on how to change passwords using the self-service portal. If a user did not change their password by the expiration date, the system replaced the password. Assistance from the help desk was required to regain application access. In anticipation of an increase in support calls, the help desk added ten temporary staff.

Results

Trends in user password changes, expirations, and support load were cyclical, with a 120-day periodicity. The time series included 3.5 cycles spanning 52 weeks, and Table 1 reports expirations and support calls per 100 password changes.

	Expirations	Support calls
Cycle 1	33	64
Cycle 2	38	72
Cycle 3	28	44

Table 1. Password expirations and support calls per 100 password changes.

We did not see the expected reduction of expirations and support calls from Cycle 1 to Cycle 2. Anecdotally, many users were not regular email users or thought the password change policy was a one-time event. The number of expirations and support calls decreased by the third cycle, and data from the incomplete fourth cycle suggests further improvement.

Conclusion

Introduction of a new password change policy resulted in low password policy compliance and high support loads for two consecutive support periods. However, compliance improved over time. Understanding different user types, developing targeted communication, support from institution leadership and pro-actively managing help desk resources were keys to our password change implementation. We plan further research into understanding the account management and communication methods of our diverse user population to better facilitate future policy changes.