SonMax Consultants Inc.
24 Manor Drive
Marlboro, NJ 07746
E: sales@sonmax.com
T: +1 732.591.1512
F: +1 732.591.5424
www.sonmax.com

The downside of complex password policies

Steven Wertheim

One of the thorniest issues facing ID and access management personnel is how to effectively manage and comply with the burgeoning, complex world of password standards. Organizational policies are rarely consistent from company to company, and significantly burden users to devise effective ways to manage growing password pools.

For example, my Keeper app on my iPhone currently stores 93 separate passwords (I have 20+ additional websites for which I have passwords, but don't have them in my Keeper). While I tend to be consistent in creating my passwords (1 Uppercase letter, 1 number and 1 special character), there are numerous sites that don't support that paradigm; I therefore have up to 25 DIFFERENT passwords in my Keeper.

I have worked with organizations that have a 30-day expiration on passwords; 90-day expiration on passwords; 180-day expiration on passwords; and no expiration on passwords. I know of organizations that require multiple special characters; multiple numbers; multiple capital letters and password lengths of up to 12 characters, all with no character runs or repetitive characters.

With so much information to recall, how can people remember every password? How can workplaces manage password change policies and those for visited sites?

Here are some of the crazy passwords I've seen written down:

- Y3Ll0w$T0N3
- M1ck3yM0u$3
- 1H8thi$p1Ac3
- Kum0nFr1dAy

Then there are security policies that randomly generate passwords such as:

- Fq4t0-uabn]p]354yu=h
- 3<M@#^@ijsujf[p_E$#n
- 236gj9%#$&Uqouc

Good luck trying to remember them!

My favorite story regarded a user workspace that had a folded note next to the hanger that read "stupid password". The password was there for all to see upon lifting the flap.

Here's the truth: This chaos **reduces** rather than increases security. Empiric evidence shows that in any workplace, up to 7.5% of all user workspaces have

passwords written down in clear text. These can be found on Post-It notes on monitors, taped to the undersides of keyboards, written on or underneath desk blotters, or on phone bases. These violations of password protection policies exacerbate security people's jobs every day and create business risk.

The problems are obvious. If 7.5% of the staff is keeping passwords out in the open, there is no security. Even if only 1% of staff is leaving passwords vulnerable, there no security.

How can this be fixed? Start by ditching passwords! Instead:

1. Enable multi-factor authentication
    a. Make the mobile device part of the password (smartphone, pad)

2. Enable biometric password controls
    a. Use FIPS certified scanners
    b. Use biometric smart cards – CCID compliant

Blending these two methods results in a much more secure environment, without many of the associated risks of compromise. Is it an investment? Absolutely. Is it better than the status quo? Totally!

Consider the following:

A biometric smart card can be used for facility access control; for example, enabling building access for Jane Doe from Monday through Friday, 7am to 7pm, with all other access restricted. The same smart card can restrict access at Jane Doe's workstation, and be set to any hours, depending on Ms. Doe's responsibilities.

Jane Doe can use her 'BYOD' or her company-issued smart phone for multi-factor authentication at her workstation. When she puts her smart card into the CCID-compliant reader while booting up her workstation, the system automatically generates a one-time use token that is sent to her smart phone. Ms. Doe enters those characters into the workstation's pop-up screen, and she is now fully logged into her workplace systems.

Nothing to remember. Nothing to write down. No issue with expiring passwords or burdensome password controls. Such security is also NIST compliant, and can be PIV-I compliant as well.

Give it a try. It's time to get rid of cumbersome password controls and begin implementing workable and real security.

To learn more, please contact me at steven.wertheim@sonmax.com.