Compliance and Beyond: Future-proofing your password policy

Months before writing this whitepaper we published an infographic, called the Specops Strong Password Guide. The intention was to direct our visually motivated readers towards better password security. Yet, despite its timeless good looks, a certain part of the infographic must face an aging reality. What was once perceived as a best practice, is now considered an anti-pattern. The Identity Protection team over at Microsoft, is calling for the end of password expiry and periodic password resets.

When we were first hit with the expiration vs. no expiration dilemma, our recommendations pledged allegiance to compliance requirements, specifically the Payment Card Industry Data Security Standard (PCI DSS). With their implementation serving to protect sensitive data, compliance bodies such as the Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley (SOX) naturally have recommendations trickling into password policies. But, as hackers find new ways to exploit password protected systems, widely accepted password policies, such as forced password expiration, must be called into question.

In this paper we will scrutinize conventional best practices, using knowledge attained from Microsoft’s “Password Guidance” whitepaper, and National Institute of Standards and Technology (NIST)’s “Digital Authentication Guideline” publication SP 800-63-3. Next, we will examine the extent to which the new best practices have penetrated compliance requirements. Finally, we’ll create a strategy for future proofing policies, while continuing to meet today’s compliance requirements.
Shifting burden from users to authenticators

At the heart of the new guidance from Microsoft and NIST lies a theme: Simplify passwords for the users, and place the burden on the authentication system. Perhaps, it has become blatantly obvious that when it comes to password security, users can’t seem to avoid predictable pitfalls. It’s time to move away from policies that encourage poor practice.

Character compositions

There is no better way to illustrate user annoyance with multiple character set requirements than through a meme.

Studies correlate user annoyance with password policies to the selection of weak passwords. When forced to create complex passwords, users will either write them down to avoid memorizing, or follow a predictable pattern (starting with a capital letter, finishing with a symbol). With the focus being on getting into the system, a strong password takes a backseat to a memorable (easy) password.

TIP: Tackle predictable user patterns with the right tools. Specops Password policy can be configured to block commonly used characters at the beginning and end of passwords.

Knowledge-based authentication

A long time ago, before every detail of our life was posted or available on social media, there was some merit associated with knowledge-based authentication. Commonly used for authentication prior to a password reset, knowledge-based authentication (KBA), is an authentication system in which users are required to answer a “secret” question to confirm their identity – Where did you attend high school?
It goes without saying that answers to such questions are susceptible to social engineering. Social engineering is a form of hacking – a hacker tricks the system into thinking they are an authorized user by using information that is readily available. As such, section 5.1.1.2 in the NIST guideline warns against “specific types of information when choosing memorized secrets.”

TIP: Replace KBA with user-friendly authentication approaches – especially during the self-service password reset process.

**Forced password expiration**

We’ve all been there. Every 90 days or so we get that automatic email prompting a password change. We aggressively hit the delete button hoping to cyber-magically send a message to IT – *we don't want to change our passwords!* The argument for password expiration is that it can prevent indefinite access through the use of compromised passwords. Hackers are not always interested in gathering data within a day, instead they could monitor data over a period of time. Regular password changes would limit this attack vector. Additionally, it can help protect your system from users who tend to reuse passwords – if their password is compromise elsewhere. There's also the aforementioned PCI DSS requirement to expire passwords every 90 days.

But, new evidence is casting doubts on the merits of password expiration. Researchers from the University of North Carolina analyzed the passwords of defunct university accounts. The users of the accounts were required to change their password every three months. After cracking the majority of the hashed passwords in an “offline” attack, the researchers formulated a cracking approach based on previous passwords set by the user. It was revealed that users followed predictable patterns that correlated current passwords with future passwords – character substitution, leetspeak, incrementing numbers, etc. Such patterns allowed the researchers to predict password changes for 41% of the accounts, in a matter of seconds.

TIP: Vary password expiration by user groups, and the complexity of the password policy.
Compliance requirements

Access management and authentication are at the core of compliance - afterall critical personal data is at risk. As long as passwords hold the access key to corporate systems, it is imperative to view compliance requirements in the backdrop of current wisdom about secure passwords.

HIPAA

While the HIPAA requirements around passwords aren’t specific, sections 164.308(a)(5)(i) and 164.308(a)(5)(ii)(D) require that the following plan is in place:

- A security awareness and training program for all members of its workforce
- Procedures for creating, changing, and safeguarding passwords

What does the aforementioned look like when put in practice? It can be as simple as common sense precautions such as not sharing your password, or as specific as character set requirements. The correlation with traditional beliefs about what a "strong password" looks like means that practices such as password expiration, and character set requirements are an unofficial standard.

PCI-DSS

In contrast, PCI-DSS requirements are more specific, and subject to less interpretation. The PCI-DSS standard has this to say about passwords:

- 8.2.3: A minimum length of at least seven characters
- 8.2.3: Both numeric and alphabetic characters
- 8.2.4: Change user passwords/passphrases at least once every 90 days

The full list of password requirements is easy to follow and can be easily achieved with a third-party password policy tool.

SOX

While there is no specific mention of passwords in SOX, in section 404 you’ll find the demand for greater internal controls:

- State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting

The aforementioned is the silent aspect of password compliance within SOX. It is not uncommon to find experts, and auditors making recommendations around character length and composition, as well as periodic password changes.
Future-proofing existing policies

There will always be various perceptions about password security. But, as authorities such as NIST and Microsoft challenge the status quo, one can’t help but re-evaluate their own password practices. If you’re in an industry that abides by compliance policies, you are not required to act until the policy catches up to new recommendations. That is not to say that you cannot take steps to strengthen password requirements, while still meeting current standards. To prepare you for your inevitable breakup with conventional practices, we’ve drawn-out the best practices from the same authorities, and added a Specops Software spin!

**Turn on MFA**
Use multi-factor authentication everywhere you can, especially for privileged users or when accessing critical system such as self-service password reset. Specops uReset enables users to authenticate with various identity services – ranging from identities they established themselves (e.g. social media) to ones that turn a smart phone into a high trust identification device.

**Educate users**
Users have a long way to go, and we have a shared responsibility to educate them on the importance of password security best practices. This means communicating the risks associated with poor practices such as using weak passwords, or reusing them across different sites. This can also include security awareness training on social engineering, phishing, key logging, etc.

**Ban common passwords**
As long as users continue using common/predictable passwords, dictionary attacks will continue to work. Attackers can use multiple dictionaries including foreign words, phonetic patterns, and lists from data breaches such as LinkedIn, Gawker, and Adobe. With the right tools in place, such as Specops Password Policy, organizations can ban any dictionary list from being used in their organization.

**Encourage length**
Size matters, and longer is stronger. Shorter passwords are prone to brute-force attacks. Passphrases, a combination of words that are meaningless together, are easier to remember and harder to crack.
Expiration based on role

Let’s return to the initial dilemma that started this all. There is no single solution to the expiry vs. no expiry debate. If your organization is regulated, you will be better off with enforcing password expiration. Otherwise, the expiration frequency should vary across different user groups and the password policies in place. Privileged accounts should still follow a frequent password expiration period. For non-privileged users you can forgo frequent expiration and strengthen your policy using multi-factor authentication, passphrases, and by banning dictionary words.

Final Thoughts

With password security best practices in constant flux, our effectiveness in safeguarding our organization requires scrutiny. Unfortunately, the regulatory bodies we must abide by do not always pave a clear direction. This is where our own judgement must fill in the gaps. Putting demands on the authentication system shifts burden away from users making poor choices. For example, using a dictionary list in your policy, specifically one that can be configured to include leaked lists, will help prevent the predictable pitfalls that users can’t seem to avoid.

When it comes to password security, it is always a good rule of thumb to take a segmented approach over a generalized one. This means your strategy should take into account different requirements for privileged users who require more security. There is no “set it and forget it” when it comes to password policies. It is a continuous process that must respond to user behavioral patterns, and the emergence of new threats.

https://specopsoft.com