Queensland
Law Society®

Do password policies reduce data loss?

Password Literature Review

February 2023

Do password policies reduce data loss?

Adopting an organisational policy that requires long and complex passwords[1] is usually among the top four or five cybersecurity measures recommended by peak information security agencies.[2] A password policy is seen as a starting point on the basis that policy adoption is a low-cost/high-impact intervention with little downside (although if complexity means a user endlessly recycles passwords, this is a negative outcome).

Use of long, complex passwords is a mandatory requirement in all the primary info-sec standards, and a direction to staff to ensure that happens is seen as a fundamental security layer.

However – just because advice is widespread does not necessarily mean it is well founded. It is therefore worth asking – *is there strong evidence poor password use is a common source of data loss, and if so, what is the best way to solve that problem?* [Short answer: yes, there is such evidence].

Summary of conclusions:

1. Stolen passwords are a significant contributing factor in many cybersecurity incidents.
2. Phishing is the most common way passwords are stolen in a targeted attack, and password policies have only limited capacity to reduce that risk.
3. However, poor password selection and use is a contributing factor in many incidents. Policies can reduce that risk.
4. A password policy will have no benefit unless the majority of network users apply it. This behaviour change requires a structured introduction process and sustained organisational commitment.
5. Passwords alone are an inadequate defence for any important account and should be supplemented with additional or alternative authentication methods.
6. In the early 2000's password construction guidelines were subject to significant research, and this research has informed standardised guidelines published by organisations such as SANS and NIST from that time.[3]
7. The QLS password selection template policy and accompanying materials are consistent with this evidence base and should be promoted as an effective intervention strategy.
8. The QLS template policy emphasises memorability vs complexity. Absent a tool such as a password manager, pass phrases are more likely to result in stronger protection in the real world despite being technically weaker than (say) a completely random 14 character string of letters, symbols and numbers.

Are password policies worth the effort, are they a priority and what should they contain?

The headline question needs to be unpacked:

- How prevalent are attacks on organisations (especially SME professional practices) using compromised user credentials?
- What type of credential compromise is most common and most dangerous?
- To what extent do these attack vectors arise from poor password selection and use vs other factors?
- Does a password policy change user behaviour in the real world?
- If so, what sort of password policies deliver the best cost/benefit trade-off and how should they be implemented?

[1] While specific recommendations vary, a "good" password will usually be between 9-14 characters and contain numbers, upper & lower case and symbols.

[2] Guidance for SME information security from the Australian Cyber Security Centre ("ACSC"), US Department of Homeland Security, US National Institute of Standards and Technology ("NIST") (NIST Special Publication 800-63-B (Revision 3)), and UK's National Cyber Security Centre ("NCSC") all emphasise this control measure.

[3] These systems are the foundation of the strategy recommended by most peak government agencies such as ACSC.

- What complementary strategies & technologies should be deployed to strengthen the user-authentication security layer?
- Would the time and effort spent attempting to influence user password choices be better spent elsewhere (phishing awareness or introducing multi-factor authentication ("MFA") for example)?

One point should be made at the outset: even if one were to conclude that password policies don't reliably reduce the risk of a data security incident in the real world, failing to take what is widely seen as a low cost, basic first step could have liability and reputational consequences if there is a security incident.

Password behaviours in the absence of formal policies

There is very strong evidence that – absent clear direction and enforcement – most people are poor at selecting and protecting passwords. Risky password behaviour includes:

Issue	Prevalence
Use of weak passwords such as "password", "Qwerty" or 123456	24%
Re-using[4] passwords sometimes	67%
Re-using passwords often	50%
Re-using passwords for work accounts and personal accounts	60%
Using publicly available data such as child's name, a birthday, a pet's name	59%

Table A: Prevalence of sub-optimal network user password behaviours.[5]

To what degree do bad password habits translate into data loss?

The correlation between poor password selection / use and economic harm is less clear. Incidents involving compromised user credentials are common, being the primary or significant root cause of 50-65%[6] of all successful information security attacks (81% of hacking related breaches as at 2017).[7] The cost of those incidents is now several billion dollars per year.

Is this the whole story? No. There are numerous ways a criminal can obtain passwords and only some of these arise from a user's poor selection and use. In many post-incident investigations, the exact pathway used by the attacker is only approximated. Once password loss is confirmed as the root-cause of an active incident the same remediation approach is often used no matter how the password was compromised so further analysis is usually not a priority.

Credential related incidents listed in order of prevalence include:[8]

[4] Either entirely or with modification, both of which significantly decrease security; Blake Ives, Kenneth Walsh and Helmut Schneider, 'The Domino Effect of Password Reuse' [2004] 47(4) *Communications of the Association of Computing Machines* 75.

[5] Survey population: US Adults, all categories. Source: *Hosting Tribunal* (amalgamating survey & observational data from Nordpass, Lastpass & Kaspersky). This is consistent with earlier research from the US Department of Homeland Security but shows a higher incidence of problem behaviour than the McAfee password survey project; Yee-Yin Choong, Mary Theofanos and Hung-Kung Liu, 'United States Federal Employees' Password Management Behaviours' [2014] 7991 *NIST Publications.*

[6] Verizon, '2021 Data Breach Investigations Report' (2021). Other sources vary significantly, often in alignment with the commercial interests of the reporting entity. Further review of the literature is required.

[7] Verizon, '2017 Data Breach Investigations Report' (2017). Figure cited 81%. Verizon, '2019 Data Breach Investigations Report' (2019). Figure cited 89%.

[8] For the reasons identified above, the evidence base for assigning risk to the sub-type of credential loss is not strong, which accounts for the high number of "unknown" incident types in Table B. This also places a question mark over the characterisation of other incidents.

Event	Description	Incidence
Phishing	Socially engineered messaging to induce user to supply a password*	36%
Unknown**	Credential theft identified as the primary cause but exact method not identified	30%
Credential stuffing	Recycled passwords (commonly stolen from online shopping or social media accounts) used to compromise work accounts	15%
Brute force/dictionary	Automated targeted attack using millions of combinations, potentially guided by social media analysis of personal data such as birthdays, pet names & sports interests	10%
Scatter-gun	Automated attack on a large number of accounts trying the most common user generated and default passwords	6%
Malicious software	Keylogger or other software which records log on information	3%

Table B: incidence of credential-based attack sub-types[9]

* Phishing is an easy "default" conclusion, so this may be an over-estimate.
** credential stuffing and (to some extent brute force) will often leave very little evidence, so a significant proportion of the "unknown" category may possibly arise from these methods.

Based on these numbers, somewhere between 30 – 40% of credential related attacks (15 – 29% of all cyber-attacks) could be prevented by better password selection and use.[10] While phishing risk is not significantly reduced by a password policy, password reset and recycling rules will reduce the length of time a compromised password (obtained by whatever method) will remain a threat and avoid contagion between a user's personal and work accounts.

Conclusion: At first glance, phishing is the #1 credential loss threat and should therefore be the #1 intervention. However, phishing methods are endlessly variable and a real challenge to address through user education.[11] Further, the choice is not binary – user awareness training to combat phishing can easily incorporate password training so both objectives can be pursued simultaneously.

Do organisational password policies work?

A significant amount of research has been conducted into this question and the answer is clear: *it depends*.

The three legs of the information security tripod are people, process and technology.[12] Measures which rely solely on one leg will be far less effective than a layered system. The "People" and "Process" levers are operated by a combination of education, policy and enforcement.

Appropriate organisational policies are a fundamental element of security culture.[13] Nevertheless, poor[14] policy content and implementation is common.[15] Downloading a standard template document and publishing it on an

[9] Verizon, '2021 Data Breach Investigations Report' (2021). This is dependent on industry sector and enterprise size.

[10] Attacks on smaller businesses are often less targeted and more automated – if the initial attempt fails the criminal may be more inclined to move quickly to the next entity on their list.

[11] Daniel Jampen, Gürkan Gür, Thomas Sutter and Bernhard Tellenbach, 'Don't Click: Towards an Effective Anti-Phishing Training. A Comparative Literature Review' (Research Paper No 10/2020, Human Centred Computer Information Sciences, 2020).

[12] NIST, 'Uses and Benefits of the Framework, *Cybersecurity Framework* (Web page, 8 December 2021) <https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework>.

[13] Neil Doherty, Leonidas Anastasakis and Heather Fulford, 'The information security policy unpacked*',* (2009) 29(6) *International Journal of Information Management*,449.

[14] Common problems include: inconsistent policy & education, the policy is out of date or does not meet the operational needs of the particular organisation.

[15] Danuvasin Charoe, Murali Raman and Lorne Olfman,'Improving End User Behaviour in Password Utilization' (2008) 21(1) *Systemic Practice and Action Research,* 55.

organisations' intranet may tick the box on an ISO compliance form but is not likely to generate real world improvement.[16]

The fundamental difference between "having a policy" and "having a good policy that the majority of network users know about and follow" is a significant problem when comparing intervention strategies. Appropriate content and implementation have a significant impact on outcome.

Conclusion: any password policy is probably better than nothing,[17] but the right policy introduced the right way can make an organisation's data tangibly safer.

So what should a password policy contain?

The objective of a password policy is to ensure that network users:

1. Choose an adequate password (a password with high information entropy);
2. Do not recycle passwords or components thereof, especially between work and private accounts;
3. Do not share or store passwords in a location that can be compromised.

As a general rule,[18] password complexity is inconsistent with the other objectives – long, complex passwords are harder to remember so tend to be recycled more or saved in a phone contacts directory or other easily compromised location.[19]

Pass phrases,[20] especially where only a portion of the word is incorporated, are a more practical way to generate an adequate credential than a random string.[21]

Strong credentials[22] that can resist protracted attempts at brute forcing are generally only required to protect high sensitivity accounts such as:

- high level network or administrator privileges;
- high volume / high sensitivity information;
- financial gateways;
- high customer impact or essential business data;
- email accounts which can be used to reset other passwords.

This entails a choice: the simplicity of a single rule without the need for risk analysis vs the convenience of reserving the strongest passwords for where they are really needed. No compelling research evidence has been identified either way.

The other viable pathway is use of a password manager which can generate and store extremely complex passwords. The two basic approaches are not mutually exclusive.

QLS suggests a dual recommendation: 14 characters as an "adequate" password, 20 characters for a "good" one, with fairly common complexity rules such as caps and numbers. Absent an exceptional memory this necessarily entails either the use of a pass phrase or a password manager.

[16] Neil Doherty, Heather Fulford, 'Do information security policies reduce the incidence of security breaches?' 18(4) *Information Resources Management Journal* 2005, 21-39.

[17] If for no other reason than to ward off negligence claims, reassure clients that your business is not a supply chain risk or keep your insurers happy.

[18] Richard Shay et al, 'Designing Password Policies for Strength and Usability', (2016) 18(4) *ACM Transactions on Information & Security Systems*, 1-34.

[19] Blake Ives, Kenneth Walsh and Helmut Schneider, 'The Domino Effect of Password Reuse' (2004) 47(4) *Communications of the ACM,* 75; Saranga Komanduri et al, 'Of Passwords and People: Measuring the effect of Password composition policies (2011) 11, NIST Publications 2595-2604. While user tolerance for longer passwords has increased over time (presumably due to increased security awareness) the inevitable outcome of increased complexity is reduced compliance with the other policy objectives. This is consistent across demographics and irrespective of the importance users attach to password security.

[20] A pass phrase is a series of random words (not a quote or expression). It can either be used in sequence ButterflySquidApple or as a memnonic to generate the password string: 15 **My Mo**ther **Sa**id **I mu**st **ne**ver **in**terrupt # = 15MyMoSaImunein#.

[21] Mark Keith, Benjamin Shao and Paul Steinbart, 'A behavioral analysis of passphrase design and effectiveness' (2009) 10(2) *Journal of the Association for Information Systems,* 63-90.

[22] 20+ characters including several symbol classes.

Hive Systems publishes a widely cited annual table estimating the time that current attack methods will take to brute force passwords with particular characteristics. The table can be found here.

How should password policies be deployed?

See QLS Guide to cybersecurity policy adoption and deployment.

What complementary strategies and technologies are required to maximise the data protection available from a password policy?

If possible, password policies should be hard-baked into the system, forcing users to employ compliant passwords and blacklisting those with poor characteristics (eg; Password1234567#).23 However this could be time consuming to implement on a small network without centralized management.

Some of the more common complexity / length requirements can be summarised as follows:

GDPR: policy specifying complexity & reset period mandatory. Content of policy not prescribed.

ISO 27001/27002: policy specifying complexity & reset period mandatory. Content of policy not prescribed, system level enforcement of complexity, storage, transmission, selection and cryptography requirement.

PCI DSS: 7 characters, alpha+numeric, 90 day reset with system control to require novelty x 4, no default passwords used, 30-minute lockout, system idle timeout of 15 minutes, cryptography & storage mandates.

NIST 800-53: 8 character minimum, ability to use special characters but not mandatory, prohibited terms dictionary (p@ssword, D0dgers).

PEXA: 8 character minimum, upper/lower alpha + number + symbol

The QLS Password policy & construction guideline template may be found: here.

A quality password manager makes appropriate password selection and use much easier, both at work and at home. Where possible, a business should select and deploy a centrally administered enterprise grade password manager. If that is not an option, staff should be encouraged to download and use a high security system. Many low or no cost quality providers exist. For more details see the QLS Guide to selecting and using password managers.

David Bowles, Special Counsel, Ethics
Queensland Law Society

[23] Shay (n 20) 3.