OCTOBER 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Important Changes to Password Best Practices Guidance

Passwords are an essential cybersecurity tool. Unfortunately, some long-standing password practices recommended by regulators and standards organizations may encourage risky behaviour. Regulators and standards organizations have recently issued updated guidance recommending simplified password practices (e.g. no mandatory regular password changes) to increase password security. Canadian organizations should assess and improve their password practices in light of updated best practices guidance.

The Problem – Risky Behaviour

Passwords are an essential and ubiquitous cybersecurity tool. However, the proliferation of password use and complex password requirements can encourage risky and insecure password practices (e.g. using passwords that are easily guessed, using simple and predictable password creation strategies, re-using the same password for multiple business and personal accounts and keeping insecure records of passwords) that present significant cybersecurity risks.

Password reuse can be a particularly significant problem. For example, an employee's use of the same or similar passwords for both business and personal accounts can allow a cybercriminal to use a compromised personal account password to gain access to the employee's business network account and possibly the entire network. Similarly, a customer's use of the same or similar passwords for multiple online accounts can allow a cybercriminal to use a compromised password for an online account to gain access to the customer's other online accounts. A July 2017 survey found that 81 percent of Americans (and 92 percent of millennials) surveyed use the same password for multiple online accounts, and more than a third (36 percent) use the same password for 25 percent or more of their online accounts.

Guidance – Password Best Practices

Regulators and standards organizations in various jurisdictions have issued helpful guidance regarding password practices to improve security and protect privacy. Many of the recommendations are based on recent research and lessons learned from cyber incidents. Following is a summary of some of the guidance.

1. Password Composition Rules

The practice of requiring passwords that are comprised of obscure characters, capital letters and numbers and are changed regularly has been attributed to the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-63 *Electronic Authentication Guideline* (2004). According to a recent *Wall Street Journal* article titled *The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!*, one of the authors of the Authentication Guideline has acknowledged that the password guidance has been shown to be "largely incorrect".

In June 2017, NIST issued new guidance for authentication processes in *Special Publication 800-63 Digital Identity Guidelines*. The Guidelines recommend allowing long passwords comprised of any characters (including spaces) and without any other composition rules (e.g. mandatory combinations of different character types), so that individuals can use hard to guess passphrases. The Guidelines also recommend authentication processes be designed to reject proposed passwords that are commonly-used, expected or compromised.

The U.K. National Cyber Security Centre (NCSC) recommends a dramatic simplification of password practices at a system level. NCSC's guidance (e.g. *Password Guidance: Simplifying Your Approach*, *Helping end users to manage their passwords* and *Password guidance summary: how to protect against password-guessing attacks*) includes the following recommendations:

- Change all default passwords before deployment.
- Choose a scheme that produces passwords that are easier to remember but harder to guess.
- Use technologies to block (blacklist) the most common password choices.
- Allow users to reset passwords easily, quickly and cheaply.
- Do not allow password sharing.
- Allow users to securely record and store their passwords.

- Reinforce password policies with user training.
- Use technical solutions (e.g. password managers) to reduce the burden on users.
- Use appropriate technical defences (e.g. account lockout, throttling or protective monitoring) against automated password guessing attacks.

2. Mandatory Password Changes

Mandatory, regular password changes are a common practice that was recommended in the original NIST *Electronic Authentication Guideline*. However, recent guidance recommends against mandatory, routine password changes.

Since at least 2016, NCSC has recommended against mandatory, regular password changes. Various guidance documents (e.g. *Password guidance summary: how to protect against password-guessing attacks* and *The problems with forcing regular password expiry*) and blog posts (e.g. *Your password expiry policy may have reached its expiry date*) explain that mandatory regular password changes may harm rather than improve security, because individuals who are required to regularly change passwords often choose passwords that are weak or used elsewhere.

Similar views were expressed by the U.S. Federal Trade Commission's Chief Technologist in the 2016 article *Time to rethink mandatory password changes*.

The recently issued *NIST Special Publication 800-63B Digital Identity Guidelines* (2017) also recommend against mandatory, regular password changes.

3. Privacy Considerations

The Privacy Commissioner of Canada's 2016 *Guidelines for Identification and Authentication* provide important guidance for identification and authentication practices that comply with Canadian personal information protection laws. Following is a summary of some recommendations:

- There is no one-size-fits-all approach to identification or authentication. Each organization must use identification and authentication processes that are appropriate for the circumstances.
- Identify individuals only when necessary and only to the extent necessary, and obtain appropriate consent before identification.
- Authenticate individuals only when necessary and use authentication processes that are commensurate with relevant risks.
- Properly train employees about relevant privacy policies and practices.
- Maintain reliable audit records of authentication transactions.
- Regularly reassess risks and threats, and deploy appropriate risk mitigation measures.

The Privacy Commissioner of Canada's July 2017 News Release provides the following guidance regarding password best practices:

- Avoid passwords that are obvious or easy to guess.
- Use passwords that are eight or more characters.
- If a user needs to record a password to remember it, then the record should be offline and in a secret, secure, locked place.
- Passwords should be supplemented with other protective measures, such as multifactor authentication, when appropriate.

The Privacy Commissioner of Canada's *Self-Assessment Tool* sets out helpful questions an organization may use to assess its password and authentication practices.

4. Password Reuse

In July 2017, the Privacy Commissioner of Canada issued a News Release explaining that it had received several reports of data breaches resulting from the use of valid customer or employee passwords obtained from previous, unrelated breaches. The Privacy Commissioner warned: "There's a simple way for individuals to prevent these types of password reuse breaches: Don't reuse passwords".

The Privacy Commissioner of Canada's July 2017 *Tips for mitigating password reuse risk* provides guidance to help reduce password reuse by employees and customers. Following is a summary of some recommendations:

- Employees:
  - Employees should change work passwords that have been used elsewhere.
  - Employee remote access to networks should be secured using various technological measures, such as multifactor authentication.
  - Employee account access should be monitored for unusual patterns.
- Customers:
  - Customers should be warned against password reuse, and educated about ways to effectively manage password overload.
  - Customer authentication should be commensurate with relevant risks.
  - Layered authentication (e.g. multifactor authentication) should be used for access to sensitive or large amounts of information.
  - Authentication processes should maintain reliable, auditable records of authentication transactions.
  - Measures should be implemented to limit the impact of a compromised password.

The NCSC has also issued *Living with password re-use* to provide consumer-focussed guidance for password reuse.

5. Increased Risk Scenarios

Best practices guidance emphasizes that enhanced-security password practices (e.g. technological measures such as multifactor authentication) should be used for high value or high risk users (e.g. senior executives or individuals with administrator privileges) or in situations with increased risk (e.g. remote access to networks).

For example, NCSC's *Password Guidance: Simplifying Your Approach* includes the following recommendations:

- Give administrators, remote users and mobile devices extra protection.
- Administrators must use different passwords for their administrative and non-administrative accounts.
- Do not routinely grant administrator privileges to standard users.
- Consider using two factor authentication for all remote accounts.
- Never use default administrator passwords.

Summary

Canadian organizations should assess and improve their password practices in light of current best practices guidance issued by regulators and standards organizations. In particular, organizations should: (1) consider simplifying their password practices (including no longer imposing password composition rules or requiring mandatory password changes) and using technology and user education to discourage or prevent risky behaviour (e.g. password reuse) and increase password security; (2) use enhanced-security password practices (including multifactor authentication) in high risk scenarios; and (3) ensure that their password practices comply with personal information protection and privacy laws. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG's Cybersecurity Law Group is available at blg.com/cybersecurity.

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349

Borden Ladner Gervais

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide St W, Suite 3400, Toronto, ON, Canada M5H 4E3
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com