NSW Bar Association Cybersecurity Guidance for NSW Barristers

20 June 2024

NEW SOUTH WALES
BAR ASSOCIATION

NSW Bar Association Cybersecurity Guidance for NSW Barristers

20 June 2024

A- Background

1. This guidance is issued by the NSW Bar Association to assist barristers in protecting against cybersecurity threats.

2. This guidance recognises that barristers' practices differ in a variety of ways, including as to their subject-matter, their scale and the nature and extent of third-party (including client) information held. In addition, some clients may impose requirements on barristers that go beyond the core or additional guidance contained below.

3. The cyber security threats faced by Australian professionals and businesses, including barristers, are liable to change. It is the responsibility of each barrister to consider whether additional steps beyond those identified below ought to be taken having regard to their own personal circumstances and changes in their exposure to cybersecurity threats.

4. A failure to take steps to protect against cybersecurity threats could result in significant harm, including to a barrister's clients, in the event of a cyber attack. Such failures may also, in certain circumstances, constitute a breach of the Barristers Rules and may be unsatisfactory professional conduct or professional misconduct.

B- Core Guidance

5. The following steps are recommended for all NSW Barristers. All NSW Barristers should take *at least* the following steps:

Security updates

- Keep your work devices, apps and software used in your practice up to date with the latest security updates. In many cases, it will be possible to turn on automatic app and software updates. Where automatic updates are not available, regularly check relevant apps and software for security updates.

- Where you are using "legacy software" (ie software that is no longer updated or maintained by a developer), consider shifting to software that is the subject of security updates.

Secure passwords

- Use strong passwords for all devices and accounts used to handle work data. Strong passwords will normally involve at least 8 or more characters, with at least one capital letter, one lower case letter and one special character. The longer the password the better. Alternatively, consider using a type of password known as a "passphrase", which is made up of four or more random words selected by you. Weak passwords (eg 1234, password) should be avoided in all cases.
- Do not use the same password across more than one app or software account. Using a single password across multiple accounts places you at greater risk of a cyberattack; if one site is compromised, your password will be known for every other site you have used it on.

- To keep track of passwords, store them securely. Do not leave them easily accessible. Consider using a "password manager" (eg "1Password") which stores your passwords in encrypted form and can enter them automatically on websites.

- If you become aware that a password has been (or may have been) compromised or if you are hacked, change the relevant password immediately. Failing to update

your passwords, or recycling old passwords, places you at greater risk of cyber attack.

- Do not share your passwords with others. While it may be necessary for some passwords (eg network or computer passwords) to be provided to your clerk or personal assistant, ensure that those passwords are kept securely by them and do not use those passwords across accounts.

Multi-factor authentication

- Turn on multi-factor authentication (MFA) where it is available. MFA means having additional checks in place to prove your identity on an account beyond just a password. For example, you may need a code from an "authenticator app", or in a text message or email in order to log in to an account or app. Authenticator apps running on a mobile phone are the most secure and most convenient. Google and Microsoft offer free authenticator apps for phones and tablets.

- MFA makes it much harder for cybercriminals to access your accounts because they lack the second piece of verification information.

- If you have MFA enabled in respect of a particular service, pay attention to login alerts which look unusual. This is often the only way to help minimise the risk of a compromised account. Do not ever give out the code from an MFA to any other person; anyone who asks for it is probably the cyber attacker trying to get into your account.

C – Additional Guidance

6. The following additional steps may be appropriate for you to take, depending on the nature of your practice and the information and work data held by you. All barristers should consider whether to take these steps.

Security software

- Many computers and devices have in-built security and antivirus software, which will provide a level of protection. You may wish to acquire additional security and antivirus software in order to provide further protection.

- Many computers and devices will run automatically scans to detect malware and viruses. In addition, you may wish to regularly run manual scans of your work devices, both at the time the device is set up and when it is reconfigured.

Access controls

- Exercise caution before providing other persons with access to your work devices, apps and software. If access is required to be given to a person (eg to a clerk or personal assistant), consider confining the nature of the access provided. For example, you might limit access to only your diary, rather than client data.

- Where one-off access to your work devices, apps or software is required (by, for example, an IT professional), supervise that access for its full duration. Where the need for one-off access has ceased, satisfy yourself that the person does not have ongoing access.

Devices

- Where work devices are used outside the home or chambers, take reasonable steps to ensure the physical security of the devices. Avoid leaving work devices unattended in public spaces.

- Where you are provided with USB sticks and/or external hard drives as part of your

practice, only connect them to your work devices if they are from sources you are confident are secure.

- Windows and Mac operating systems have an ability to encrypt hard drives to protect the information on them if the device is lost or stolen. Consider the benefits of full disk encryption where your devices contain sensitive, confidential or privileged data.

- Where you stop using a work device (eg when you upgrade to a new computer, tablet or phone), ensure that it remains physically secure until such time as its contents are permanently and securely erased or deleted.

Data retention

- Modern briefing practices often result in barristers receiving large volumes of data in electronic form. This data is often loaded onto a device or cloud service, and (unlike with paper documents) it is easy to leave it there once a matter completes. That material may be compromised in a successful cyberattack, and files containing personal information or other commercially confidential material can be of significant value to attackers. If access to the material is no longer needed, that risk can be eliminated by deleting the files or moving them to "offline" storage (eg on an external hard disk stored in a secure location).

- When closing a matter, consider moving its files off the cloud. Consider putting aside time to review long-closed matters to delete files that no longer need to be kept, and/or moving them to offline storage. In particular, be mindful of storing data containing "personal information" that is subject to provisions of legislation such as the *Privacy Act 1988* (Cth).

Ensure unattended devices are kept in a secure location

- Ensure that all your devises are secure when unattended, especially overnight. For example, you should lock the screen of your computer and consider whether you need to lock the door to your chambers at the end of the day.

- Be alert to cyber attacks (and attempts).

- Exercise caution before downloading apps or files from the web from sources that you do not know or trust. Many cyber-attacks occur via the unintentional downloading of malware online.

- Be aware that "phishing" attacks may occur through fabricated emails or weblinks that appear to have been sent by a colleague, acquaintance, or business. This is called "social engineering".

- A particularly common phishing attack is a fabricated alert about a bank transaction, Dropbox, Microsoft Onedrive, Amazon transaction, PayPal, an "order confirmation" for an expensive purchase, or login attempt. Some of these will try to use personalisation.

- Be wary of any link or attachment in an email that you were not expecting, even an email from an apparently known and trusted sender. Be wary of replying to such emails (including to "unsubscribe") as this is often used to "harvest" information from you, such as appears in your email footer.

- Take the time to consider and follow recommendations and occasional guidance from Government Agencies, the Bar Association, network operators and reputable software and security agencies.

D – Professional Conduct Considerations

7. While the Barristers Rules do not specifically impose requirements on barristers in relation to cyber security, a range of rules may be engaged in particular cases by a barrister's failure to take appropriate steps to protect against cyber threats. For example:

    - A barrister must not engage in conduct which is prejudicial to the administration of justice: r 8(b)

    - A barrister must not engage in conduct that is likely to diminish public confidence in the legal profession or the administration of justice or otherwise bring the legal profession into disrepute: r 8(c)

    - A barrister must not disclose (except as compelled by law) confidential information obtained by the barrister in the course of practice concerning any person to whom the barrister owes some duty or obligation to keep the information confidential unless certain requirements are satisfied: r 114.

8. While there is no separate requirement for Barristers to receive technology or cybersecurity training, it is reasonable for members of the public to expect reasonable competence to include the appropriate management (including in digital format) of confidential information received by Barristers in the course of their practice to help minimise the risk of disclosure.

9. Unsatisfactory professional conduct includes conduct of a barrister occurring in connection with the practice of law that falls short of the standards of competence and diligence that a member of the public is entitled to expect of a reasonably competent barrister: *Uniform Law*, s 296. In certain circumstances, and having regard to a range of relevant circumstances, a barrister's failure to take appropriate steps to protect against cyber threats may fall within this concept.

10. Professional misconduct includes: (a) unsatisfactory professional conduct, where the conduct involves a substantial or consistent failure to reach or maintain a reasonable standard of competence and diligence; and (b) conduct of a barrister, whether occurring in connection with the practice of law or occurring otherwise than in connection with the practice of law, that would, if established, justify a finding that the barrister is not a fit and proper person to engage in legal practice: *Uniform Law*, s 297. In certain serious circumstances, and having regard to all relevant matters, a barrister's failure to take appropriate steps to protect against cyber threats may fall within this concept.

NEW SOUTH WALES
BAR ASSOCIATION

Selborne Chambers 174 Phillip Street, Sydney, New South Wales, 2000
DX 1204 Sydney **P:** +61 2 9232 4055 **F:** +61 2 922 1149
E: enquiries@nswbar.asn.au