BAR ASSOCIATION OF QUEENSLAND

GUIDELINES FOR CYBER RISK MANAGEMENT

A. INTRODUCTION

Technology and data systems underpin many of the services delivered by barristers and the methods that barristers use to engage with their stakeholders. Within modern practices, barristers will retain significant amounts of sensitive commercial, professional and personal information. The information is highly attractive to malicious cyber threat actors (**Threat Actors**), who may try to access and misuse this information during a Cyber-attack.

Threat Actors will also try to target the accounts and technology devices used by barristers. Once compromised, Threat Actors can then attempt to commit social engineering and financial frauds against a barrister and stakeholders that engage with that barrister.

This guideline outlines how barristers can manage their Cyber Security risks, and the Cyber Security investments that will help barristers reduce the likelihood of a Cyber-attack occurring. The guideline also highlights the importance of barristers carefully considering their individual circumstances and revisiting Cyber Security regularly as the area continues to evolve due to Threat Actors continuously developing new Cyber-attack methods.

B. ABOUT THIS DOCUMENT

The purpose of this guideline is to help Queensland barristers understand their Cyber Security risks and how Cyber Security will relate to their professional and ethical obligations under the *2011 Barristers' Rule,* as amended (**Barristers' Conduct Rules**). This guideline also seeks to highlight the risks that are present to barristers who do not adopt appropriate measures to manage their Cyber Security risks and how Cyber-attacks against barristers may diminish public confidence in the legal profession.

C. COMMON TERMS

Anti-Virus Software – An application that scans a device or endpoint for Malware and removes or isolates the Malware to prevent it causing further harm.

Backup – A copy of digital data, files or programs that are kept in a separate environment or location. A backup can be used to restore and recover the copied data in the event of a Cyber-attack, or system loss event.

Control – A safeguard, process or countermeasure designed to protect an information system and mitigate the risk of a Cyber-attack.

CVSS – The Common Vulnerability Scoring System is a technical standard used to assessing the severity of vulnerabilities that are found in computer systems. Scores are calculated based on a formula and range from 0 to 10, with 10 representing the most severe vulnerabilities.

Cyber-attack – Any intentional attack undertaken by a Threat Actor to compromise a digital environment to access, steal, expose, alter, disable, or destroy data, applications, and other assets.

Cyber Security - The steps, processes and practices that are used to protect applications, technology systems, networks, and the users of technology services from a Cyber-attack and the malicious steps taken by Threat Actors.

Cyber Extortion – A form of Cyber-attack where the Threat Actor compromises a technology environment and then demands an Extortion Payment from the victim.

Encryption – Refers to the process of converting data into a format that can only be read by a user who holds the decryption key.

Endpoint Detection & Response – A cybersecurity tool designed to continuously monitor and responds to threats on network-connected devices such as computers and smartphones. It helps detect suspicious activities, analyse potential threats, and take action to mitigate them.

Exfiltration – The unauthorised copying of sensitive information stored within a technology environment. A part of exfiltration data and records are copied to an external third-party hosting or file server that is typically under the control of a Threat Actor. The Threat Actors will commonly threaten to publish exfiltrated data to cause harm to the victim.

Extortion Payment – During a Cyber-attack Threat Actors will commonly demand that a victim pay money or an equivalent form of security to the Threat Actor. The payment is typically made so that the Threat Actor will restore access to the victim's systems or deleted sensitive data that the Threat Actor has stolen or deleted during Exfiltration.

Firewall – a Control designed to monitor, permit and block incoming and outgoing network traffic based on predetermined security rules. Its primary purpose is to establish a barrier between trusted devices and networks and untrusted external locations and networks, such as the internet, to prevent unauthorised access and protect sensitive data. Firewalls can be implemented using hardware, software, or a combination of both.

IT Support Vendor – A third-party service provider specialising in the management, maintenance, and support of an organisation's information technology infrastructure. This can range from simple help desk support to a full Managed Service Provider or Managed Security Service Provider. These vendors offer a range of services, including troubleshooting technical issues, ensuring network security, managing software updates, and providing user support.

Malware – Malware, short for malicious software, is commonly used by Threat Actors during a Cyber-attack. Malware is often designed to disrupt computer systems and prevent users from being able to access key records and applications.

Multi-factor authentication – a security Control that requires two or more verification steps or proofs of identity to grant access to sensitive data or resources. The first form of verification is typically a username or password, while the second authentication is done via an authenticator application, token, phone or other messaging device.

Phishing – A technique used by Threat Actors to acquire sensitive data, such as passwords, bank details, or payment information through a fraudulent solicitation in communication which may be in email, web site or other form of electronic communication. As part of a Phishing communication the Threat Actor will masquerade as a legitimate business or reputable person to encourage the victim to share sensitive information. Phishing attacks may also come from another victim's account where the Threat Actors have compromised the victim and have access to their email and telecommunication systems.

Ransomware – Ransomware is a form of Malware that is designed to encrypt data and exfiltrate sensitive information stored in technology environments.

Strong Passwords – A strong password typically consisting of a combination of uppercase and lowercase letters, numbers, and symbols that is at least 12 characters long. Passwords of this length and complexity are more difficult for Threat Actors to guess and are more resistant to brute force attacks.

Threat Actor – Threat actors, also known as malicious actors, are individuals or groups that intentionally cause harm to digital devices or systems. Threat actors exploit vulnerabilities in computer systems, networks and software to perpetuate various Cyber-attacks, including Phishing, Ransomware and Malware attacks.

D. WHAT DOES CYBER SECURITY INVOLVE?

Cyber Security is a broad term which encompasses the steps that are taken to protect users, applications, information systems, data, networks and devices from Threat Actors. Cyber Security is an emerging field of expertise and the controls and processes that are adopted to manage Cyber Security risks continue to evolve.

The starting point for examining Cyber Security, is understanding the most common methods that Threat Actors use to commit Cyber-attacks. These methods include :

Social Engineering which involves the exploitation of people by convincing them to take an action or step which will allow the Threat Actor to gain access to a device or technology environment.

Business Email Compromises when Threat Actors access a breached mailbox or email account and pretend to be an employee or third party that has previously communicated with the Cyber-attack victim. Once successful, Threat Actors will impersonate a barrister to conduct further phishing or spam campaigns in an attempt to compromise further victims, including

other barristers, judges, and clients. This can have severe reputational and ethical implications if not detected and remediated as soon as possible.

Third-Party Exposures which occur where a third party is compromised by a Threat Actor and the third party has direct access into the technology environments of another individual or organisation.

Unpatched Vulnerabilities which involve the exploitation of known bugs or weaknesses in programs or systems. Threat Actors use sophisticated automated tools to scan for vulnerabilities, both from within and outside an environment.

Compromised Credentials which occurs when Threat Actors obtain data from previous Cyber-attacks which contains a user's personal information and login credentials. Threat Actors can identify the common password formats and passwords and use these to access an individual's online accounts and services.

Malware which may be installed after a Threat Actor gains a foothold in a technology system and then installs malicious executable code which can damage, disrupt or provide unauthorised access to the Threat Actor.

Many of the practices and approaches that are used to manage Cyber Security are drawn from industry standards and technical frameworks. Within Australia common frameworks and standards used to manage Cyber Security risks include the Australian Signal Directorate's Essential 8 Maturity Model, Dynamic Standards International's SMB1001 Standard and the ISO-IEC 27001 series of Standard. While Cyber Security insights can be taken from these standards, each standard is designed to apply to a broad cross section of industries and organisations, which can make it difficult to directly apply a standard to a particular barrister's individual circumstances.

Whether or not industry standards and frameworks are adopted, Cyber Security should be managed by deploying key Controls across the devices and technology services used by an individual or organisation. These Controls can be implemented directly by the end user or be deployed and managed using the assistance of an IT Support Vendor.

E. DANGERS OF POOR CYBER SECURITY

Cybersecurity is a shared risk and must be managed collectively by chambers and collaborating barristers. Once a Threat Actor has gained a foothold in an environment the Threat Actors will routinely look to exploit other devices and systems on the network and individuals who work within the environment or who have connected devices. They deploy sophisticated scanning, reconnaissance and mapping tools to map the environment, and use technical and social engineering tactics to attempt to move laterally across the environment and gain control of other systems. This means that if a single barrister is compromised, others within the same chambers may also be vulnerable to the Threat Actor.

Cyber Security investments reduce the likelihood of an individual or organisation sustaining a Cyber-attack and help to reduce consequential harms that result from a Cyber-attack. Threat

Actors are constantly attempting and succeeding in perpetrating attacks. In a recent report, the Australian Cyber Security Centre advised that it received over 97,000 notifications of Cyber-attacks against Australian individuals and organisations during the 2022 to 2023 financial year.[1]

Cyber-attacks are regularly conducted against the legal industry and can have devastating effects on barristers and the wider legal community. Barristers falling prey to a Cyber-attack or failing to take adequate measure to protect the data they hold may have ethical implications and may diminish public confidence in the legal profession.

In 2024, Brick Court Chambers suffered a Cyber-attack that resulted in 141 gigabytes of sensitive information becoming publicly available for anyone to download. This included internal documents, court recordings, passports, and sensitive working documents from current and historic court cases. Also in 2024, the Victorian Courts were subject to a Cyber-attack that compromised court recordings going as far back as 2016.

In April 2023, HWL Ebsworth became victim to a Cyber-attack which involved the Exfiltration of approximately four terabytes of data, which equated to approximately 2.2 million files. The data breach exposed a range of sensitive information including legal advice provided to government entities, sensitive personal information, data relating to national security and law enforcement matters, corporate information, and sensitive client records.

In 2022, the UK Bar Council and Bar Standards Board were victims of a Cyber-attack which required them to isolate and disconnect their technology systems to prevent the Threat Actor from causing further damage and data Exfiltration.

Cyber-attacks can also result in business interruption, when Threat Actors deploy Malware and damage data assets they can prevent a technology environment from functioning correctly. Restoring damaged technology environments can take weeks or months, depending on the sophistication of the attack and the quality of the victim's Backup and recovery capabilities.

F. BARRISTERS' CONDUCT RULES

In accordance with Rule 5 of the Barristers' Conduct Rules, barristers must maintain high standards of professional conduct and act with competence and diligence.

Implementing adequate Controls assists with ensuring the continuity of a barrister's practice and protecting the confidential information they hold. This, in turn, prevents the risk of a barrister from contravening the following Rules:

> ***Rule 12*** *A barrister must not engage in conduct which is…*
>
> *(c) likely to diminish public confidence in the legal profession or the administration of justice or otherwise bring the legal profession into disrepute.*
>
> ***Rule 56*** *A barrister:*

[1] Australian Signals Directorate, 'ASD Cyber Threat Report 2022-2023', see https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023.

(a) must seek to ensure that the barrister does work which the barristers is briefed to do in sufficient time to enable compliance with orders, directions, Rules or practice notes of the court…

Rule 108 *A barrister must not disclosed (except as compelled by law) or use in any way 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 such information confidential unless or until:*

(a) the information is later obtained by the barrister from another person who is not bound by the confidentiality owed by the barrister to the first person and who does not give the information confidentially to the barrister;
(b) the person has consented to the barrister disclosing or using the information generally or on specific terms; or
(c) the barrister discloses the information in a confidential setting, for the sole purpose of obtaining advice in connection with the barrister's legal or ethical obligations.

Rule 109 *A barrister must not disclose (except as compelled by law) or use confidential information under Rule 108(b) in any way other than as permitted by the specific terms of the person's consent.*

If a barrister is a victim of a Cyber-attack which makes their systems inaccessible, they will likely be prevented from completing their work in sufficient time and complying with Court directions or orders. A Cyber-attack may also compromise the confidentiality of documents stored on their system.

Implementing the Minimum Cyber Security Controls set out in section G of this document will reduce the likelihood of a Cyber-attack and any potential contravention of the Barristers' Conduct Rules which may result.

G. CYBER SECURITY CONTROLS APPROACH

The most appropriate strategy to manage a barrister's Cyber Security risks will depending on their individual circumstances and the types of technology used across their practice. Given this background it is important that barristers carefully consider which Cyber Security investments will best meet their needs.

To provide guidance on this issue the Bar Association of Queensland has developed recommended:

1. Minimum Cyber Security Controls which should be implemented by all barristers; and

2. Additional Cyber Security Controls that barristers should consider, to determine whether they are appropriate for their individual circumstances.

Minimum Controls

(a) Multi-Factor Authentication (**MFA**)

MFA should be used for access to all email accounts.

Where possible MFA should also be used to restrict access to applications which store sensitive commercial and client information.

MFA is a foundational control that helps ensure that only authorised individuals such as yourself, your secretary, or other support staff can access sensitive files or records. MFA requires a second form of verification, in addition to a username and password. This means that even if a Threat Actor steals a username and password, they cannot access a barrister's confidential information unless they also compromise the second form of authentication. The American Cyber Defence Agency considers that implementing MFA reduces the risk of Cyber-attacks by as much as 99%.[2]

(b) Strong Passwords

Strong Passwords should be used for all devices and accounts that handle working documents, client data, or other sensitive information. A simple way to create a Strong Password is to combine three unrelated words as well as a number and symbol. This creates a strong and memorable passphrase; an example could be "LoudArgumentativeChord1$". This password is easier to remember as it is not a random string of characters and is resistant to many of the brute force methods used by Threat Actors to breach user accounts.

(c) Password Hygiene

Passwords should not be shared with other users or support staff. Each user and support staff should have their own individual passwords and accounts when accessing shared devices, applications and mailboxes.

Passwords should never be shared over email or text. By communicating in this manner, passwords can be unintentionally exposed to a Threat Actor in the event the recipient's email account or device is compromised.

It is also important that passwords are periodically changed and refreshed to reduce the risk of a Threat Actor gaining access to valid credentials. Passwords that are used for key services should be changed when either of the following occur:

i) The user becomes aware that their accounts and password data may have been involved in a Cyber-attack or data breach; or

ii) Every year.

(d) Enable Automatic Software Updates and Patches

[2] Cybersecurity and Infrastructure Security Agency, 'Multifactor Authentication', see https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication.

Tested and approved patches and security updates should be set to automatically update or automatically remind you of when updates are ready. This should extend to all devices which a barrister uses to store confidential client data. Automatic updates and update schedules can either be managed directly by a barrister or managed using an IT Support Vendor. Automatic updates should also be applied within 72 hours of becoming available.

Updates commonly contain patches to severe security flaws that can be exploited even without any user error. Many of these types of vulnerabilities are widely exploited within the first few weeks of being discovered. This means delaying a security update increases the risk of a Threat Actor conducting a successful Cyber-attack. Threat Actors also can use automated scanning tools to look for unpatched devices, which can then be exploited.

Recent improvements in the automatic update processes used for Windows and Mac operating systems have also reduced the risk of updates causing a user to lose unsaved work or being forced to implement an update at an inopportune time. The risk of losing data can be further minimised by saving regularly, using Backups, and working in the cloud.

(e) Anti-Virus Software

All devices which contain client data should have Anti-Virus Software installed to protect the device and client information from Threat Actors and Malware. Anti-Virus Software can often be subject to yearly subscription fees and will need to be renewed periodically. Barristers should ensure any subscriptions remain valid, as Anti-Virus Software will not be effective against new forms of Malware that are developed past the expiry date of a current subscription.

Anti-Virus Software can also be bundled into other products. For example, Microsoft Windows comes with Microsoft Defender, which is a sophisticated anti-virus platform and is included with a Microsoft operating system licence. Mac devices include a similar application called XProtect.

(f) Regular Backups

Backups of important data and client information should be undertaken weekly or monthly, with sophisticated chambers considering daily backups. Backups can either be done manually or by purchasing a Backup storage service. Backups can either be managed directly by a barrister or with the assistance of an IT Support Vendor.

Windows and Mac devices will also both provide small amounts of free cloud storage with OneDrive and iCloud respectively. There are also many other providers who provide Backup solutions such as Dropbox or Google Drive. Barristers should carefully review the terms of their cloud storage solution provider, as the terms of service for personal cloud storage may contain contractual terms relating to intellectual property, privacy, data sovereignty, data ownership and waiver of liability.

Additional Controls

While the Minimum Controls outlined above provide a baseline level of Cyber Security, they may still leave barristers exposed to Threat Actors. To provide a higher level of Cyber Security each barrister should also consider whether the following Controls would also be appropriate for use within their practice.

(a) Unique Passwords

Where possible separate passwords should be used for critical applications or websites. Threat Actors regularly check whether a user's passwords have been exposed in previous data breaches. Where this occurs, the known passwords can be used to attempt to compromise the user using various attack methods such as credential stuffing.

If you would like to check if accounts and passwords associated with your email address have been compromised there are websites available which compare an individual's personal information and email details against data obtaining from previous Cyber-attacks which have been posted onto the dark web.

As remembering many unique passwords is difficult, barristers should consider using password managers. A password manager is an application that saves usernames and passwords for other accounts and websites and can randomly generate Strong Passwords for those accounts. Some popular password managers are LastPass, 1Password, and Proton Pass.

(b) Engaging Specialist IT Support Vendors

IT Support Vendors can provide managed services and assistance to help build and manage a technology environment. IT Support Vendors should also have a good understanding of Cyber Security and can provide assistance with implementing the Controls outlined in this Guidance Document. IT Support Vendors are commonly engaged on a part-time or fractional basis and can also help with day-to-day technology and Cyber Security queries.

Barristers should consider the terms of service of any key technology services which they consume and contracts made with IT Support Vendors . Key considerations include what rights the IT provider retains over the data, what security measures the IT provider has in place, whether any data provided is stored in Australia or overseas, and what responsibilities each party will have in the event that a Cyber-attack occurs.

(c) Personal and Work Device Separation

Where possible personal devices should not be used for work purposes and work devices should not be used for personal purposes. The wider the 'footprint' of a device, the more opportunities for it to be compromised by a Threat Actor. Devices used for social media, personal use of the internet, banking, and other activities of daily life may be more susceptible to compromise as Threat Actors often target these activities to conduct Phishing attacks and to attempt to install Malware on a device. It is also

recommended to avoid letting a spouse or child use a device with access to sensitive client documents or confidential information.

(d) Restrict Microsoft Office Macros

Macros should be disabled for all Microsoft Office Applications as this is a common exploit that Threat Actors use. A compromised word document opened by the barrister or secretary can be used to Exfiltrate data or implant Malware. This has become a standard setting in Microsoft 365, but older versions of Microsoft Office still have macros enabled by default.

Macros can be disabled by opening the 'File' menu at the top of the Microsoft Office application, opening 'Options' from that menu, then opening the 'Trust Center' and selecting 'Macro Settings'. Macros can still be re-enabled if they are required.

(e) Endpoint Detection and Response

Endpoint Detection and Response (EDR) tools should be used for practices or environments where practitioners are working on shared networks and where multiple devices and users access common resources like files, printers, and internet connections. EDR tools consistently monitor and protect devices connected to that network by identifying suspicious behaviour and using analytics to detect anomalies. EDR software quarantine and contain impacted digital and network assets. Examples of EDR software includes Microsoft Defender for Business, CrowdStrike, or Symantec Endpoint Detection and Response. Some Anti-Virus Software also includes EDR capabilities.

(f) Encrypt Data on Laptops and Phones

Encryption of internal storage on a device will protect data stored on the device in the event it is lost or stolen. Most modern devices and operating systems have built in features to allow you to Encrypt laptops and phones. These features can generally be found in device's settings, usually under "Security", "Privacy" or "Device Encryption" options.

Specialist software such as BitLocker (Windows), FileVault (Mac) or other drive Encryption tools can also be used to protect data on your laptop and desktop computer. This protects the confidential information on the laptop if the device is physically stolen or lost, unless Threat Actors also compromise the user's account (username and password) or compromise the decryption key.

(g) Patching Cadence

If automatic updates and automatic patches are not available for key systems, servers or devices, a barrister or their IT Support Vendor should apply the security update manually.

Patches and updates should be applied as part of a regular routine and ideally be conducted at intervals of no more than 3 months. Critical patches that have a CVSS of 8.0 and above should be applied within 14 days of patches or updates being released.

Patches and updates should also include all on premises servers, virtual cloud servers, and any servers provided by external providers such as web servers and mail servers.

(h) Immutable Backup and MFA

An immutable Backup is a copy of data that cannot be changed or deleted after it is created. The immutable Backup is placed in a "read-only" format which makes it difficult for a Threat Actor to manipulate or destroy, because they cannot overwrite the file. This increases the likelihood that the data can be recovered in the event of a Cyber-attack. Most Backup solutions include settings that allow the user to enable "Immutable Backup" or "Immutable Storage" options.

(i) Multi Factor Authentication for Service Accounts, Administrator Accounts and Backups

During a Cyber-attack Threat Actors will typically seek to compromise login accounts that have a high degree of privilege or administrative rights within an environment. If these accounts are compromised, it will become easier for the Threat Actor to install Malware and damage the environment.

To reduce this risk MFA should be used for Service Accounts and Administrator Accounts. Service Accounts are a special type of non-human privileged account used to execute applications and run automated services and processes. Administrator accounts are privileged accounts with high-level permissions that can be used to manage system settings, configurations, installations, networks and system tasks. IT Support Vendors can help barristers identify and manage the Service Accounts and Administrator Accounts that are in place on their environments.

Access to Backups should also be restricted using MFA to reduce the risk of an unauthorised Threat Actor compromising the credentials used to access Backups.

(j) Configure Firewalls for Work Devices

A Firewall helps to reduce the risk of connections between the trusted devices and internal network of your home or chambers, and untrusted external networks. Configuration steps should include installing and updating the firewall, identify network assets and resources that should be protected and establishing access control lists. IT Support Vendors can help barristers configure and manage a Firewall.

H. LEGISLATIVE REQUIREMENTS

Save for the above Conduct Rules, there are few specific legislative requirements that impose Cyber Security requirements or specific data handling practices on Barristers. Presently, most of the requirements in the *Privacy Act 1988* (Cth) only apply to businesses and sole traders that have an annual turnover of over $3,000,000. While the government has indicated that it intends to remove the turnover exemption, it did not include do so in the first tranche of privacy amendments in late 2024. If the turnover threshold is removed in later privacy reforms, barristers may need to comply with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles.

This may then require a barrister to establish or update their privacy policy, report to the Office of the Australian Information Commissioner if a data breach has occurred, ensure the security and availability of personal information held by the barrister through technical controls, and delete personal information after it no longer has a use. This would predominantly affect barristers who work with individuals but would also include documents that include information or opinions about a person such as interviews, submissions related to an individual or witness, and other related information.

I. RESPONDING TO CLIENT QUERIES AROUND DATA SECURITY

In recent years organisations across Australia and globally have become increasingly concerned by the risks that can arise when they share sensitive data and the cyber security expectations that they have for the third-party providers which they rely upon.

This has resulted in many law firms and their clients become increasingly concerned about data security events and data breaches, which can arise from Cyber-attacks. Against this background barristers may find that they are required to provide details of their own Cyber Security investments and strategies, prior to being engaged by a perspective client.

Some law firms and clients may avoid engaging barristers who cannot provide sufficient comfort around their Cyber Security posture.

To best navigate these issues, barristers should understand their systems and be capable of answering questions around how they hold, manage and secure the sensitive data that is within their care, custody or control.

J. CONCLUSION

Cyber Security is not an issue that can be ignored as it is becoming a key issue for governments, legal professionals, and clients. Cyber-attacks can also have devastating impacts for the public and cause long term business interruption and reputational harm. Ultimately, barristers should ensure that they are taking reasonable measures and steps to manage their Cyber Security risks and act in a manner consistent with their professional and ethical obligations under the Barristers' Conduct Rules. These reasonable measures include those noted in section G of this guideline, which are being widely adopted in Australia and seen as minimum standards across many industries. As technology continues to evolve barristers should remain aware of the risks and ensure they are using adequate protection in the future. Failing to take adequate measures can lead to disastrous outcomes for clients, as well as the potential for disciplinary action and costs orders.

K. MORE INFORMATION

For further information, visit:

- Australian Cyber Security Centre website;
- Microsoft Support website to enable device encryption; and
- Apple Support website to enable device encryption.

Version 1.0 – November 2025.