QLS Guide: Cybersecurity risk assessment tool for small law firms

To use this tool: The objective is to decide which star rating best describes the current state of your practice. To achieve a particular star rating you should be able to tick all or most of the items in that column. Once you have determined the rating, check the traffic light colour that applies to that rating. (For example, one star in “Clients” is a yellow). Mark the colour in the far right column. An alternative risk reduction measure can also be coded “green”.

A Red light is a warning, and something that needs to be fixed as a priority. A Yellow rating means there is work to do. Green means that appropriate processes are in place for a small practice with limited resources.

Metric	Level 0 No protection	Level 1 ★	Level 2 ★★	Level 3 ★★★	Our Rating	Comment	Traffic Light
People							
Leadership & responsibility	There is no person in firm management with specific responsibility for cyber and information security (“info-sec”).	Firm leadership has collectively agreed to pursue information security goals.	There is a senior person within the organisation who has assumed personal responsibility to ensure a reasonable standard of information security. That person has undertaken limited self-education.	The leader in the firm with responsibility for cyber and info-sec has set aside time to undertake improvement measures. The firm has prepared a budget and allocated resources to achieve and maintain appropriate cyber and information security measures.		Governance is not an end in itself, but a precondition of good cybersecurity. In very small organisations the test is whether the leadership has enough knowledge and a plan to effect change. 0 = Red ★ or ★★ = Yellow ★★★ = Green	
Training	Employees have never had cybersecurity training.	The majority of Employees have had generic “awareness” training.	Employees have cybersecurity training on induction, generic awareness training, training in organisation policies.	Level 2 plus: Employees have cybersecurity awareness training tailored to their roles, a knowledge of firm information security policies and their own part in implementing these. Training is compulsory and updated periodically.		Training is an essential element of a security culture. “Awareness” training is generic, it is not referenced to your network or your policies. Policies will not be understood or applied unless employees are trained in them. 0 or ★ = Red ★★ = Yellow ★★★ = Green	
Personal devices and networks [Only relevant if employees access firm documents from own devices or at home] [Under review]	Employees have no understanding of security on their personal devices or home networks. There is no BYOD policy governing how personal devices are to be used. We don’t know if employees are using personal devices to work on firm data.	Employees have had training on risks posed by their personal devices. Employees are aware that there is a BYOD policy and have read it as a precondition of BYOD access to firm data.	Level 1 measures plus: Employees have been given limited guidance on implementing personal device security. Employees have installed device security software. Remote devices connect via VPN if any traffic is unencrypted.	Level 2 measures plus: Employees have been given detailed guidance and assistance on implementing security on personal devices and home networks. Employees have installed device security software including remote wipe options. Or BYOD access and security is provisioned using centralised Mobile Device Management options.		Unless you have been very clear on the subject, many law firm staff will take work home and do it on their home computers or pick up email on their phone. Many home networks are very poorly defended. Even the fact that the information is no longer under firm control can be regarded as a “data breach”. Deficiencies in this area are a priority. 0 or ★ = Red ★★ = Yellow ★★★ = Green	
Employee vetting	No reference or background check prior to employment.	Basic reference checks are conducted.	Detailed reference checks and CV checks are conducted.	All “level 2” processes plus: A police and verification of identity check on employment is conducted.		“Insider” information theft and fraud are both reasonably common and extremely damaging when they occur. Dishonest employees often have indications in their history.	

Metric	Level 0 No protection	Level 1 ★	Level 2 ★★	Level 3 ★★★	Our Rating	Comment	Traffic Light
						0 = Red ★ or ★★ = Yellow ★★★ = Green	
Process							
Clients	No warnings are given to clients about communications security.	Generic warning given to clients in retainer documents and initial correspondence. Clients are warned large funds transfers will never be arranged solely via email. Relevant Lexon Risk Pack processes are followed.	Level 1 measures plus: If no Risk Pack applies, clients are given written warnings appropriate to the matter type, backed by reminders at relevant intervals.	Level 2 measures plus: Matter and communication subject types are graded by risk, and in high risk matters: • clients are contacted to discuss security options; and • given appropriate information about information security risks. Clients are warned not to undertake sensitive communication or send high volumes of confidential information via email.		Information compromise at the client end can be almost as dangerous as intrusion into the firm's network. The primary risks are faked funds transfer instructions or the loss of important data (such as identity documents) on route to or from the firm. Solicitors should take reasonable steps to minimise a client's risk of loss. Even if we are not ultimately liable, the firm can be left with a major problem if a client is subject to attack. 0 = Red ★ or ★★ = Yellow ★★★ = Green	
Supply chain	No assessment or consideration of contractor and supplier information security capacity or market reputation. Contractors are chosen primarily on price.	Reputable suppliers and contractors are chosen and assumed to have appropriate information management or vetting processes in place.	Level 1 measures plus: Suppliers specifically address cybersecurity and vetting measures (as applicable) in documentation. Supply contracts contain appropriate information security provisions.	Level 2 processes plus: Key contractors: • can provide specific information to substantiate information security claims; and • can substantiate claimed vetting processes.		This can be difficult for a small firm to control. The most significant mitigation is to assess which suppliers/contractors (such as cleaners, IT contractors, cloud vendors etc) are a critical risk and then check what controls they have in place. 0 = Red ★ or ★★ = Yellow ★★★ = Green	
Email	Email is not encrypted or encryption status is unknown. No training has been conducted on email risks.	Email is automatically encrypted in transit. Incoming attachments are scanned by an appropriate software suite. Employees have a general understanding of phishing and malware. Clients have been warned that email is inherently insecure. Lexon Risk Packs concerning email communication are applied.	All level 1 processes plus: A matter and activity risk assessment has been conducted and incorporated into relevant policy. Employees are trained at least annually on email risks and policies to mitigate them. An alternative or supplementary communication system for high risk data and matters is available.	All level 2 measures plus: Detailed information or guidance provided to clients in high risk matters. Sensitive communication in high risk matters and exchange of high volume or critical data does not occur via email.		Email is a significant factor in over 80% of data loss incidents (lost data storage makes up most of the balance). Email can never be trusted as a source of truth or as a means of conveying highly confidential data without additional protection. Deficiency in this area is a priority. 0 = Red ★ or ★★ = Yellow ★★★ = Green	

Metric	Level 0 No protection	Level 1 ★	Level 2 ★★	Level 3 ★★★	Our Rating	Comment	Traffic Light
Policies	No express policies concerning cybersecurity or information security have been adopted.	Generic policies on the most critical security issues have been adopted.	The firm has adapted generic policies to suit their particular needs, and employees have been given guidance about them.	A comprehensive suite of security policies have been drawn in consultation with individual work units and role based training has been provided. Policies are supplied on induction together with detailed instruction and guidance.		Law firm employees are often good at following policies and procedures, but these need to be explained. An adequate policy that is understood and applied is far superior to an elaborate policy that sits unused. Deficiencies in this area are a priority. 0 or ★ = Red ★★ = Yellow ★★★ = Green	
Where are critical data assets?	The firm has no understanding of where critical information is located.	The firm has a general idea of where critical information is located.	The firm has a detailed understanding of information location and a general understanding of how it is accessed and protected.	The firm has undertaken a data audit. The firm has detailed understanding of information location, all known access methods and controls on how this is managed. All critical data is being backed up regularly.		It is very hard to protect data or ensure it is properly backed up if you do not know where it is. Copies of whole drives are commonly made and forgotten, similarly work-around measures can put critical information in risky locations. 0 = Red ★ or ★★ = Yellow ★★★ = Green	
Risks	The firm has not undertaken an information security risk assessment.	The firm leadership has a general understanding of the broad categories of risk and mode of attack. The firm has considered the severity of that risk to the various information assets it holds.	The firm has analysed the likely risks, mode and consequences of various attacks. A basic strategy to mitigate the highest priority risks has been planned. Policies in response are applied.	All level 2 measures plus: The firm has conducted a basic risk assessment with expert assistance. The outcome is built into the technology, policy and training recommendations.		Few firms have the resources to address all possible threats to information security. Prioritising spending, time and focus requires an understanding of the most likely attack routes having regard to the work you do. Awareness of the problem of limited benefit unless a mitigation strategy is implemented. 0 or ★ = Red ★★ = Yellow ★★★ = Green	
Breach planning	The firm has no data breach plan and has never considered the need for one.	The firm knows where to acquire generic guidance to deal with data breach if and when required.	The firm has an outline data breach response plan and basic guidance is given in the cyber training.	The firm has a detailed cyber breach response plan, template response documents and an implementation team in place.		The first hours and days of a response can make a significant difference to the outcome of an attack for the firm and clients. Even a basic plan can help reduce losses and reputation damage. 0 = Red ★ = Yellow ★★ or ★★★ = Green	
Improvement planning	The firm does not have a plan to assess or guard against cyber risk.	The firm has elected to engage in an improvement process and has obtained the QLS cybersecurity improvement plan most relevant to them. OR an appropriate alternative risk and mitigation plan.	The improvement plan is being implemented. Appropriate resources have been assigned and deployed.	The firm has completed the relevant QLS cybersecurity improvement plan and has continuing effort in place.		A plan is of no use without implementation. Ad-hoc mitigation without a coherent plan will be more expensive and less effective. 0 = Red ★ or ★★ = Yellow ★★★ = Green	

Metric	Level 0 No protection	Level 1 ★	Level 2 ★★	Level 3 ★★★	Our Rating	Comment	Traffic Light
Controls on software used on devices.	There is no security assessment of software, apps or hardware prior to deployment. The firm does not know what is installed on network enabled devices.	Employees have been instructed not to install software, apps, screensavers, browser add-ons nor use third party services without permission. (See also technical measures – application white listing). Internet research concerning safety and suitability of software is conducted before it is used.	Employees have been instructed not to install software, apps, screensavers, browser add-ons nor use third party services without permission. (See also technical measures – application white listing). Vendor documentation as to software security obtained and considered prior to deployment.	All level 2 measures plus: Vendors are given specific questions prior to software deployment and the responses checked by a qualified person.		Many organisations have unauthorised software, apps, or browser add-ons installed on the network. Even basic controls and checks before installing software can reduce the risks. 0 = Red ★ = Yellow ★★ or ★★★ = Green	
Moving data	Employees choose how to move high volume data.	Employees are given direction on how to move high volume data. An option to move high volume data with comparative safety has been supplied.	All level 1 measures plus: There is a system in place to prompt compliance. Contents of missing portable storage can be listed accurately.	High grade encrypted drives supplied with AES-256 capability and FISP certification. Or commercial grade encrypted cloud storage equivalent.		Firms regularly exchange high volume data, and need a way to do so efficiently. However, lost storage and USB devices are a common source of data breaches. Basic policies and some alternatives can ameliorate this risk. 0 = Red ★ = Yellow ★★ or ★★★ = Green	
Backups	Backup state is unknown. Backups are done occasionally or manually.	Backups are run at appropriate intervals using standard software.	Backups are set to run regularly and are checked. All backups are encrypted.	Professionally configured backup regime (GFS rotation or similar) is in place and is checked at periodic intervals. All backups are encrypted.		Ransomware or hardware failure can render large volumes of data unusable. Backups are a very cost effective way to prevent this loss, but need to be set up properly to ensure the copy is not also infected. Backups need to run automatically but also be checked. Backups data is itself a risk and should be encrypted. 0 = Red ★ or ★★ = Yellow ★★★ = Green	
Compliance	There are no policies, so no need to enforce them.	There is no formal enforcement of security policies.	Where a contravention of a policy becomes obvious it is followed up and dealt with.	There is a system of audits and spot checks.		Information security usually involves a trade-off of convenience and speed. Without checks and enforcement, both policies and procedures will fall into disuse. 0 or ★ = Red ★★ = Yellow ★★★ = Green	

Metric	Level 0 No protection	Level 1 ★	Level 2 ★★	Level 3 ★★★	Our Rating	Comment	Traffic Light
Technology							
What can run?							
Workstations	Staff can install software on their work devices if they choose to do so.	Standard user rights do not permit installation of new software.	Level 1 measures plus: Anti-Malware suite prevents blacklisted script from running. Or Application control software manages installation.	Application whitelisting is implemented on all workstations. Whitelisting of executables and software libraries is enforced.		Application whitelisting is the gold standard of software control recommended by the Australian Signals Directorate. This should be discussed with your IT-Pro. In the interim, other measures can make it harder for Employees to (accidentally or deliberately) install software. 0 = Red ★ or ★★ = Yellow ★★★ = Green	
Servers **Under review – whitelisting may be too expensive for many firms**	Application whitelisting is not implemented on all important servers (eg Active Directory, email servers and other servers handling user authentication). Or Whitelisting of executables is not enforced.	Application whitelisting is implemented on all important servers (eg Active Directory, email servers and other servers handling user authentication). Whitelisting of executables is enforced.	Application whitelisting is implemented on all important servers (eg Active Directory, email servers and other servers handling user authentication). Whitelisting of executables and software libraries is enforced.	Application whitelisting is implemented on all important servers (eg Active Directory, email servers and other servers handling user authentication). Whitelisting of executables, software libraries, scripts and installers is enforced.		These measures should be at least discussed with an appropriately qualified consultant.	
Is it up to date?							
Workstations	No updating is applied. Or Non-vendor-supported versions software is used.	Software is set to update automatically and users have been instructed not to prevent updates. Only vendor-supported versions of Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are used.	All level 1 measures plus: Patches for extreme risk security vulnerabilities in Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are applied periodically.	All level 2 measures plus: Patches for extreme risk security vulnerabilities in Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are applied within two weeks.		Hackers and Software developers engage in an endless war. Attackers find a vulnerability in software and the vendor plugs it up. These fixes are then released as “Patches”. If the firm does not download and apply these patches the firm network remains vulnerable. Many successful attacks are executed using vulnerabilities which could have been Patched. (continued below)	

Metric	Level 0 No protection	Level 1 ★	Level 2 ★★	Level 3 ★★★	Our Rating	Comment	Traffic Light
Servers	Server software is no longer supported or this is not known. Software patches are not applied.	The server operating system is up to date and is patched periodically.	Patches for extreme risk security vulnerabilities in web server software, server applications that store important (sensitive or high-availability) data, and other internet-accessible server applications are applied within one month for all servers. Only vendor-supported versions of are used.	Patches for extreme risk security vulnerabilities in web server software, server applications that store important (sensitive or high-availability) data, and other internet-accessible server applications are applied and verified within 48 hours for all servers. Only vendor-supported versions web server software, are used.		Eventually a vendor stops updating software, at which point it should be replaced. Automatic updates are a part of the solution, but a more hands-on management is usually required. 0 or ★ = Red ★★ = Yellow ★★★ = Green	
Macro Settings	Microsoft Office macros can run without limitation.	Microsoft macros not required for regular use are disabled. Employees are aware of macro virus risks and to exercise care when opening office documents.	As for level 1.	Only signed Microsoft Office macros can execute. Microsoft Office macros from the Internet are blocked. Microsoft Office macro settings can't be changed by users. Or only macros required by the firm practice management platform can run.		Macros are scripts used by Microsoft Office documents to automate tasks. They can also be used to create malware that are hard to detect using standard anti-malware suites. Later versions of Office are better at defending themselves against this attack. 0 = Red ★ or ★★ = Yellow ★★★ = Green	
Security settings on?	Web browsers automatically play Adobe Flash content. Or Web browser Adobe Flash settings can be changed by users.	Web browsers use 'click to play' for Adobe Flash content. Web browser Adobe Flash settings can't be changed by users.	Web browsers block or don't support Adobe Flash content. Web browser Adobe Flash settings can't be changed by users. Web browsers block web advertisements and Java from the Internet.	Web browsers block or don't support Adobe Flash content. Web browser Adobe Flash settings can't be changed by users. Web browsers block web advertisements and Java from the Internet. Flash and OLE functionality is disabled in Microsoft Office. Unneeded features in Microsoft Office, web browsers and PDF viewers are disabled.		Adobe Flash and other similar software runs content from websites visited. Security has been historically problematic, requiring high attention to patching and these features being disabled by preference. 0 = Red ★ or ★★ = Yellow ★★★ = Green	
Account privileges?	New accounts are routinely set up with wide data access and privileges. Or Privileged (eg. Administrator) accounts are capable of reading emails and web browsing.	New accounts are routinely set up with wide data access but limited privileges. There is no ongoing monitoring of privileges and access. Role based priviliges are not applied.	Requirements for privileged accounts are validated initially and on an annual or more frequent basis. All privileged accounts are restricted from reading emails and web browsing using policy controls. Duties based privileges are applied.	Level 2 measures plus: Requirements for privileged accounts are validated initially and on an annual or more frequent basis.		When a user account is set up it is given "privileges", or the ability to do certain things on the network. The more privileges a user has, the more damage an attacker can do if that account is compromised. An account should not have any more privileges than is required for the user to do their job. The most privileged accounts should be carefully protected from infection. 0 or ★ = Red ★★ = Yellow ★★★ = Green	

Metric	Level 0 No protection	Level 1 ★	Level 2 ★★	Level 3 ★★★	Our Rating	Comment	Traffic Light
Are operating systems current?	Patches for extreme risk security vulnerabilities in operating systems are not applied or are applied on a greater than monthly basis for any workstation. Or A non-vendor supported operating system version is used.	Patches for extreme risk security vulnerabilities in operating systems are applied within one month for all workstations. Only vendor-supported operating system versions are used.	Patches for extreme risk security vulnerabilities in operating systems are applied within 48 hours for workstations of high-risk users and two weeks for all other workstations. Only vendor-supported operating system versions are used.	Patches for extreme risk security vulnerabilities in operating systems are applied and verified within 48 hours for all workstations. Only vendor-supported operating system versions are used.		Timeframes are under review, however you should discuss the cost/protection trade off of rapid operating system patching.	
Multi Factor Authentication	Multi-factor authentication is not implemented.	Multi-factor authentication is implemented for all key systems (eg VPNs, remote desktops, corporate webmail) when access is requested from a new device.	Multi-factor authentication is implemented for all users using remote access solutions (eg VPNs, remote desktops, corporate webmail). Multi-factor authentication is implemented for all users performing privileged actions. In addition to passphrases, only U2F security keys, physical OTP tokens, biometrics, smartcards, mobile apps, SMS messages, emails and/or voice calls are used for multi-factor authentication.	Multi-factor authentication is implemented for all users using remote access solutions (eg VPNs, remote desktops, corporate webmail). Multi-factor authentication is implemented for all users performing privileged actions. Multi-factor authentication is implemented for all users accessing important (sensitive or high-availability) data repositories. In addition to passphrases, only U2F security keys, physical OTP tokens, biometrics and/or smartcards are used for multi-factor authentication.		Multi factor authentication (“MFA”) (such as the tokens used to generate bank account access numbers) is a mechanism in addition to a password required to gain access to critical information. It is currently one of the best protection-vs-cost trade-offs available. Many vendors and services offer MFA but this needs to be activated. There are differing levels of protection offered by MFA systems. 0 = Red ★ = Yellow ★★ or ★★★ = Green	

Metric	Level 0 No protection	Level 1 ★	Level 2 ★★	Level 3 ★★★	Our Rating	Comment	Traffic Light
Physical protections	USB ports are all operational and accessible, including in public areas. There is no physical security for laptops, backup devices and drives. Not all office areas containing confidential information are secured. No secure document destruction facilities. No access log. No key ledger.	USB ports accessible from reception counter and public areas have been turned off. Laptops and desktops accessible in public areas secured with McKenzie locks or equivalent. Document destruction arrangements in place. Windows auto-play turned off. Adequate after-hours security. Key and access log kept.	All laptops are secured with McKenzie locks or in lockable storage after hours. Desktops in public areas also secured. USB Ports accessible from counter and public areas turned off + port blocker fitted. Unused USB Ports on server fitted with locks. Document destruction arrangements in place backed by training and spot checks. Malware detection suite can scan USB devices prior to granting access. Access control to work areas, key codes renewed periodically. Safe custody in fire resistant storage.	All “Level 2” measures plus: Server physical access restricted. Duplicate key in office safe. Backup storage encrypted and kept in physically secure environment. USB access controlled on all workstations. Safe custody in fire resistant storage. Hard drives of all retired equipment is securely wiped or destroyed.		Not all security is electronic. Basic measures can prevent identity theft or data loss from discarded documents and equipment, targeted attacks using USB ports or incidental data loss from stolen or misplaced portable devices. 0 = Red ★ = Yellow ★★ or ★★★ = Green	
Software protections	Virus protection, malware and firewalls not implemented, not updated, or in unknown state.	Basic virus protection and malware software is in place, up to date and working on computer network and mobile phones. Firewalls operational.	A comprehensive suite of malware and virus protection software is in place on computer network and mobile phones. Firewalls operational and checked periodically.	Professionally installed antivirus and malware suite updating regularly. Firewalls operational and checked regularly, blocking access to unused ports.		Anti-malware suites should be used on all devices with network access, including mobile phones. 0 = Red ★ = Yellow ★★ or ★★★ = Green	