LAW INSTITUTE VICTORIA

CYBER SECURITY ESSENTIALS FOR LAW FIRMS

LAW TECH ESSENTIALS

TECHNOLOGY AND THE LAW COMMITTEE NOVEMBER 2017

CONTRBUTED BY IAN BLOOMFIELD,
MANAGING DIRECTOR, IGNITE SYSTEMS

These are mitigation measures intended to provide a law firm with a minimum level of cyber security. It includes information about the rationale for each measure and implementation guidance.

1. ENFORCED PASSWORD POLICY

Measure – Have a clear password policy that is well communicated and enforced. This should include the requirement to use a password manager.

Rationale – Simple passwords make the hacker's job easy. Even complex passwords that are 5 or 6 characters can be relatively easily cracked using the latest tools available to a hacker. Most people know the importance of using strong passwords, but it is not easy to implement good password practices. If staff are aware there is a simple, clear password policy, and have access to a password manager that makes it practical to implement, there is a much higher probability of compliance.

Guidance

- The password policy should include the following:
  - A minimum standard for password creation:
  - Length: minimum of 16 for any account that stores confidential or personal information, and a minimum of 10 for any other account.
  - Variety: where possible, a combination of lowercase and capital letters, numbers and symbols.
  - Words: no use of dictionary words, including compound words or combinations.
  - Personalisation: no use of names, locations or addresses.
  - Recognition: avoid patterns e.g. sequential numbers or letters.
- Ensure that all staff are aware of their personal responsibilities for following the password policy.
- Wherever possible, require systems to be configured to enforce the password policy e.g. computer user accounts, Office 365.
- Wherever possible, require systems to be configured to enforce an account lockout policy; the maximum number of failed sign-in attempts that will cause a user account to be locked. Use a figure of three to five attempts.
- Avoid requiring the periodic changing of passwords. The latest research has identified that periodic password changes is a significant burden that does not improve password security. Passwords only need to be changed when a compromise is suspected.
- Preferably provide staff with a password manager; they are a minimal cost.

2. EMAIL FILTERING

Measure – Use an email service that provides business grade email filtering.

Rationale – Email is the primary attack path for cyber-criminals; the main way of delivering malware into an organisation. By using a quality email filtering service, you minimise the likelihood of infected or high risk email from reaching a user's inbox, thereby greatly reducing the risk of a cybercrime incident.

Guidance

- The email service should allow for the configuration of spam rules, handling of infected attachments, whitelisting and blacklisting.

3. WEB TRAFFIC FILTERING

Measure – Use an internet filtering service to prevent access to high risk websites, including when laptops are used remote from the office.

LAW INSTITUTE VICTORIA

Rationale – Compromised or malicious websites play a major part in many cybercrime schemes, so blocking access to high risk websites is an essential cyber security measure. Internet filtering minimises the likelihood of a user reaching a compromised or malicious website, thereby greatly reducing the risk of a cybercrime incident.

Guidance

- Use a DNS based web filtering service to block high risk websites. This type of filtering carries out a check of each website being accessed, then blocks access to sites that have malware content or are considered dangerous before anything is downloaded to the computer. Search online for "DNS based web filtering".
- Test if you have adequate web filtering- this is a test website that should be blocked: www.malware.wicar.org

4. SECURITY SOFTWARE

Measure – Protect all computers with business grade security software that includes a firewall, anti-virus and anti-spyware, and keep it updated.

Rationale – Having security software in place on all computers is the final defence if all else fails. Effective security software will greatly reduce the risk of a security breach taking place at a computer level by: blocking the malicious email attachment from executing and doing its nasty work, preventing a malicious download from a high risk website from infecting a computer. Business grade security software has additional features and functionality to deal with a business environment. Security is only as good as the weakest link, and any computer without properly configured and up to date security software puts the whole organisation at risk.

Guidance

- Have a reputable business grade security software application installed on every computer. You can check for suitable products here: www.av-test.org/en/antivirus/business-windows-client
- Do not use free versions; these might be fine for a home user, but they are not suitable for use in a business.
- Make sure the software is setup so that:
  - The signature database is updated at least daily.
  - There is a full scan of all files on the computer at least weekly.

5. TWO-FACTOR AUTHENTICATION

Measure – Use two-factor authentication for access to cloud applications.

Rationale – Cloud based systems do not have the additional layer of security that a computer has when it is connected to a local network and protected by a firewall. The only thing stopping a cyber-criminal getting access to a cloud system is a username and password. Multi-factor authentication adds another layer of security that significantly reduces risk. Two-factor authentication is a form of access control that requires two different types of evidence to verify the user's identity. Typically, what the user knows (password), and a one-time passcode generated by something held by the user (security token or mobile phone app). An everyday example of multi-factor authentication is using a credit card where you swipe the card and also have to enter a PIN.

Guidance

- Use multi-factor authentication for access to all cloud based systems.

6. SOFTWARE UPDATES

Measure – Have arrangements in place so that all computers are kept up to date with the latest software versions as well as any patches or updates that are released by the vendor.

Rationale – Prioritised and timely installation of software updates greatly reduces the likelihood of a computer being at risk from an unpatched vulnerability. Software vulnerabilities are weaknesses, and software providers regularly release updates or patches to 'fix' these vulnerabilities. Vulnerabilities are continuously being identified and these are then exploited by hackers, so computers that do not have the software update or patch installed are at risk.

Guidance

- For Microsoft Windows computers, use Microsoft Update and make sure it is setup to automatically install updates. If you are using Windows 10, then Microsoft updates should be taken care of.
- Keep all of the software on your computer up to date by ensuring all updates and security patches are installed.
- Make sure you get an alert from software vendors when they release updates, then install these promptly.

7. REMOVABLE MEDIA

Measure – Implement a policy for the use and control of removable media. Some examples of removable media are: USB memory stick, memory cards (SD), portable hard drives, and optical discs (Blu-ray discs, DVDs, and CDs).

Rationale – Removable media introduces the capability to transfer and store confidential and personal information as well as the ability to import malicious content. The failure to manage the import and export of information using removable media exposes an organisation to several risks: loss of information (this type of media is very easily lost), introduction of malware, and reputational damage as a result of a data breach.

Guidance

- The removable media policy should include the following:
  - Removable media should not be the default mechanism to store or transfer information. Information should be stored using the organisation's business systems and exchanged using appropriately protected mechanisms, such as encrypted email.
  - Define the types of removable media that can be used e.g. only USB memory sticks supplied by the organisation or purchased new by the person using it.
  - Define the arrangements for using removable media e.g. when connected to a computer, and before use, it should be scanned using up to date security software.
  - Removable media should only be used to store or transfer confidential or personal information as a last resort. Confidential or personal information should always be encrypted if stored on removable media.
- Ensure that all staff are aware of their personal responsibilities for following the removable media security policy.
- Consider the use of a Data Loss Prevention (DLP) solution. This is a system that allows documents to be categorised so that documents containing confidential or personal information can be controlled to prevent them being transferred outside an organisation's systems.

8. OFFICE WIRELESS NETWORK

Measure – Control what devices are able to connect to the office network using Wi-Fi.

Rationale – It is essential to protect an organisation's network, as access to this potentially provides access to everything connected to the network. An organisation should control what devices are connected to its wireless network the same as it controls what is connected to the wired network.

Guidance

- Ensure that any wireless network is configured to enforce WPA2 authentication.
- It is preferable to set up two wireless networks, a 'business' network that allows access to the organisation's internal systems, and a separate 'guest' network that is segregated from the organisation's internal systems and only allows access to the internet.
- Restrict connection to the 'business' wireless network to trusted computers only i.e. computers owned by the organisation, and having a minimum standard of security in place.
- Put arrangements in place for staff to use the 'guest' wireless network to connect phones and other devices that only need internet access. Access to the 'guest' wireless network can also be safely made available to people who are temporarily located at the office.
- Knowledge of the passphrase for the 'business' wireless network should be restricted as much as possible. Ideally only one person needs to know the passphrase and they can input this at the time a new computer is setup to connect to the 'business' wireless network.

9. LAPTOP SECURITY

Measure – Protect files stored on a laptop running a Windows operating system by enabling BitLocker encryption. BitLocker is a full disk encryption feature included with later versions of Windows.

Rationale – Being portable devices, laptops present additional risks, such as being lost or stolen when taken outside an organisation's office. Encrypting the files stored on a laptop so that they cannot be accessed by anyone unauthorised mitigates these risks.

Guidance

- Enable BitLocker encryption at the time a new Windows laptop is first setup for use.

10. REMOTE ACCESS

Measure – If there is a requirement for remote access to the organisation's internal systems, use a secure method for remote access and maintain a register of people who have this access.

Rationale – Remote access arrangements can provide a convenient way for staff to get access to your internal business systems. By its very nature, remote access allows parties located remotely to access your IT systems and so exposes them to risk. In order to mitigate this risk, the method used for remote access needs to be secure, and who has this access needs to be restricted to trusted parties.

Guidance

- Best practice is to use a Virtual Private Network (VPN) for external remote access. A VPN is a method used to provide a secure encrypted link between two remote systems that are connecting via the internet.
- There are different types of VPN, and the recommended type is Layer 2 Tunnel Protocol with Internet Protocol Security, better known as L2TP/IPsec.
- Restrict remote access to staff that require it and maintain a record of who has remote access.
- Ensure that disabling remote access accounts is included as part of staff departure procedures.

11. BACKUP

Measure – Use an automated daily backup of all important business files that are stored by the organisation's internal (on premise) systems.

Rationale – Daily backup of all important business files makes it possible to quickly and simply recover files in the event they become corrupt, go missing or are accidentally overwritten. Storage off-site is essential so that the integrity of the data is maintained at all times, and not subject to events or incidents that occur 'on-site'. Backup is a significant component of a disaster recovery capability.

Guidance

- Backup all important company files daily, anything less frequent than this will greatly increase your risk in the event you need to recover files.
- It is essential that the backup process is automated; you will not remember to do it consistently every day.
- The backup data has to be stored off-site at all times. The backed up data will be of no use if there is an incident that takes out the source computer and the device storing the backup e.g. fire, theft, water damage.
- Preferably back up to the cloud. Using a reputable cloud storage solution mitigates against the risk of data corruption or loss that exists with locally stored data.
- It is essential that the backup arrangements provide for retention of past versions (a minimum of 3 is desirable), and retention of deleted files (a minimum of 3 months).

12. DISASTER RECOVERY PLAN

Measure – Have a documented disaster recovery plan in place, with specific procedures detailing what actions are required to be taken to enable a resumption of business operations in a timely manner following a disaster, such as loss of critical data, failure of critical applications, failure of critical IT infrastructure, or prolonged loss of internet.

Rationale – A recovery plan will help an organisation respond effectively if an incident or crisis impacts IT systems and prevents normal operations. A good disaster recovery plan that is effectively implemented will reduce the recovery time and minimise losses in the event of a disaster event.

Guidance

- The plan should identify a range of potential disaster scenarios, and then outline arrangements for dealing with each of these. It should include:
  - Details of key resources and contact details, equipment and staff required to be involved.
  - Procedures and arrangements to recover your internal IT systems.
  - Recovery time objectives.
  - Checklist of things to do; notify staff, advise insurance company etc.

LAW INSTITUTE VICTORIA

13. TRAINING AND AWARENESS

Measure – Ensure all personnel have an awareness about the importance of cyber security, and are provided with cyber security training.

Rationale – Staff play an important role in maintaining the cyber security defences of any organisation. Despite the best levels of cyber security, cyber-attacks can still be successful if all staff are not aware of their role and maintain vigilance.

Guidance

- Provide structured training that outlines the importance of cyber security, highlights the important role of staff in maintaining cyber security defences, and focusses on the practical measures they can take to contribute.
- Create a risk-aware culture and do not simply rely on awareness training.
- Refer to the Law Council of Australia 'Cyber Security Training Toolkit'.

14. CYBER INSURANCE

Measure – Have a cyber insurance policy in place.

Rationale – There is no way for an organisation to be protected against all possible cyber threats, and there will always be some risk of a cyber incident impacting an organisation's business operations. Cyber insurance is an insurance product that covers the policy holder against internet related risks and information technology infrastructure risks. In general, a cyber insurance policy will provide cover for one or more of the following in relation to a cyber incident: direct losses, indirect losses and/or any post-attack expenditure such as hiring computer forensic experts, credit-monitoring services and communication managers.

Guidance

- Cyber insurance products are relatively new and still evolving, so seek professional advice from an insurance broker.

15. ASSESS YOUR CYBER SECURITY RISK

Measure – Carry out a periodic review to assess the adequacy of the current cyber security arrangements.

Rationale – Cyber security needs to be measured like any other business activity, so that you can gauge how effective it is, and identify areas for improvement. A good cyber security regime, by its very nature, has to be continually improved and enhanced to combat the ever changing cyber threats.

Guidance

- A senior manager, preferably a law firm principal, should have specific responsibility for cyber security governance.
- The person responsible for cyber security should make use of the publicly available resources on cyber security to learn and understand the basics of cyber security relevant to law firms.
- Consider hiring a consultant or cyber security firm.

RESOURCES

Law Council of Australia - Cyber Precedent:
www.cyberprecedent.com.au

Stay Smart Online:
www.communications.gov.au/what-we-do/internet/stay-smart-online

SCAMwatch:
www.scamwatch.gov.au

The Australian Signals Directorate (ASD) - Strategies to Mitigate Cyber Security Incidents:
www.asd.gov.au/infosec/mitigationstrategies.htm

Australian Cybercrime Online Reporting Network (ACORN):
www.acorn.gov.au

iDcare (non-profit national identity support service):
www.idcare.org

DATE OF ISSUE: 22/11/2017 **CODE:** WEBFORM