the global voice of
the legal profession®

Cybersecurity Guidelines

By the IBA's Presidential Task Force on Cybersecurity

October 2018

Task Force Chair

Simon Walker, Chair of IBA Online Services Committee, UK

Task Force Members

Anurag Bana, Legal Policy & Research Unit, UK

Sophia Adams Bhatti, Bar Issues Commission, UK

Nazar Chernyavsky, Technology Law Committee, Ukraine

Natasha Chiumya, Bar Issues Commission, Zambia

Luke Dembosky, Cyber Security Practice Lawyer, USA

Bruno Lobato, Law Firm Management Committee, Brazil

Monty Raphael, Criminal Law Committee, UK

Tshepo Shabangu, Bar Issues Commission, South Africa

Meg Strickler, Criminal Law Committee, USA

Graham Wladimiroff, Corporate Counsel Forum, The Netherlands

Valentina Zoghbi, Regulation of Lawyers Compliance Committee, UK

Contents

Introduction

Law firms hold large volumes of valuable personal and commercially sensitive information about their firms, employees, case information and clients. This makes law firms of all sizes a highly attractive target for cybercriminals.[1] Breaches of data security can have devastating legal, financial and reputational consequences for a law firm's clients and business, as well as the law firm. As such, it is critical that firms have effective cybersecurity technologies and processes that focus on protecting the confidentiality, integrity and availability of sensitive data.[2]

The threat of large-scale cyberattacks against law firms is a real risk. It has been reported that attackers have targeted law firms because they hold valuable commercial information and are regarded as 'weak links' because they do not usually take cybersecurity as seriously as their clients[3] or do not have the financial capabilities to invest in efficient technologies that protect the firm from cyberattacks. Global law firms have been the subject of targeted attacks by hackers attempting to acquire insider knowledge ahead of major business negotiations and mergers and acquisitions (M&A).[4] While smaller law firms commonly believe that they are less likely to be a victim of cybercrime,[5] experts have suggested that hackers target small businesses, including law firms, because they usually have lower cybersecurity defences due to a lack of financial and human resources.[6] In 2015, it was estimated that up to 50 per cent of small businesses had been a victim of a cyberattack and 60 per cent of those who suffer a significant cyber breach go out of business within six months.[7] Such attacks will continue with increasing sophistication and frequency.[8] Consequently, it is essential that law firms of all sizes are aware of cybersecurity threats and have policies and procedures to counter such threats.

This report forms part of the International Bar Association's (IBA's) ongoing work on cybersecurity. The IBA Presidential Task Force on Cybersecurity (the 'Task Force') has the objective of: producing a set of recommended best practices to help law firms: to protect themselves from breaches of data security; assisting their ability to keep operations running if a breach of data security or ransom attack does occur; giving their clients the best possible assurances that their data is protected; and helping protect the reputation of the profession. It will do so by establishing a dialogue with practitioners and experts, both in the legal profession and external bodies, such as information technology (IT) suppliers and cybersecurity consultants. It will take a practical approach, including segmenting the market by financial capacity. The concepts in this report are designed to be easily understood by all lawyers, although some recommendations will require the law firm to call on at least some technical support for assistance. Just as lawyers have to learn new subjects for their work, often with the help of outside experts, they also need to do so here in order to protect their clients and business from cybersecurity threats.

There are many resources that provide information on cybersecurity; some are listed in Appendices A to C and I. The Task Force has assumed that all large law firms will have implemented cybersecurity strategies. Accordingly, while these guidelines are relevant for all law firms, they are particularly relevant for the following:

- single practitioners;
- small firms: up to 20 employees;
- medium-sized firms: from 21 up to 40 employees; and
- intermediate-sized to large firms: from 41 employees.

Indeed, firms of these sizes may face greater exposure to the risk of a security breach as they are less likely to have the infrastructure to protect themselves, unlike larger firms.

We recognise that not all of the recommendations that we make here are applicable, or applicable to the same degree, to solo and small firm practitioners, who may not, for example, see much benefit in a particular recommendation or have the scale of network operations to warrant its use. We therefore include, in Appendices D and E, detailed lists of the same recommendations with suggested applicability based on firm size and the type of issue.

These guidelines can be categorised into the following three broad areas:

1. technology;
2. organisational processes; and
3. staff training.

This report discusses each of these categories in turn.

Chapter 1: Technology

Regardless of a law firm's size, security vulnerabilities in technology can have detrimental effects on its legal practice. As such, it is critical that law firms employ up-to-date and efficient technologies to sufficiently protect the firm's data. Our goal is to convey the security concepts which follow rather than immerse you in the technical details. You will need to work with an IT professional to implement these principles; however, it is important that you know to ask about them and whether – and how – they are being put in place for your firm's protection.

Firms should implement a layered programme of technical defences to mitigate the risk of a cyber incident, including the following:

- **Keep system software updated.** The software that runs your network will often require updating through patches. It is very important to make these updates in a timely manner because they usually fix vulnerabilities that the programmer has found in the code. This is particularly so for law firms that are using legacy systems due to historical factors, such as mergers or even the arrival of a new lawyer. Your IT support should handle firm-wide patching, as opposed to leaving it up to individual lawyers and staff. We encourage you to ask them about the following points:
    - Purchase business-grade antivirus and email filtering software (often bundled).
    - Ensure operating system updates (eg, Windows and Mac OS X) are applied as soon as practicable to mitigate the risk of cybercriminals exploiting vulnerabilities. When updating systems, be cautious and only download updates from trusted sources (eg, Windows' official website). The software should be updated when new versions are released.
    - Ensure that firmware updates are applied not only to individual computers but also physical devices, such as modems and routers.
    - For critical business systems, software updates should be installed and monitored by trained IT or cybersecurity professionals.
    - Autoscan all email attachments – do not leave it up to users.
- **Implement endpoint protection.** The computers and other internet-connected devices that have access to your network are known as 'endpoints'. As they are the gateway in and out of your network from the internet, it is extremely important that they are protected and monitored. We encourage the following:
    - Implement 'endpoint' protection to ensure all interconnected devices that are part of the firm's network comply with the firm's cybersecurity standards.
    - Endpoint protection includes both antivirus software that is designed to identify and stop malicious code (malware), as well as firewalls that filter certain types of network traffic to protect your systems and log the traffic, enabling you to monitor and investigative suspicious traffic.

- Configure the settings of the default macro functions of Microsoft programs, such as Word, Excel and PowerPoint, so that macros from the internet are blocked, and allow only macros from controlled trusted locations and/or digitally signed macros.[9]

- **Use secure internet connections.** Cybercriminals may intercept personal or sensitive information by attacking unsecured Wi-Fi connections (eg, public Wi-Fi locations such as airports and coffee shops). Ensure that devices used to access the firm's network do so using a secure internet connection, including by implementing the following:

  - If staff work remotely (eg, at home, at a client's office and while travelling on business), ensure that the internet connection used is secured through a virtual private network (VPN)[10] and not an unsecured public Wi-Fi network. A VPN connection is an encrypted, virtual tunnel back to your network, and is easily established by ordinary users with a simple software application that your IT support can show them how to use.

- **Secure web browsing and email.** Emails and web browsing (surfing) are the main and most successful attack vectors used, which means they are the most common communication pathways that hackers exploit. You should discuss with your IT support using one or more of the following defences:

  - Deploy at the network's perimeter:

    – a web filtering system to restrict and log web access and to prevent downloading of unwanted content;

    – gateway antivirus/anti-malware;

    – sandbox security, which is a mechanism for separating running programs, to reduce exposure to zero-day attacks, which are unknown vulnerabilities in software; and

    – deep package inspection (DPI) for analysing certain traffic for content that you may not want to come in to or go out of your network.

  - Browsers must always:

    – be updated;

    – have endpoint security solution plug-in and popup blockers enabled;

    – have autocomplete and autofill features disabled; and

    – have the content filter feature enabled, if available.

  - Disable internet access from servers and computers that do not need it.

  - Do not operate on free web-based email accounts (eg, Gmail and Hotmail). Reputable paid web-based services[11] are recommended as being appropriately secure.

- **Implement data retention, loss recovery capability.** Data is critical to a law firm's business. Yet data becomes a liability if, as a few examples, you collect data you do not need, you keep large volumes of email in your inboxes or you make it easy to email a file that contains a large volume of data. One email compromise (something rather common) or an email sent by an employee of a large data file can become a significant incident. A data retention policy sets out a strategy for reducing these risks. Similarly, if data is compromised in a cyber incident, then it is essential that it can be restored. Data recovery capability is therefore also extremely important. In light of these considerations, we recommend that you consult your IT support about the following:

    - Implement automatic deletion or archiving of emails and files older than designated dates that you establish. You may need these items for later reference or to meet legal requirements, and you can do that by archiving them in a separate and more tightly secured data repository. Similarly, if lawyers need an older email for an ongoing case, for example, then they can also move a copy of the email to a separate data file specific to that case.

    - Implement database backup technology that automatically backs up data daily. Cloud-based backup services are a highly common and secure backup solution. It is important that firms consider the type of cloud-based backup services they use. For example, OneDrive and similar services only protect against local device failure or theft of the device. If local data is deleted or encrypted (ransomware), then these changes will be replicated (possibly very quickly) to the cloud-based service. Some services, such as Dropbox for Business, allow for the storage of multiple copies of files going back in time, which should allow firms to recover from deletion or ransomware attacks. In addition, it is imperative to read all the fine print from third-party (cloud) vendor contracts/policies to ascertain compliance requirements, and, more importantly, the language regarding security protection.

    - If practicable, also keep on-site and off-site backup copies of data. Give attention to off-site storage's physical distance from the main site. Do not store it too close so that it can be compromised, but do not store it too far away so that it affects restoration time. Keeping periodic backups that are no longer connected to the network is important to allow recovery from a ransomware attack.

    - Consider configuring your system to block the ability to email or otherwise transmit files that contain large volumes of data without certain approval. Your IT support can assist in establishing these types of data loss prevention (DLP) measures.

- **Encrypt data and devices.** Encryption refers to making electronic files unreadable to individuals who do not have the encryption password or key to unlock them. Data in storage may be encrypted or data in transmission may be encrypted (eg, a VPN creates an encrypted, virtual tunnel for the secure transmission of files when an employee is working remotely). Encrypting entire devices, as well as sensitive files, is an extremely important approach to reducing cyber risks. Please consult your IT support about implementing the following steps:

    - Encrypt sensitive stored records and data so that only users with the encryption key or password can access the information.

    - Require encryption on all laptops, tablets and other mobile devices that can store or transmit sensitive data.

- Attempt to limit sensitive data to only the devices/employees that need it.

- **Enable remote erasure.** The loss of a laptop or other mobile device that contains a law firm's data is a common problem with potential for significant liability. Where the device is encrypted (as discussed above), risk is greatly reduced, if not eliminated. Another tool to ensure data on a lost device is not exploited is to erase or wipe the device remotely:

  - Consider installing software that remotely erases sensitive data and/or the entire content of a device. The software will only be able to remotely erase data/content once the device reconnects to the internet, but this will protect confidentiality in the instance of a breach of cybersecurity when a device is lost or stolen, or upon the termination of employment.

  - Consider a mobile device management (MDM) solution, which is a security software solution used by IT support, that can be installed on employees' business or personal mobile phones to secure email, contacts and other types of data.

- **Ensure that the cloud computing provider is secure.** If using cloud computing, it is very important to consider the security features used by the provider. Top cloud computing providers, such as Google, Microsoft and Amazon, are recommended as cost-effective and secure options.

  - When assessing which provider to use consider the following:[12]

    – Does the cloud computing provider physically operate in or outside the law firm's own jurisdiction? Client data should be stored in the jurisdiction in which the firm operates because many jurisdictions allow third parties (notably, government authorities) to review their records (eg, search and seizure laws may apply), which could compromise a client's confidentiality and ability to claim client legal privilege. The question of what happens if data is not stored in the same jurisdiction as that in which the firm operates is something that you should consider from a legal standpoint.[13]

    – What security policies and measures have been implemented by the provider?

    – Has the cloud computer provider obtained information security accreditations, such as ISO 27001?

    – Is the data stored on the cloud encrypted?

    – What authentication procedures are used to access the data stored on the cloud? Is it possible to set up multi-factor authentication processes?

    – Does the provider regularly back up data? What methods of data retention and restoration does the provider use?

    – Carefully read all aspects of the provider's policies and procedures. Where possible, draft a cloud policy that is customised to address the firm's specific needs.

- **Strictly manage access control.** Access control refers both to the rights that you grant certain individuals (administrators) to access all or a portion of your network and particular resources and files it contains. Consider the following steps to reduce risks related to the misuse or exploitation of access controls on computers, systems and networks:
    - Keep administrative accounts (ie, those that have access beyond that of a normal user) reduced to a minimum.
    - Identify elevated access needs and use specific administrative profiles with reduced privileges.
    - Each administrator should have its own account.
    - Restrict access to documents and assets to only users who need it to conduct their professional duties.
    - Promptly terminate the access of employees who depart the firm so that a former employee cannot further access your network remotely and so that hackers do not discover unused accounts available to them.
    - Prevent unauthorised devices from connecting to the network. Consider deploying MAC filtering/restriction on ports of network's switches/routers (may suit best smaller firms) or implementing IEEE 802.1x ('dot1x') on the network (may suit best larger firms). Remember to keep an updated inventory of authorised devices.
- **Create robust network segmentation.** A network with only a perimeter defence and not divided into separate segments means that a hacker who gains access to one portion gains access to the entire network. Discuss with your IT support how to create divisions or rings of security within your network to make it difficult for a hacker to move laterally within your network to reach your most valuable data:
    - Use a segmented virtual local area network (VLAN) to control and restrict access to critical assets. Place them on a separate VLAN with firewall filtering, and control users' access.
- **Implement audit logs.** Monitoring what is and is not occurring within your network on an ongoing basis is important, both to spot suspicious activity early and to identify unused accounts that a hacker could use to its advantage:
    - Audit system, user and application accounts on a frequent basis and disable any account that has no business need.
    - Subject to the law firm's budget:
        - Implement a security information and event management solution (SIEM), which is a software solution that collects logs and events of different sources throughout the network to detect suspicious activity that can compromise corporate data security.
        - Monitor events in real time, generate logs and analyse them periodically to understand what is happening or what has happened in the firm (eg, monitor insider behaviour to identify suspicious activity).

- At a minimum, logging tools should be configured to send alerts automatically whenever pre-defined suspicious activity occurs (eg, security group changes, mass file copy, export or erasure).

- **Consider application whitelisting/blacklisting.** Your network has a foundational software programme (typically a Microsoft or Apple operating system) onto which are added various application software programmes (apps) that perform specific functions. Apps often have code vulnerabilities that pose a security risk in themselves, and must be evaluated and updated on an individual basis. Rather than allowing individual users to install their own apps on your firm devices, discuss the following with your IT support:

  - consider installing systems that will allow only certain types of applications to run (a whitelist) and/or prevent others from running (a blacklist).

- **Secure mobile devices.** There has been a huge increase in mobile device usage, both personal bring your own device (BYOD) and corporate devices, to conduct professional activities. Mobile devices are an integral part of the legal workplace. Smartphones, laptops and tablets are essential for staff and client communication, but they contain both valuable personal and commercially sensitive data. As noted above with respect to the importance of using encryption, this presents a number of cybersecurity risks if the device is lost or stolen, the operating system is faulty or the device provider's IT procedures and policies fail to adequately protect sensitive data. In addition to encrypting mobile devices, consider the following additional steps to reduce these risks:

  - Implement a strict mobile access and BYOD policy that clearly defines the conditions and limits of using mobile devices to conduct business affairs.

  - Deploy a centralised MDM solution to protect corporate data on the go. If possible, prefer solutions that separate user's personal data from corporate data, which is kept in a secure (encrypted) logical container and managed by corporate IT staff.

  - If a personal device is used in any way for business purposes, separate personal and firm data:

    – Firm data must be held and accessed in a sandboxed environment (ie, an isolated environment to perform the testing and running of applications without affecting the main operating system), which will be difficult to achieve if an MDM solution is not used.

    – Define mandatory security settings to ensure a secure working environment (eg, strict password protection, password expiration, lock automatically after a certain time and device encryption).

- **Secure devices that retain data.** Mobile storage devices such as flash or thumb drives present risks both because of the potential loss of the data that they store and because they can become infected with malware that is then transferred to your network when the drive is plugged into a networked computer. Consider the following to reduce these risks:

  - Flash drives or memory cards are an easy way to store, back up and transfer data. Removable devices such as these should be virus scanned and generally used with extreme caution because they could be infected with malware.

- These devices should be kept securely to prevent theft or loss.
- When used, these devices should be encrypted.
- These devices should also be subject to the firm's cybersecurity policy, and the policy must include a procedure for the secure disposal of such devices.
- Firms may consider limiting/blocking the use of removable devices, such as flash drives, at work to prevent the risk of a malware infection.[14]

Chapter 2: Organisational processes

The vast majority of successful cyberattacks are due to human error. It is not possible to prevent all attacks; therefore, organisational processes are crucial in defining how the law firm's activities, roles and documentation are used to mitigate the risk of a cyberattack. Processes should assess the firm's cybersecurity risk profile, identify sensitive and valuable data, and enforce cost-effective strategies to mitigate cybersecurity threats. Cybersecurity should be supported by a clear governance structure, which is actively maintained by the partners and senior managers of the firm. As these concepts are much less technical, and more familiar to lawyers and other non-IT personnel, we have provided less background on these points and more specific practical advice for firms.

Organisational processes that a law firm should consider implementing include the following:

- **Implement strong username and password management along with multi-factor authentication:**
    - Implement strong username and password requirements. Complex passphrases are recommended (eg, '50%like2sleepunder@'), but at a minimum, a combination of uppercase, lowercase, digits and symbols are encouraged (eg, SundaY100%). Automatically require users to change their passwords regularly: every three months is fairly common.
    - It is very important to implement multi-factor authentication that requires users to prove their identity through a second method.
    - Encourage the use of a password manager.
    - Ensure that passwords are not used across multiple systems.
    - For one-off registrations into a system, make up a password of random characters and then use the password reset option if you ever need to return.
- **Allocate roles and define responsibilities:**
    - Staff must understand their roles and responsibilities to ensure cybersecurity and manage associated risks.
    - If practicable, the firm should have a designated cybersecurity officer who enforces the firm's cybersecurity policies.
    - It may also be useful to designate particular roles, such as privacy officer, to particular staff members in order to ensure compliance with local data protection laws, for example, law firms with more than 250 staff who handle data of European Union residents must comply with the General Data Protection Regulation.
- **Identify sensitive data and implement protection protocols:**

- Identify sensitive data (eg, personal information, client information, information about the firm, designs, forecasts, formulas, practices, processes, records, reports, documents, third-party trade secrets and any other information subject to contractual or legal protection) and consider who creates it, where it is stored and with whom it is shared.[15]
- Implement special procedures, which should be regularly reviewed, so that the protection of this information is ensured.

- **Conduct cybersecurity risk assessment and periodic system testing:**
  - Identify the firm's benchmarks: what are you comparing the firm to?
  - Consider additional protections for the firm's finance team.
  - To conduct a cybersecurity risk assessment, firms should:
    1. identify the firm's information assets connected to the network, such as a database containing a large volume of sensitive client information, or the human resources database with personal data of your partners and staff;
    2. identify threats: internal and external, accidental and malicious;
    3. identify system vulnerabilities;
    4. consider third-party service providers' access to and responsibility for data;
    5. if possible, engage external threat assessors;
    6. consider the likelihood of an incident; and
    7. consider the financial, legal and reputational impact that an incident would have.
  - What is the state of the firm's technical, procedural and legal protections?
  - Where does the firm need to go to get to an acceptable level of protection?
  - Repeat the risk assessment process periodically (suggested once a year).
  - Do not advertise defences publicly.
  - In addition to a risk assessment, the firm should consider more frequent testing in the form of vulnerability assessments (to search for weaknesses in the firm's technical defences), compromise assessments (to search for existing breaches of the system), and penetration testing (to use a forensic vendor to attempt to hack the network and thereby identify potential gaps to address).

- **Implement a cybersecurity policy document that aligns with identified risks and has minimum standards:**
  - Implement a layered programme of technical defences (ie, strong usernames and passwords, multi-factor authentication, antivirus and malware protection, network segmentation, regular back up of data, data encryption (Pretty Good Privacy (PGP)/Gnu Privacy Guard (GPG) encrypted

attachments[16]), regular updating and patching software, and protection of physical devices (encryption) and premises).

- Develop a data retention policy that reduces exposure, consistent with the technical data retention measures discussed above.
- Take measures to identify security risks and breaches, including by implementing an outbreak alert system to ensure that the right people in the firm are notified quickly.
  - Train all personnel.
  - Obtain insurance coverage.
  - The policy document should be widely circulated, readily accessible, consistently followed, and periodically reviewed and updated.

- **Develop business continuity plans:**
  - Segment system backups carefully; practice restoration of files from backups.
  - Develop system resiliency when the main network is unavailable.
  - Identify means of alternative communications outside the network.
  - Ensure that paper copies of your cyber response plan are maintained in the event that the network is unavailable.
  - Consider backup plans to replace or substitute for key vendors who might experience their own disruption from a cyber event.
- **Develop and test a comprehensive incident response plan (IRP):**
  - List the name and emergency contact information of the members of the core team of responders, including, where appropriate, representatives from legal, IT, information security, communications, human resources, operations and client relations, depending on the size and nature of the firm. This team becomes the 'computer security incident response team' for the incident.
  - Clearly explain the designated roles and responsibilities for the responders, and include a clear and useable incident triage approach that escalates non-routine incidents for higher-level and cross-functional review by the core team addressed above. Routine incidents should be handled by IT, which should periodically report on trends in the number and types of attempted attacks.
  - Include contact information for external counsel, an outside forensic vendor, a public relations firm (to assist with reputation management) and any other outside experts that the firm is likely to need when responding to an attack.
  - The generally accepted phases of an IRP are:
    1. preparation;
    2. identification;

3. containment;
4. eradication;
5. recovery; and
6. lesson learnt.

- Track the phases of the response:
  - The response team should meet to evaluate the response and identify and document any information that could be beneficial in a future incident.
  - Document the root cause of the incident, business impact and steps taken in response.
  - Continue monitoring these factors and task individuals with specific responsibilities.
  - Learning from the incident is vital. Technical controls should be improved, the IRP should be refined, and monitoring and testing should continue.
- Test the IRP and core team in a live, simulated training exercise periodically, or at least twice a year, and make adjustments to it based on observations from the exercise.

- **Evaluate legal and regulatory obligations:**
  - Understand and comply with what is required of law firms in your jurisdiction, both legally and by your regulator regarding data protection and breach notifications to data protection authorities, regulators, clients and third parties.
  - Legal and regulatory obligations should be included in the IRP. In addition, consider the jurisdictions of the third-party contractors that your firm engages with who may hold data in an offshore location (eg, the General Data Protection Regulation for companies with an appropriate nexus to the EU).
  - Create a decision tree or notification matrix to allow the firm to identify obligations quickly if the need arises.
- **Implement vendor and third-party service provider risk management:**
  - Before they are appointed, where practicable, conduct due diligence on all vendors and third parties that handle/store firm data or have access to the firm's systems.
  - Assess all contractual obligations with vendors and third parties, and to the extent possible, require vendors and third parties to adhere to minimum cybersecurity standards. When reviewing contracts, firms should consider the following:
    1. What are the firm's business requirements?
    2. Conduct a risk and compliance analysis.
    3. Is there scope for negotiation?

4. Who is responsible for investigating a data breach that affects your firm's systems or data?

5. Who is responsible for notification of a data breach as required in the jurisdiction?

- Develop adequate controls and monitoring for vendor and third-party access to systems.
- Consider sharing criteria for suppliers with other law firms.

- **Conduct training and testing:**
  - Require regular cybersecurity awareness training of all employees using nationally accredited trainers.
  - Require specialised training updates for IT and information security personnel.
  - Undertake penetration testing and other practical threat assessments (eg, active phishing campaigns) to test the firm's security and response at least once a year.
  - Conduct periodic vulnerability scans and compromise assessments.
- **Consider cyber liability insurance:**
  - Even if law firms implement the best cybersecurity technologies and processes, firms will still have some level of risk exposure.[17]
  - Law firms should assess their risk exposure as outlined and take out adequate cyber insurance as part of the firm's overall cybersecurity risk mitigation strategy.[18]
  - Cyber liability coverage can help a law firm to cover the costs related to a data breach, including privacy breach, notification expenses, litigation, loss of income, regulatory fines and penalties, and other expenses.
- **Participate in cybersecurity information sharing:**
  - Consider participating in an information-sharing system with similar businesses or other organisations (eg, governments, bar associations and cybersecurity companies)[19] to benefit from shared cybersecurity threats and experiences, and in accordance with any local regulatory requirements.
  - Consider what cyberthreat sharing is available through your national and local law enforcement.

The Center for Internet Security (CIS) Controls™ has produced a list of controls that span both the technology and organisational process sections. These are set out in Appendix F, with suggested applicability based on firm size and the type of data at issue. More information on these controls can be found at **www.cisecurity.org/controls**.

Chapter 3: Staff training

People, due to lack of knowledge or inattentiveness, are usually the weakest link in cybersecurity, which is a fact that cybercriminals exploit. Various types of cyberattacks are designed to appear legitimate but contain malicious links that can obtain sensitive information, such as usernames, passwords and credit card details, are commonly used by hackers because it is more efficient than breaking into a computer's security defences.

For this reason, it is critical that staff understand the common forms of cyberattacks and receive training on how to deal with such attacks. Staff should be educated on the applicable cybersecurity policies, procedures and guidelines of the firm. Staff induction, onboarding, and further education and training provided periodically should all include cybersecurity and cyberattack information sessions to maintain awareness. Where practicable, staff should also be tested by a phishing email campaign with an inert link to monitor organisational compliance. This will help to establish a cybersecurity-conscious culture in law firms, which creates a strong first line of defence.

Staff training should cover the following:

- **What cybersecurity is:**
    - Staff should learn that cybersecurity is the state of being protected against the criminal, unauthorised or negligent use of electronic data, as well as the measures taken to achieve this.
    - Staff should learn that a cyberattack can be both overt (eg, an attempt by an attacker to manipulate, disrupt or destroy a computer network or the information contained within that network, often with the effect of compromising national security or business profitability) and covert (eg, theft of data).
- **Why cybersecurity is important:**
    - Staff should be aware that cybersecurity is important because cyberattacks are becoming increasingly sophisticated and frequent. Simultaneously, the data stored in databases, including those of law firms, is becoming more valuable.
    - Staff should be aware that a lawyer's duty of confidentiality is of paramount importance and breaches of cybersecurity may have legal implications if confidential information is revealed.
    - Staff should also be aware of the reputational and economic risks associated with breaches of cybersecurity.
    - Staff should be trained in how to respond to a cyberattack to mitigate the risk of further loss.
    - Staff should become extremely familiar with the firm's IRP, particularly regarding what types of things to report and to whom.

- **Examples of common threats:**

  Staff should be aware of different types of cyberattacks they are likely to face while working at a law firm, including the following:

  - malware:
    - malicious software such as viruses, worms, Trojan horses, spyware and adware;
  - ransomware:
    - ransomware encrypts or locks valuable data and cybercriminals demand payment for the encryption key to restore access to data;
  - phishing/spear phishing/whaling emails:
    - phishing is an attack contained in legitimate-looking emails, which may have links infected with malware or links that attempt to gather personal and financial information from recipients;
    - spear phishing and whaling are targeted forms of phishing;
  - denial-of-service (DoS) attacks:
    - cyberattacks designed to overload devices with requests with the intention of making them crash and become unavailable;
  - digital identity theft;
    - digital identity is the body of online data information that uniquely describes an individual, organisation or electronic device. It includes unique identifiers, such as an email address, username and password used to prove a person's individuality;
    - cybercriminals might use phishing emails and malware as methods of stealing personal and financial information;
    - cybercriminals might pose as senior employees within a firm by hacking or spoofing their email account and convince someone with financial authority to make a payment;[20]
  - zero-day exploits:
    - vulnerabilities in software unknown to those interested in mitigating the vulnerability (eg, vendor of the software) and able to be exploited by cybercriminals who discover them first.[21]

- **Essential cybersecurity tips and advice:**

  Staff should be taught the following key messages:

  - Do not click on links you do not recognise.
  - Challenge and enquire: do you need more information; does the enquiry/instruction appear usual or uncharacteristic in terms of the sender?

- Protect your personal data.
- Be aware of where you are sending your data.
- Create complex passwords, protect passwords and change them regularly, do not reus passwords across multiple systems and do not share passwords with colleagues.
- Use multi-factor authentication.
- Do not use public/free Wi-Fi – personal hotspots are safer.
- Be aware of the risks of working from home with extended family/friends having access to the same network.
- Be alert and watch out for common characteristics of phishing/spoof emails (eg, poor or odd spelling, emails that ask for personal or financial information and offers that seem too good to be true).
- Use VPN and dongles (small, removable devices that have secure access to wireless broadband) when travelling.
- If you are concerned about security when travelling, use your phone rather than your desktop.
- When travelling, do not remain logged on to the internet longer than necessary.
- Ensure that you only use apps from a reputable source.
- Uninstall apps you are not using.
- Understand the permissions you are granting to apps (eg, tracking your location and access to your contacts or camera).
- Use a strong, well-regarded browser. Google Chrome is the strongest in industry tests.
- Report all phishing/spear phishing to the person designated to deal with cybersecurity concerns, even if the email is sent to your personal account rather than work.
- Have good awareness of cybersecurity breach trends and attacks.
- It is best to avoid using the consumer versions of public services from Dropbox, Google and so on for sharing business content. If there is a requirement to use these services for any purpose, then it is strongly advised to use the business versions for enhanced data security and support.
- Adopt the practice of having a regular data clear out. Do not retain data or share it (eg, in Dropbox) for longer than is necessary given its purpose, and remove shared access to data when it is no longer needed.
- Be aware of the security implications of using personal devices for professional matters. If practicable, consider requiring staff to encrypt attachments they email if they contain a significant volume of sensitive data.

- Turn on your browser's popup blocker. A popup blocker should be enabled at all times while browsing the internet.
- Check for 'https:' or a padlock icon on your browser's URL bar to verify that a site is secure before entering any personal information.
- Do not use public phone chargers to avoid the risk of 'juice jacking'.

For a guide on the minimum levels of awareness that your staff should have on cybersecurity training, see Appendix G. For a more detailed resource on how to provide staff with cybersecurity training, see Appendix H.

For an example of a cybercrime awareness campaign that law firms can implement in their environment, see that prepared by LexisNexis, which can be found at **www.lexisnexis.com/uk/lexispsl/practicecompliance/document/393739/5CTY-7851-F189-118W-00000-00/Cybercrime_awareness_campaign_for_law_firms**.

APPENDIX A: Bar Association resources

For further information and resources on cybersecurity reading material, see the following:

- Australia: Law Council of Australia[22]
- Canada: Canadian Bar Association[23]
- China: All China Lawyers Association[24]
- Europe: Council of Bars and Law Societies of Europe[25]
- Germany: German Bar Association[26]
- South Africa: Law Society of South Africa[27]
- United Kingdom: Law Society of England and Wales[28]
- United States: American Bar Association[29]

For an overview of the cybersecurity guidelines available in the above jurisdictions see **www.ibanet.org/Document/Default.aspx?DocumentUid=8B58AEA5-FF20-49B8-B021-2B29CFCC1B0E**.

APPENDIX B: Government resources

- Australia: Australian Cyber Security Centre[30]
- Commonwealth: Commonwealth Cyber Declaration[31]
- Europe: EU International Cyberspace Policy[32]
- New Zealand: National Cyber Security Centre[33]
- UK: HM Government Cyber Aware,[34] National Cyber Security Centre (NCSC)[35] and the NSCS Cyber Essentials[36]
- US: National Institute of Standards and Technology[37]

APPENDIX C: Corporation and organisation resources

- Google Safety Centre[38]
- International Organization for Standardization[39]
- McAfee Threat Center[40]
- Microsoft Office Micro Secure[41]
- Norton by Symantec[42]
- SANS Institute[43]
- Sophos Knowledge Center[44]
- Wombat Security Awareness Resources[45]

APPENDIX D: Technology by firm size

1	Keep system software updated	E	E	E	E
2	Implement endpoint protection	E	E	E	E
3	Use secure internet connections	A	D	E	E
4	Secure web browsing and email	E	E	E	E
5	Implement data retention, loss recovery capability	A	D	E	E
6	Encrypt data and devices	A	D	D	D
7	Enable remote erasure	D	E	E	E
8	Make sure cloud service provider is secure	A	D	E	E
9	Strictly manage access control	O	D	E	E
10	Create robust network segmentation	O	O	D	E
11	Implement audit logs	O	O	D	D
12	Consider application whitelisting/blacklisting	O	A	D	D
13	Secure mobile devices	E	E	E	E
14	Secure devices that retain data	D	D	E	E

O – Optional; A – Advised; D – Desired; E– Expected

APPENDIX E: Organisational processes by firm size

1	Implement strong username and password management along with multi-factor authentication	D	D	E	E
2	Allocate roles and define responsibilities	O	A	D	E
3	Identify sensitive data and implement protection protocols	E	E	E	E
4	Conduct cybersecurity risk assessment and periodic system testing	A	A	D	E
5	Implement a cybersecurity policy document that aligns with identified risks and has minimum standards	O	A	D	E
6	Develop business continuity plans	A	A	A	D
7	Develop and test a comprehensive IRP	A	A	D	E
8	Evaluate legal and regulatory obligations	E	E	E	E
9	Implement vendor and third-party service provider risk management	A	A	D	E
10	Conduct training and testing	D	D	E	E
11	Consider cyber liability insurance	A	A	D	E
12	Participate in cybersecurity information sharing	A	A	D	D

O – Optional; A – Advised; D – Desired; E– Expected

APPENDIX F: Security controls by firm size*

1	Inventory of authorised and unauthorised devices	A	A	D	E
2	Inventory of authorised and unauthorised software	O	A	D	E
3	Secure configurations for hardware and software on mobile devices, laptops, workstations and servers	A	A	A	E
4	Continuous vulnerability assessment and remediation	A	D	E	E
5	Controlled use of administrative privileges	A	D	E	E
6	Maintenance, monitoring and analysis of audit logs	O	O	A	A
7	Email and web browser protections	E	E	E	E
8	Malware defences	E	E	E	E
9	Limitation and control of network ports, protocols and services	O	A	A	D
10	Data recovery capability	A	D	E	E
11	Secure configurations for network devices	A	E	E	E
12	Boundary defence	O	A	D	E
13	Data protection	E	E	E	D
14	Controlled access based on the need to know	A	D	E	E
15	Wireless access control	D	E	E	E
16	Account monitoring and control	O	A	E	E
17	Security skills assessment and appropriate training to fill gaps	A	A	D	E
18	Application software security	O	O	O	D
19	Incident response and management	O	O	A	E
20	Penetration tests and red team exercises	O	O	E	E

O – Optional; A – Advised; D – Desired; E– Expected

* Produced by The Center for Internet Security (CIS) Controls TM

APPENDIX G: Awareness and training programme

1	Password management awareness.	E	E	E	E
2	Multi-factor authentication on all business and personal accounts.	D	D	D	E
3	Awareness of the dangers (both cyber and ethically) in the use of social media.	E	E	E	E
4	Physical access control: Training on the importance of only allowing authorised personnel to physically access a building. Within the building, access to server equipment should be limited to essential IT staff only. An environment should be created whereby staff members are encouraged to challenge persons that they do not know.	E	E	E	E
5	Logical access control: Computer systems should operate to a standard of least privilege.	D	D	D	E
6	Where appropriate, all portable devices should be fully encrypted. This includes hard drives, USB flash drives, memory cards and optical media. If encryption is not available, then password protected ZIP/RAR files provide an alternative.	E	E	E	E
7	Staff should be encouraged to report suspicious activity on their computer, such as unexpected windows or applications launching, independent mouse movement and unsolicited emails.	E	E	E	E
8	Staff should not click on any links or open any attachments to an unsolicited email. However, rather than simply deleting the email, the organisation should have a mailbox to which suspicious emails can be forwarded (without being opened). This allows the organisation to develop email intelligence, including analysis on why certain emails were not detected by preventative security software.	A	A	D	D
9	Staff should be made aware of when they will be legitimately prompted (after clicking a link) to enter their login credentials.	A	A	A	A
10	Active phishing campaigns should be conducted as a training and educational exercise.	A	A	D	D
11	Tips and reminders about confidential information and policies, such as information security, clean desk policy, BYOD device policy, remote working and removable media policy, document retention policy, MDM policy, privacy policy and social media policy.	A	A	D	D
12	Policies should include protocols on the use of web-based email and storage systems (eg, Dropbox, OneDrive, Gmail and Yahoo! Mail).	A	A	D	D

13	Mobile phones are a potential vulnerability for an organisation. As a guide, staff who use their personal mobile devices for business purposes should ensure that a minimum passcode length is six digits, remove wiping capabilities should be turned on, Apple iOS devices should be configured to wipe after ten unsuccessful login attempts, backups to computers should be encrypted, memory cards (if applicable) should be encrypted, and application and operating system updates should applied as practicable.	E	E	E	E
14	Contractors and third-party suppliers due diligence.	E	E	E	E
15	Awareness raising of current threats and warning signs.	D	D	D	E

O – Optional; A – Advised; D – Desired; E– Expected

APPENDIX H: Cybersecurity staff training

Cybersecurity refers to the protection of electronic systems to maintain the confidentiality, integrity and availability of data. While it is common to consider an external attacker as the greatest threat, it is equally important to consider that internal staff, contractors and third-party suppliers can intentionally, accidentally or negligently cause data loss and damage to systems.

It is recommended that an organisation's staff receive training in the following key areas as well as any organisation-specific training that may be required.

Password management	Training should be provided on the importance of good password management. This should be reinforced as applicable to both business accounts and personal accounts (to reduce social engineering attacks). The following general rules may assist: • Passwords should not be recorded on paper and attached to computer equipment. • Passwords should not be shared between users. • Strong passwords should be used. This should comprise numbers, upper and lower case letters, and special characters. Depending on the organisation's network policy, Windows password rule complexity may be insufficient (eg, Sunday1 meets the complexity rules). Staff should be encouraged to use passphrases such as '50%like2sleepunder@*' . • Personally identifiable information such as dates of birth, postcodes, children's or pets' names, should be avoided. • Password reuse, that is, using the same password across multiple systems, should be avoided. Ideally, a password manager should be used where one only needs to remember the master password and the application generates and inputs the rest. • When a password is required to enrol in a system or make a one-time or rare purchase, consider making up a random one-time series of characters and then using the password reset feature if subsequent access is required. • Strongly encourage users to have separate passwords for business and private accounts.
Multi-factor authentication	Multi-factor authentication should be activated on all business and personal accounts. Staff should be made aware that attackers target personal accounts to gather intelligence and to send phishing emails to colleagues for social engineering attacks. Staff should be provided with how-to guides to implement multi-factor authentication on the most common applications, such as LinkedIn, Gmail, Yahoo!, Facebook, Instagram and Apple iCloud.
Social media	Staff should be aware of the dangers (both cyber and ethically) in the use of social media. Social media provides a valuable source of intelligence for potential attackers, including details of potential clients, colleagues and suppliers. Staff should also be trained in the dangers of posting any material to social media accounts (eg, photographs) that could provide a would-be attacker with information about the physical layout of a building.

Physical access control	Training should be provided on the importance of only allowing authorised personnel to physically access a building. Within the building, access to server equipment should be limited to essential IT staff only. An environment should be created whereby staff members are encouraged to challenge persons that they do not know. Staff members must make sure that their access/security cards are kept safely so that no one can use them to access the building. They must also not exchange their security cards with other staff members. Staff should bring old devices that may contain corporate data to IT to be forensically wiped or physically destroyed.
Logical access control	Computer systems should operate to a standard of least privilege. On this basis, staff should only request access to systems and data that they need access to. They should be warned of the dangers of accessing (browsing) systems and data that they do not need access to. Where appropriate, all portable devices should be fully encrypted. This includes hard drives, USB flash drives, memory cards and optical media. If encryption is not available, then password protected ZIP/RAR files provide an alternative.
Suspicious activity	Staff should be encouraged to report suspicious activity on their computer, such as unexpected windows or applications launching, independent mouse movement and unsolicited emails. Staff should not click on any links or open any attachments to an unsolicited email. However, rather than simply deleting the email, the organisation should have a mailbox to which suspicious emails can be forwarded (without being opened). This allows the organisation to develop email intelligence including analysis on why certain emails were not detected by preventative security software. Staff should be made aware of when they will be legitimately prompted (after clicking a link) to enter their login credentials. Active phishing campaigns should be conducted as a training and educational exercise.
Policy awareness	Staff should be aware of the following policies, if applicable, the reason for their implementation and the implications of not following them: • appropriate use of IT systems • BYOD device policy • document retention policy • working from home policy • MDM policy • privacy policy • social media policy These policies should include protocols on the use of web-based email and storage systems (eg, Dropbox, OneDrive, Gmail and Yahoo! Mail).

Mobile phones	Mobile phones are a potential vulnerability for an organisation. As a guide, staff who use their personal mobile devices for business purposes should ensure the following: • a minimum passcode length should be six digits • remote wiping capabilities should be turned on • Apple iOS devices should be configured to wipe after ten unsuccessful login attempts • backups to computers should be encrypted • memory cards (if applicable) should be encrypted • application and operating system updates should applied as practicable. Where possible, the organisation should develop and educate staff on a BYOD device policy. Subject to the size of the organisation, an MDM solution may also be appropriate.
Contractors and third-party suppliers	Staff should be made aware of the risk that poorly validated contractors and third-party suppliers can have to the organisation. Staff who engage contractors and third parties should be encouraged to thoroughly review the security credentials of all external parties before being allowed to access IT systems and before sending organisational data to them. All contractors and third parties should be monitored if they are provided with access to the data holdings of the organisation. Unless absolutely essential, contractors and third-party suppliers should not be given administrative-level access to the network.
Continued training	Security awareness training should be delivered on a regular basis. Continued training and the development of a 'cyber aware' culture is paramount to mitigating the ongoing cyberthreat.

APPENDIX I: Endnotes

1 See, Camilla Hodgson, 'Law firm cyber breaches could result in huge thefts and insider trading' *Business Insider UK* (London, 19 October 2017) http://uk.businessinsider.com/cyber-crime-law-firms-vulnerable-2017-10, accessed 15 June 2018.

2 Jill D Rhodes and Robert S Litt, *The ABA Cybersecurity Handbook* (2nd edn, American Bar Association 2017).

3 Chloe Smith, 'M&A hack attack on 48 elite law firms' *The Law Society Gazette* (London, 4 April 2016) www.lawgazette.co.uk/practice/manda-hack-attack-on-48-elite-law-firms/5054524.article, accessed 15 June 2018; Nicole Hong and Robin Sidel, 'Hackers Breach Law Firms, Including Cravath and Weil Gotshal' *Wall Street Journal* (New York, 29 March 2016) www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504, accessed 15 June 2018.

4 Chloe Smith, 'M&A hack attack on 48 elite law firms' *The Law Society Gazette* (London, 4 April 2016) www.lawgazette.co.uk/practice/manda-hack-attack-on-48-elite-law-firms/5054524.article, accessed 15 June 2018; Nicole Hong and Robin Sidel, 'Hackers Breach Law Firms, Including Cravath and Weil Gotshal' *Wall Street Journal* (New York, 29 March 2016) www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504, accessed 15 June 2018.

5 See Cert-UK, 'Cyber threats to the legal sector and implications to UK businesses' www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-threats-to-the-legal-sector-and-implications-to-UK-businesses.pdf, accessed 15 June 2018.

6 Mark Smith, 'Huge rise in hack attacks as cyber-criminals target small businesses' The Guardian (London, 8 February 2016).

7 See the testimony of Dr Jane LeClair, Chief Operating Officer, National Cybersecurity Institute at Excelsior College, before the US House of Representatives Committee on Small Business (22 April 2015) http://docs.house.gov/meetings/SM/SM00/20150422/103276/HHRG-114-SM00-20150422-SD003-U4.pdf, accessed 15 June 2018.

8 See n 2 above.

9 See National Cyber Security Centre, Government Communications Headquarters, 'Macro Security for Microsoft Office' www.ncsc.gov.uk/guidance/macro-security-microsoft-office, accessed 15 June 2018 and Australian Cyber Security Centre, 'Microsoft Office Macro Security'.

10 See National Cyber Security Centre, Government Communications Headquarters, 'End user devices: VPNs' 1 August 2017 www.ncsc.gov.uk/guidance/end-user-devices-vpns-1, accessed 15 June 2018.

11 Eg, G Suite by Google Cloud https://gsuite.google.co.uk, accessed 15 June 2018.

12 See National Cyber Security Centre, Government Communications Headquarters, 'Implementing the Cloud Security Principles' www.ncsc.gov.uk/guidance/implementing-cloud-security-principles, accessed 15 June 2018.

13 See Brief of the Council of Bars and Law Societies of Europe as Amicus Curiae in Support of Respondent, *United States of America v Microsoft Corporation*.

14 Australian Small Business and Family Enterprise Ombudsman, Australian Government 'Cyber Security: The Small Business Best Practice Guide' http://asbfeo.gov.au/sites/default/files/documents/ASBFEO-cyber-security-research-report.pdf, accessed 15 June 2018.

15 See n 2 above

16 PGP is used for signing, encrypting and decrypting texts, emails, files, directories and whole disk partitions, and to increase the security of email communications. GPG is a free software replacement for PGP.

17 See n 2 above.

18 See The Law Society of England and Wales, 'Cyber insurance guidance for law firms' 10 October 2016 www.lawsociety.org.uk/support-services/practice-management/cybersecurity-and-scam-prevention/cyber-insurance-guidance-for-law-firms, accessed 15 June 2018 and Association of Corporate Counsel, 'Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information' March 2017, item 12 www.acc.com/advocacy/upload/Model-Information-Protection-and-Security-Controls-for-Outside-Counsel-Jan2017.pdf?_ga=2.193324781.1506201640.1512572020-1373712223.1512572020, accessed 15 June 2018.

19 See, eg, the Cyber Security Information Sharing Partnership (CiSP) www.ncsc.gov.uk/cisp, accessed 15 June 2018.

20 See n 6 above.

21 See n 2 above.

22 See http://lca.lawcouncil.asn.au/lawcouncil/cyber-precedent-home, accessed 15 June 2018.

23 See www.oba.org/Professional-Development-Resources/Cyber-Security-in-Law-Firms, accessed 15 June 2018.

24 See www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm, accessed 15 June 2018.

25 See www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommentations/EN_ITL_20160520_CCBE_Guidance_on_Improving_the_IT_Security_of_Lawyers_Against_Unlawful_Surveillance.pdf, accessed 15 June 2018.

26 See https://digital.anwaltverein.de/de/news/details/das-bea-in-der-praxis-neue-broschuere-zum-elekronischen-rechtsverkehr-kopie, accessed
15 June 2018.

27 See www.lssa.org.za/upload/files/Resource%20documents/Information%20Security%20for%20South%20African%20Law%20Firms%20LSSA%20Guidelines%202018.pdf, accessed 15 June 2018.

28 See www.lawsociety.org.uk/support-services/practice-management/cybersecurity-and-scam-prevention, accessed 15 June 2018.

29 See www.americanbar.org/groups/cybersecurity/resources.html, accessed 15 June 2018.

30 See www.acsc.gov.au/index.html, accessed 15 June 2018.

31 See http://thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf, accessed 15 June 2018.

32 See https://eeas.europa.eu/topics/eu-international-cyberspace-policy_en, accessed 15 June 2018.

33 See www.ncsc.govt.nz, accessed 15 June 2018.

34 See www.cyberaware.gov.uk, accessed 15 June 2018.

35 See www.ncsc.gov.uk, accessed 15 June 2018.

36 See www.cyberessentials.ncsc.gov.uk, accessed 15 June 2018.

37 See www.nist.gov/topics/cybersecurity, accessed 15 June 2018.

38 See www.google.com/safetycenter/everyone/cybercrime, accessed 15 June 2018.

39 See www.iso.org/isoiec-27001-information-security.html, accessed 15 June 2018.

40 See www.mcafee.com/uk/threat-center.aspx, accessed 15 June 2018.

41 See www.microsoft.com/en-us/security/default.aspx, accessed 15 June 2018.

42 See https://uk.norton.com/cyber-security-insights, accessed 15 June 2018.

43 See www.sans.org, accessed 15 June 2018.

44 See www.sophos.com/en-us/security-news-trends/whitepapers.aspx, accessed 15 June 2018.

45 See www.wombatsecurity.com/resource-center, accessed 15 June 2018.

the global voice of
the legal profession®

To view online, visit: **www.ibanet.org/LPRU/LPRU-Cybersecurity.aspx**

To find out more, email: **LPRU@int-bar.org**