IBA cybersecurity guidelines for law firms during the Covid-19 crisis

Slowly and silently the virtual world has taken over our lives, drawing us into the swirling whirlpool of Covid-19, pandemic lockdowns, social distancing and invisible cyber vulnerabilities. More than ever before, global legal professionals need to effectively secure access to legal services from online threats of emerging novel viruses.

Recently, two law firms in Canada's Manitoba province were hit by a ransomware named 'Maze'. Also in February 2020, Maze hacked five United States law firms and demanded **two ransom payments of 100 bitcoins each** (approximately US$933,000 at the time).

The Law Society of Manitoba has issued a statement[2] on the internet virus pandemic alerting the firms of the hidden risks. The statement specifically mentions that the ransomware viruses are often hidden in email attachments. The infected attachments appear to have been about Covid-19 including, as follows:

- emails with a Covid-19 outbreak maps in an attachment;
- emails inviting you to a seminar to discuss responses to Covid-19, which includes a link to register for the seminar;
- emails claiming to be from vendors or associations about Covid-19 that include links to PDFs and Word documents; and
- SMS (text) messages, indicating you need to 'click here' to find out about modified firm operations.

Smaller law firms are being targeted by hackers specifically because such firms believe themselves to be unlikely targets and therefore frequently do not have the infrastructure in place to protect themselves. Law firms tend to store the most important and valuable client files on accessible online platforms. It is quicker and easier to find such files via a law firm than by searching through all the information on the client's server. Such attacks have been continuing with increasing sophistication and frequency. It is essential for law firms of all sizes to be aware of such threats and have data protection policies and procedures in place to counter them.

The cybersecurity guidelines were released in October 2018 and has been available on the LSSA website. Click here to view the guideline.

While the guidelines are relevant to all firms, they are particularly relevant to single practitioners and small-to-intermediate sized firms.

The firms should implement a layered programme of technical defences to mitigate the risk of a cyber-incident. Some of the key technology-related points to note and to act on during the current crisis, are as follows:

1. 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. Remote users must make sure to update their software to the latest version in line with the security policies of the firm.

2. Use secure internet connections

If staff work remotely, ensure that the internet connection used is secured through a virtual private network (VPN) 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.

3. Secure web browsing

Remote users must make sure that web browsers, such as Google Chrome, Internet Explore and others, must always:

- be updated;
- have endpoint security solution plug-in and pop-up blockers enabled;
- have autocomplete and autofill features disabled; and
- have the content filter feature enabled, if available.

4. Secure email accounts

Avoid or minimise operating on free web-based email accounts (eg, Gmail, Yahoo) to communicate with clients, as far as possible, and try paid web-based services providers for appropriate security.

5. Implement data retention, loss recovery capability

Cloud-based back-up services are a highly common and secure back-up solution. It is important that firms consider the type of cloud-based back-up 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.

6. Encrypt data and devices

Encrypt sensitive stored records and data on laptop, tablets and mobile devices, so that only users with the encryption key or password can access the information.

7. Enable remote erasure

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.

8. Ensure that the cloud storage/computer 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.

9. Consider application whitelisting/blacklisting

Application software programmes (apps) often have code vulnerabilities that pose a security risk in themselves, and must be evaluated and updated on an individual basis. Consider installing software that will allow only certain types of applications to run (a whitelist) and/or prevent others from running (a blacklist).

10. Secure mobile and other devices that retain data

Mobile storage devices (eg, flash drives, thumb drives, USB sticks) and other removable devices such should be virus scanned and generally used with extreme caution because they could be infected with malware that may get transmitted to the network when the drive is plugged in. These devices should also be encrypted.

The guidelines highlight the crucial role of organisational processes as the vast majority of successful cyberattacks are due to human error. The processes should assess the firm's cybersecurity risk profile, identify sensitive and valuable data, and enforce cost-effective strategies to mitigate cybersecurity threats. Law firms should consider implementing the following:

1. 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 per cent). Automatically require users to change their passwords regularly: every three months is fairly common.

2. 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.

3. Develop 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.

4. 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.

5. Consider cyber liability insurance

Law firms should assess their risk exposure and take out adequate cyber insurance as part of the firm's overall cyber security risk mitigation strategy. This 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.

In present times threats and risks have been aggravated by on-site lockdowns and increased online presence. In addition to the risk of ransomware attacks, malware attacks and phishing emails, there are growing challenges posed by cyber stalkers who are exploiting the increased flow of internet-enabled communications (Internet of Things). The intersection points transmitting the flow of data in multiple interoperable devices can challenge the security of the devices because of the changing structure and architecture of networks.

Lawyers are also increasingly participating in videoconferencing to talk to their clients via Zoom which is an easy-to-use popular online software platform used for real-time video-based communications. However, there is a risk of *'zoom bombing'* where uninvited attendees can abruptly join the call and disrupt it due to the visibility of the private unprotected link in the public domain. In order to communicate securely via Zoom, users should make sure to:

- circulate the Zoom default password only to the approved participants of the meeting;

- lock the meeting once all participants have joined;

- disable screen sharing for all non-host attendees and use 'mute all' controls; and

- note it down if the host intends to record the meeting.

The basic security approaches from the IBA cybersecurity guidelines (outlined earlier) are standard safeguards for the firm that should ideally not incur any significant financial or human resource challenge for achieving the purpose of providing security from cyberattacks. Security awareness training for law firm employees and staff is very essential to make sure that everyone is aware of the latest techniques used by cybercriminals.

These are certainly unprecedented times where all stakeholders of the legal profession are trying their best to navigate their way around the Covid-19 pandemic crisis. It is critical to instill and implement these necessary safeguards in place to prevent hackers and cyber criminals from exploiting this vulnerable situation. It is important to remember that operating outside of a conventional office space does not necessarily exclude or excuse the lawyers from their fundamental duty of making all efforts in keeping all communications and data confidential. The professional obligation of confidentiality requires lawyers to be active in promoting and protecting data security for a healthy and a trustworthy fiduciary relationship with their clients and thereby securing the access to justice

Evolving threats need enlightened approaches. The IBA Legal Policy & Research Unit and the IBA Cybersecurity Working Group (transitioned from the Presidential Task Force) continue to monitor developments and track potential emerging risks in the area of cybersecurity to enhance awareness, initiate dialogue and develop and implement solutions for the global legal profession

You may also want to have a look at the LSSA guideline on information security published in 2018. Click here to view it.