Living online/working online: cybersecurity issues you must address

GRANT FEARY, DEPUTY DIRECTOR, LAW CLAIMS

Online communication using mobile devices (phones/tablets/laptops) is so convenient and seductive it has become almost ubiquitous. Similarly, the use of email has become so common it is now almost certainly the most used mode of communication in the vast majority of businesses, including legal practices. The dangers of email and the use of mobile devices have been well documented both in these pages and in the general media in recent years. Fraudsters who target money transactions or data are clever and resourceful and will almost always be one or several steps ahead of those they are targeting.

The Society has recently sent out a survey to SA legal practices to ascertain the level of implementation of mitigation strategies to maintain good levels of cybersecurity. The results of this survey will assist the Society in planning relevant Risk Management education sessions and will be the subject of a further article in the coming months.

The survey questions were designed in conjunction with the PII Scheme's underwriter and were based on the *"Essential Eight"* cybersecurity strategies published by the Commonwealth Government. Being able to answer *"Yes"* to these questions is an indicator of good cybersecurity, both from the point of view of minimising risk to your clients and your own practice. Even if you didn't respond to the survey it is well worth a few minutes of your time reflecting on how your practice would answer the questions. The survey questions were as follows:

- Does your Practice require a password to access all computers and other devices (e.g. laptops, tables, phones etc.)?
- If yes, is there a policy in place requiring password complexity and periodic changing of passwords?
- Does your Practice require multifactor authentication for remote access to the Practice's computer systems?

(Note: multifactor authentication means the requirement to provide two or more methods of verification to be granted access.)

- Does your Practice restrict administrative privileges and application usage based on user duties?
- If yes, does your Practice regularly review the need for those users with such privileges to retain those privileges?
- Do all your Practice's computer systems have antivirus protection?
- Does your Practice conduct regular (minimum monthly) updates / patching of software systems – including any antivirus protection?
- Does your Practice conduct a daily backup and have recovery procedures for all clients' and business data?
- If yes:
  Is the backup data stored:
  - Remotely and disconnected from the Practice's computers?
  - For at least 3 months?
- Is the proper restoration of the Practice's computer systems from the backup data tested annually?
- Does your Practice have a hardware firewall protecting your network?
- Does the Practice have Application Whitelisting implemented? (This is where only approved / trusted programs can run, and non-approved applications (including malware) are automatically prevented from executing.)
- Do you have a secure method of sending and receiving confidential client documents electronically? (Note: email is not a secure method.)
- Does your Practice encrypt all confidential and sensitive data?
- Is USB access disabled on all computers used in your Practice?

Judge Joana Fuller

- Do you have a practice to verify client instructions as to monetary transactions?
- Does the Practice conduct penetration testing of the Practice's computer systems?
- Does the Practice actively monitor network traffic to regularly identify and assess new threats?

Whilst there is no guarantee that your practice will always be safe—after all the hackers and fraudsters have compromised the computer systems of government agencies and multinational companies—getting your practice into a position where you can answer *"Yes"* to these questions will be of tremendous benefit because the bad guys will most likely move on to an easier target.

Another important point relating to cybersecurity and the use of mobile devices outside your office is that it has to be recognised that public/free Wi-Fi is **not secure**. For example, we understand that most airport Wi-Fi systems have been hacked or are easily hackable. Despite the convenience, it is not recommended that any confidential client-related matters be conducted using public/free Wi-Fi connections, such as that available in airports, coffee shops and the like—you never know who has hacked into the connection.

Living and working online comes with its own set of risks which should never be ignored.