# How to protect your agency **against cybercrime**

The emergent risk of cybercrime poses a very real threat for businesses engaged in service industries, such as real estate agencies.

MICHAEL GAPES
Partner, Carter Newell Lawyers

**In the course of their daily operations, real estate agencies routinely collect, store and compile a substantial amount of personal and financial information about clients and third parties.**

In this article, we will define what is encompassed by the term *"cyber risk"* and provide some examples which highlight some of the key cyber risk exposures confronting real estate agencies. We will also detail a number of best practice strategies which can be implemented by agencies to mitigate against cybercrime.

## WHAT IS CYBER RISK?

It is important to appreciate that cyber risk is not limited to circumstances where IT systems are attacked or networks infiltrated by cyber criminals. Cyber risk can also arise from employee negligence or poorly managed data sharing and monitoring within a business, and can often lead to significant financial loss, disruption and reputational damage to the business.

The following examples demonstrate some of the differing types of cyber risks faced by real estate agencies.

### Scenario 1: Ransomware

A small real estate agency conducted all of its business, banking and trust accounting using two office computers which were linked over a shared network (with limited firewalls installed).

An employee accessed Facebook on one of the office computers and inadvertently clicked on a link in a newsfeed. A pop-up message appeared on the screen advising the employee that the computer and the agency's network had been locked and would only be unlocked in exchange for the payment of $10,000 into a specified bank account.

This example demonstrates a typical system breach by cyber criminals using "ransomware". As a result of the breach, the agency was unable to access its client database and records, its sales and property management files and its trust and general account records.

### Scenario 2: Data sharing over a public network

A sales agent conducted some business outside of his office at a local café. The agent accessed the agency's client database on his laptop, having connected using the café's Wi-Fi.

The agent updated a spreadsheet containing all of the names, addresses and contact details of his existing and former clients.

The agent saved the file remotely and also sent a copy of the file to his other devices using iCloud. However, the Wi-Fi in the café did not have strong data integrity and the document was unintentionally available to all Wi-Fi users on the café's network, including one of the agent's competitors.

This scenario demonstrates an inadvertent disclosure of sensitive personal information due to data sharing over a public network. Due to the nature of the information contained in the agent's spreadsheet, the potential ramifications of such disclosure could have been severe. It is worth remembering that since March 2014, the maximum potential penalties for breaches of the *Privacy Act 1988* (Cth) have increased to $300,000 for an individual and up to $1.7 million for businesses.

Further, the reputational damage to the sales agent and the agency could have been significant.

### Scenario 3: Employee breach

A disgruntled former employee of a large real estate agency noticed that the agency's computer passwords had not yet been updated following her termination. She logged onto the agency's database from her home computer and deleted numerous files from the agency's network. The deleted files related to the agency's


management of a multi-million dollar commercial property portfolio and could not be retrieved from the system, even with the assistance of the IT remediation experts.

## HOW REAL IS THE RISK?

Quantifying cyber risk can be difficult, as a large number of instances go undetected and unreported. However, it has been reported that the cost of cybercrime in Australia could be as much as $2 billion annually.[1] Further, the 2014 *Cost of Data Breach Study: Australia* has estimated that the average cost to an Australian business which has been subjected to a data breach is $2.8 million.[2]

Notwithstanding the highly publicised cyber attacks of recent times, including Woolworths, iiNet, and the unforgettable Ashley Madison debacle, the majority of cyber attacks that are taking place involve small businesses, presumably because their IT systems are easier to infiltrate.

In light of the rising threat of cyber risk, real estate agencies need to appreciate that they are not immune to the risk and must ensure that sufficient safeguards are implemented.

## BEST PRACTICE RECOMMENDATIONS

A whole of business approach towards minimising cyber risks should be taken. In this regard, we make the following best practice recommendations:

1. **Install reputable security software which includes a firewall, anti-virus and anti-spyware applications**

   It is also vital that the agency's security software is updated regularly as thousands of new worms, viruses and malware are created each day. Security software should cover the agency's entire operating network, including all applications and programs. In addition, the use of a robust spam filter should be installed, which will reduce the amount of spam received by the agency.

2. **Change all passwords regularly**

   Passwords should have a minimum of eight characters and use a combination of letters, numbers and symbols. Further, unique passwords should be used for access to all systems, including each website subscribed to.

   Individual passwords should also be changed regularly. In the event that an employee leaves, it is important to ensure that their access to the agency's network is immediately terminated and that all passwords are changed.

3. **Practice safe online practices**

   All real estate agencies must have an *Acceptable Use Policy* which governs the use of email and the internet at the agency. Employees should be provided with a copy of the policy in their induction and annual refresher training on compliance with the policy should be provided to all employees.

   Employees should also be educated to be wary of unsolicited emails or phone calls, and to be cautious of opening attachments or clicking on links received via email.

4. **Examine your remote access services**

   With many employees having access to agency networks on their mobile telephones, iPads and other portable devices, it is important that agencies also implement a *Bring Your Own Device Policy*, which sets out what part of the agency's network can be accessed remotely and the security measures which must be implemented to ensure that sensitive agency and client information and data is not compromised. It is a good idea to use encryption technology when providing remote access facilities to employees.

5. **Develop a backup strategy for your data**

   Daily backups of all data should be undertaken, in addition to weekly or monthly backups, with both offline copies as well as offsite storage of at least the weekly backup being preserved. Regular testing should also be undertaken to ensure that the agency can readily recover its backup data.

6. **Obtain cyber liability insurance**

   To ensure that real estate agencies are properly protected from the losses stemming from cyber risks, it is strongly recommended that cyber liability insurance be obtained.

   The REIQ Professional Indemnity Scheme policy (underwritten by QBE Australia and brokered by Aon Risk Services) has an optional cyber liability extension which will provide cover for, inter alia, civil liability resulting from data breaches, the costs of network repair and data restoration, cyber extortion and public relations expenses to mitigate reputational damage. Further enquiries in relation to cyber liability insurance for real estate agents should be directed to Aon's Real Estate Team on 1300 734 274.

## CONCLUSION

Cyber risk is an issue of growing concern to the real estate profession and agencies should implement the best practice recommendations above in order to protect against cyber breaches. If you become suspicious about a cyber security threat, the matter should be referred to the relevant authorities (including the Police and Office of Fair Trading).

[1] Norton Cybercrime Report 2012.

[2] Ponemon Institute *"2014: Cost of Data Breach Study"* (2014) at 1.