# Cyber fraud against lawyers

**Claire Kelly**
Product Specialist, Professional & Financial Lines
QBE Insurance (Australia) Ltd

The swift progression of technology over the last few decades has resulted in increased efficiencies, improvements to accuracy and reduced costs to business as IT infrastructure demands are reduced.

Emerging technologies such as cloud computing, which reduce infrastructure requirements and allow business to operate virtually and with portability have changed how we operate.

With these changes comes an increased risk of fraud. Not all these risks are resultant of new technologies, but rather inventive ways that fraudsters try to scam the innocent, which has resulted in a boom of new types of fraud by cybercriminals.

There has been a significant increase in incidents of cyberattacks for legal firms which has been supported by research from the National Cyber Security Centre of the UK.[1]

Technology has been considered a major enabler of the operations of fraudsters, who are adept at social engineering fraud and cyber fraud. This can be further evidenced by KPMG's 2016 report on technology and weak controls.[2]

## What is Social Engineering Fraud?

'Social Engineering Fraud' primarily involves people. Cyber criminals will trick people into handing over confidential information or money via telephone or using fake emails.

There are various types of Social Engineering Fraud, some of which are detailed below:[3]

- **Phishing and spear phishing:** Possibly the most common where people either email or telephone and pretend to be someone in authority or a client of a business. This can also include malware on emails that steals confidential information.
- **Vishing and smishing:** This includes persuading victims to give personal information via telephone or text.
- **Tailgating/piggybacking:** This is more common than we think; People gain access to a business by following closely behind an employee entering their business.
- **Pre texting:** Again gathering confidential or sensitive information by using a believable reason to impersonate an authority.
- **Quid pro quo:** This is where random calls are made and a benefit or gift is offered for certain personal information.
- **Baiting:** An example here could be a USB drive being left at a business where an employee will plug in the device and in turn infect the business computers.

## Law firms aren't immune to Social Engineering Fraud

**Case study 1[4]**
A number of law firms in Australia were targeted in a social

# Cyber fraud against lawyers

engineering fraud attack in Australia recently where losses to the law firms were apparently significant.

The cybercriminals didn't hack the law firms' systems but emailed promising business to them. They then sent emails with links to a file sharing site where emails and passwords were required by the lawyers. The email credentials were then stolen by the cyber criminals who gained access to the lawyers' email accounts.

They were then able to monitor the email accounts, and as large invoices were due for payment they inserted their own payment details. Security Brief reported on this attack which was initially broken by the Brisbane Times.

**Case study 2[5]**
Another trick that cyber criminals use is pretending to be a supplier and obtaining personal information. An employee of a law firm received an email from Microsoft saying their account was suspended and they needed to verify their account details to resume access.

The employee provided their login information and the attackers were able to access the employee's email account.

They copied an email address from a major client purchasing a property. For example, they may have changed one letter or number in the email address so that it looked similar and wouldn't be detected by the law firm.

The law firm believed that the fake email was authentic and a transaction occurred where they transferred a significant sum for the property to their bank account.

The Real Estate Institute of NSW have more details on this scam reported by CFC Underwriters.

## Hacking and data breaches

**Case study 1[6]**
Another law firm was targeted last year in the UK and their systems hacked. The hackers harvested the firm's data and released it publicly via social media.

The Law Society Gazette reported on the attack and what measures the firm took to remediate.

This type of attack not only results in a costly and time-consuming process to improve IT security following the attack, but even firms not required to notify the Privacy Commissioner of a data breach have a considerable reputational and litigation risk to manage.

**Case study 2[7]**
A well-known case reported last year by the Sydney Morning Herald involved a conveyancing firm who had their email account hacked. The hackers then added a new account with PEXA, the online property transfer platform, under the conveyancing firm's account.

They were then able to interrupt a settlement and switch bank details and transfer significant funds to their own account.

## Solutions

Fortunately, there are many strategies and measures that law firms can take to protect themselves from cyber fraud.

In terms of protecting against social engineering fraud there are a number of measures even small businesses can easily implement. Two of the most important are training staff on how to avoid fraud, including internet usage and authenticating certain correspondence, and implementing dual authorities for approving and establishing fund transfers.

It is imperative that your business has dual authentication processes in place. An email with payment information should never be considered adequate.

The Federal Government has a Small Business Guide on protecting your business in five easy steps which also provides further guidance.

In terms of IT security, ensure that you have up-to-date virus and firewall protection and have systems set up to automatically update software and virus protections so

that any new threats are eradicated by the updates. Staff should also refrain from using free WiFi and never send business emails to their private email addresses.

Fortunately, there is insurance protection available in the event of a cyberattack or social engineering fraud. Contact your broker to discuss cyber and crime insurance so that you are protected not just in the event that the company is defrauded of money, but for cyberattacks too. These insurances can assist with the financial loss to your business, as well as meeting the costs to reinstate and repair your IT systems, protect your reputation and help you to notify your clients in the event of an attack.

Keep in mind that insurers will assess your business's risk culture. A strong risk culture may result in insurers offering you more competitive coverage and pricing.

QBE's Cyber Insurance expert Ben Richardson details some of these measures in his paper *Out of the shadows: Data breach mandatory reporting and cyber insurance*.

Within this, he states the importance of demonstrating that you have internal data handling and internet usage policies for all employees across the business as this will ensure data is managed in a safe and consistent manner, while also preparing employees to identify and escalate potential incidents as soon as possible.

Ben also discusses how internal data breach incident response plans are necessary. Law firms of any size, including those not subject to the new Mandatory Data Breach Notification legislation, hold a lot of exposure to data breach and cybercrime events, which can lead to business interruption, expensive forensic investigations, or third-party liability claims.

A multi-pronged strategy incorporating a documented approach to people, IT security and risk, which is underpinned with insurance protection, will help protect your business from opportunistic cyber criminals.

**Helpful links**

*https://www.staysmartonline.gov.au/get-involved/guides/smallbusinessguide*

*https://www.marsh.com/au/services/cyber-risk.html*

*https://asd.gov.au/*

*https://www.qbe.com.au/au/media-centre/press-releases/qbe-releases-white-paper-on-cyber-risk*

1 *https://www.ncsc.gov.uk/legalthreat*
2 *https://assets.kpmg/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf*
3 *https://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud*
4 *https://securitybrief.com.au/story/case-study-how-cybercriminals-targeted-qld-law-firm-social-engineering*
5 *https://www.reinsw.com.au/Realcover/News/phishing_for_funds.aspx*
6 *https://www.lawgazette.co.uk/practice/hacked-firm-says-client-and-staff-details-spread-on-twitter/5065491.article*
7 *https://www.smh.com.au/business/companies/a-simple-cut-and-paste-let-cyber-criminals-steal-homes-worth-millions-20180629-p4zogn.html*