Law Council OF AUSTRALIA
Legal Practice Section
Australasian Law Management Journal

Edition: September 2020

Social engineering – the human factor in cyber risk

Staff training to raise awareness of cybersecurity threats is essential for law firms at a time when scammers are using sophisticated social engineering strategies to steal data and carry out fraud, writes Simone Herbert-Lowe.

Cybercrime is predicted to lead to the biggest transfer of wealth in human history.

In Australia, cybersecurity incidents are estimated to have cost businesses up to $29 billion per year. At the same time, law firms are attractive targets for cybercriminals because they act on high-value funds transfers and handle sensitive and confidential information.

While most business and personal transactions are 'above board', unfortunately there has always been some people who have used fraud, forgery and dishonesty to obtain an advantage for themselves or to cause harm to others.

Dark days

Historically, fraud was usually carried out by a person known to the victim, however with the move to a digital economy it has become easier for complete strangers to identify a target, collect information about them and then impersonate the targeted individual for ulterior motives. This collected information is sometimes obtained from the dark web, a part of the internet used for illegal transactions, and sometimes by using information disclosed in data breaches or simply found on social media.

Many forms of cyber events now involve imitation fraud. For example, scam emails may impersonate colleagues, clients, suppliers, or other businesses or individuals. These scams may involve no computer intrusion at all and simply use the display name on an email to impersonate another individual, business or government organisation. Imitation fraud using fake websites, emails and text messages is widespread, with the Australian Competition & Consumer Commission reporting an increase of more than 30 per cent in losses caused by scams in the first six months of 2020 compared with 2019. This is due to frauds that have leveraged the COVID-19 pandemic and summer bushfires.

In other cases, impersonation is used to infiltrate a computer by tricking the email's recipient into inadvertently opening the door to a computer network. This can be achieved, for example, by tricking the user into visiting what appears to be a genuine website, but which is actually a fake site so that the user's log in credentials and password can be captured and used to compromise other accounts. A common method is through the use of fake emails that appear to provide links to documents shared via popular services such as Dropbox or OneDrive. In other cases, the attachment to an email could install malicious code or redirect a user to a website containing malicious software.

Email threat

While people are becoming more aware of these types of methods, the impacts remain devastatingly effective, with 91 per cent of cyber incidents reportedly starting with an email. However, cyber incidents do not only involve online methods, and no industry or company appears to be immune. Police allege that the recent attack on Twitter, in which the accounts of Bill Gates, Joe Biden and others were hijacked, occurred as a result of phone spear-phishing, a targeted attack designed to trick people into handing over information such as passwords. The successful hacking of these high-profile accounts was reportedly masterminded by a 17-year-old.

Ransomware attacks are also prevalent and often start with a phishing email. Earlier this year, logistics giant Toll was the victim of two serious ransomware attacks. Toll's Chairman John Mullen told the Financial Review: "It is an element of human behaviour that creates these entry points or the chink in the armour, it is rarely the actual firewall that didn't work…People somehow get access to a master password, whether it's via guile or whether it's through criminal activity or bribing ... they will use human weaknesses to get around the system."

Cyber criminals now know that the easiest way to access to a network is via its people, using social engineering techniques that allow for new and sophisticated means of committing fraud, forgery and dishonesty in the modern era. While many lawyers might assume that cyber security is something that can be delegated to an IT contractor or department, it is increasingly recognised that training, awareness and processes such as verifying payment instructions using another method are now an essential part of any business's cybersecurity solution.

5 risk-prevention tips:

1. Make sure that all staff understand it is everyone's responsibility to protect the firm and its clients from cyber-attacks, particularly during remote-working arrangements where there are more emails and less face-to-face interaction.

2. Ensure staff receive cyber-risk awareness training and learn to recognise suspicious emails. Key points are to:
   - adopt a "zero trust" mindset to emails and look out for features such as the lack of a proper salutation, changes to email signatures, spelling mistakes, time-sensitive requests, and poor grammar;
   - avoid opening suspicious attachments or clicking on suspicious links;
   - check the reply address to emails and access websites via a browser instead of clicking on a link when you are asked to log in to an account – the email may be directing you to a fake website to capture your log-in credentials.
3. Pay particular attention to training staff in high-risk roles such as accounts and finance teams and staff members who have administrator privileges over online accounts.
4. Ensure that payment instructions received by email are confirmed by a phone call – and use a phone number that has previously been verified, **not** the one contained in the email requesting a funds transfer.
5. Implement a strong passwords policy and multi-factor authentication for all online accounts, especially firm networks and emails.

Simone Herbert-Lowe is the Legal Practitioner Director of Law & Cyber. Law & Cyber's online course,* Cyber Risk for Lawyers*, has been recommended for all lawyers and law firm employees insured by the Legal Practitioners' Liability Committee.