CYBER PRECEDENT

Strengthening the legal profession's defence against online threats

FACT SHEET: RANSOMWARE[1]

Ransomware is becoming a more common cyber threat. There were four times as many ransomware incidents in 2015 as there were in 2013; this is particularly noteworthy given that the number of most other types of cyber security incidents remained stable over the same period.[2]

Law firms and legal practitioners should therefore be familiar with ransomware, how it can be protected against and what can be done to minimise the seriousness of a ransomware incident.

WHAT IS RANSOMWARE?

Ransomware is malicious software that, once on a computer and activated, prevents the use of that computer and access to anything on it. The victim is then required to pay a 'ransom' in order to restore use and access.

HOW CAN RANSOMWARE GET ONTO COMPUTERS?

Emails. Typically a plausible-looking email is sent which either has an attachment or asks the recipient to click a link in the email itself. If the recipient opens the attachment or clicks on the link, the ransomware will be activated.

HOW COMMON ARE RANSOMWARE ATTACKS?

In 2015, the Australian Cyber Security Centre conducted a survey of major Australian businesses covering 12 industry sectors. Of the 149 respondents, 50% reported one or more cyber security incidents in the past 12 months. Of those incidents, the most common was ransomware (72%).[1] The Law Council is also aware of several incidents where law firms have been subjected to ransomware.

WHAT ARE SOME BASIC STEPS TO HELP MITIGATE RANSOMWARE ATTACKS?

Train and educate staff. If the dodgy attachment isn't opened in the first place, the ransomware can't be activated. Unexpected or unsolicited emails that ask you to open an attachment or click on a link should be treated with caution.

Keep operating systems and software up to date. Updates often close holes that malicious software could otherwise get into. This is critical. A key step is to keep software updated (ie utilise vendors' patches and updates).

Use anti-virus software and keep it up to date. While anti-virus software may not prevent all malicious software from getting into computers (such software is constantly evolving), it can capture most of it. Ensuring that you install all anti-virus software updates promptly will ensure your anti-virus software evolves as the method of attack evolves.

Back up electronic information and keep the backed up information separate from the computers or system. This way, even if a computer or system is infected with ransomware, important data could still be accessed.

[1] This fact sheet relies, in part, on information contained in Adrian McCullagh, *Ransomware: Strategies to Avoid Capture* (August 2016).

[2] Australian Cyber Security Centre, *2015 Cyber Security Survey: Major Australian Businesses*, www.acsc.gov.au/publications/ACSC_CERT_Cyber_Security_Survey_2015.pdf, 17.

[3] Ibid.