Law Council OF AUSTRALIA
Legal Practice Section
AUSTRALASIAN Law Management Journal

Edition: May 2020

Home truths for all after ransomware attack hits celebrity law firm

A potentially costly ransomware attack on a major American law firm is a reminder for all firms to educate their employees about cyber risks at a time when more people are working on unsecured home networks during the COVID-19 crisis, writes Simone Herbert-Lowe.

In recent months, the media has reported extensively on cyberattacks targeting companies such as Toll, MyBudget and Bluescope Steel.

For sheer audacity, though, the ransomware attack on US entertainment law firm Grubman Shire Meiselas & Sacks is a standout. The New York firm acts for celebrity clients, including Lady Gaga, Madonna, Elton John, U2 and Bruce Springsteen. In May, the firm confirmed it has been the victim of a cyberattack in which a group of hackers known as REvil gained access to a treasure trove of 756 gigabytes of data contained in legal files held on behalf of dozens of clients. The data included contracts, non-disclosure agreements, phone numbers, email addresses and personal correspondence.

A spokesperson for the firm told *Rolling Stone* magazine that "despite our substantial investment in state-of-the-art technology security, foreign cyberterrorists have hacked into our network and are demanding US$42 million as ransom. We are working directly with federal law enforcement and continue to work around the clock with the world's leading experts to address this situation".

After the firm reportedly hired cyber-extortion specialists and refused to pay the ransom, the hackers published files such as contracts, promotional agreements, expense sheets and confidentiality agreements relating to Lady Gaga. When it became clear the ransom would not be paid, the hackers reportedly moved on to auctioning the files off to the highest bidder. It also posted correspondence with Grubman Shire Meiselas & Sacks indicating that the firm had offered an amount of US$365,000 as a ransom payment, well down on the US$21 million originally demanded after the initial attack.

This type of incident is clearly a nightmare scenario for a legal practice that holds sensitive client information that it is required to keep confidential.

Phishing threats

While media reports to date have not disclosed the method of attack used in this instance, the most common way ransomware infects a network is through a phishing email. True to form, cyber criminals have wasted little time in seeking to exploit anxiety and the desire for information about COVID-19 by adapting phishing emails and other methods of cyberattacks and scams to reflect the pandemic.

Phishing emails and messages are designed to manipulate users into clicking on a malicious link, opening a malicious attachment, or giving away sensitive information such as login credentials. Most people are now aware of these type of emails, and while there are a range of measures that can prevent them reaching their intended recipients, unfortunately the sheer number of such emails and their constant evolution means it is impossible to prevent them all. So vigilance and staff education is critical.

Cyber criminals are exploiting the current environment by impersonating organisations such as banks and the Australian Government with the aim of tricking email recipients into visiting websites designed to install malware or steal personal information. Between March and April this year, cyber criminals and other malicious actors distributed a wide range of COVID-19-themed SMS and email campaigns, together with a variety of scams. The Australian Competition & Consumer Commission's Scamwatch received more than 1100 reports about COVID-19 scams, while the Australian Cyber Security Centre received over 115 cybercrime and cybersecurity incident reports from individuals and businesses.

Other risk areas

However, there is more to cyber fraud than phishing emails, as pure impersonation fraud may not involve any computer intrusion at all. Instead, this type of business email compromise relies on tricking the victim into misdirecting a payment to a fraudster by misrepresenting the true sender of the email.

A key area of concern in the current environment relates to scams impersonating government stimulus payments or attacking superannuation funds. (To date, more than a million Australians have applied for early access to their superannuation, with A$9.4 billion of retirement savings approved for early release). Allegations of identity theft involving 150 Australians led the Government to pause the early release of superannuation, after police froze A$120,000 believed to have been defrauded from retirees.

Law Council OF AUSTRALIA
Legal Practice Section
AUSTRALASIAN Law Management Journal

The risk of such threats to law firms and other businesses has been heightened during COVID-19 because of the number of people working remotely or from home. Remote-access scams targeting people working from home can include scammers who impersonate personnel from IT companies, telcos and banks to trick people into giving remote access to a computer in order to 'fix' a bogus issue. Other scams purport to be from Microsoft, or even the victim's employer's IT help desk.

IT departments that have had to transition firms to working-from-home arrangements almost overnight have never been busier. At the same time, typical security checks on users' behaviour may no longer apply in the work-from-home environment, and things that were once unusual are now seen as normal.

VPNs an essential safeguard

Many more people have now brought their work laptops into home WiFi networks that may lack the security of the office environment. Unqualified staff may now have to act as their own IT support team, thereby increasing opportunities for scammers.

As a result, setting up virtual private networks, or VPNs, is essential to protect business information shared between the office and home. Even leaving aside the challenges of working while minding or home-schooling children, COVID-19 means that many people now have an underlying level of anxiety and distraction that means that things that might otherwise have been noticed can now be missed.

With the vast majority of law firm staff now working from home, cyber education is more important than ever. While remote working has kept people safe from the virus, increased reliance on email – and distractions caused by COVID-19 – present greater opportunities for scammers and hackers. With law firms likely to be some of the last businesses to go back to the office, increased cyber awareness in the current environment is essential.

Simone Herbert-Lowe is the Legal Practitioner Director of Law & Cyber Pty Ltd.
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.