WannaCRYpt ransomware – Just the tip of the cyber risk to law firms

Over the past few days, new ransomware has spread across the globe to infect hundreds of thousands of PCs. For nearly half a day health infrastructure in the UK was compromised, badly affecting dozens of hospitals. Telecommunications, banking and logistics infrastructure were also disrupted.

What is Ransomware?

WannaCRYpt is ransomware, self-replicating code that attacks a network by encrypting the files on the system. Victims are then asked to pay a ransom to unscramble their files. If payment is not made, there is a threat to delete files. Some enterprises who paid the ransom did not have files restored.

For now, this particular ransomware outbreak has been somewhat contained by the response of UK security companies, but the attack software may be modified at any time. In any event, WannaCRYpt is only one of hundreds of malicious attack methods in circulation and by no means the most dangerous.

This attack breached NHS defences without even being targeted

This was not a targeted attack on the UK's National Health Service, Chinese banks or the other affected organizations.

It was the most primitive form of cyber-attack – a random infection spread by malicious links. Compromised systems then spread the software in emails that appear to come from colleagues, clients and family.

Targeted attacks are even more dangerous. At a recent *QLS Core: Cybersecurity and Minimising Data Breaches* session, penetration testing consultant William Ulyate walked through a typical attack scenario. Participants were somewhat shocked to learn that many law firms could be "hacked" in under 10 minutes using valid user names purchased from sophisticated online criminals.

Other firms are a tougher target, but in most cases a "socially engineered" attack directed at the firm's specific employees would eventually get through unless staff are aware of the risks.

How can it be worse than losing access to all your files?

Losing your files is bad, but if an attacker gains access to your network, they may quietly sit there for months accessing every document, email and photo entrusted to you by your clients. The first you know of it is a demand for tens or hundreds of thousands of dollars, failing which the relationship you have spent decades building with your clients can be destroyed by the publication of their data.

Restoring an infected network from backups is disruptive and expensive, but not the end of the world – provided of course that the backup copies are not infected as well. Restoring client trust following a major cyber breach may be impossible.

What can we do about it?

The most important thing to understand is that this is not just an issue for your IT team. Any employee can be the one to let the attackers through the firm defences - perhaps by using a recycled password or clicking a phishing email link.

Basic training to create a security culture within the firm is a critical adjunct to the work of the IT professionals.

The QLS Ethics Centre recommends that law practices implement basic training in Cybersecurity and review their procedures as soon as possible.

An audit of your technical defences and response plan if the defences fail is also highly advisable.

The Law Council of Australia has prepared an excellent resource for law firm leaders who are not expert in IT: website here.

Please also note QLS guidance here: Ethics and protection of confidentiality in a digital world.

David Bowles
Ethics Solicitor
17 May 2017