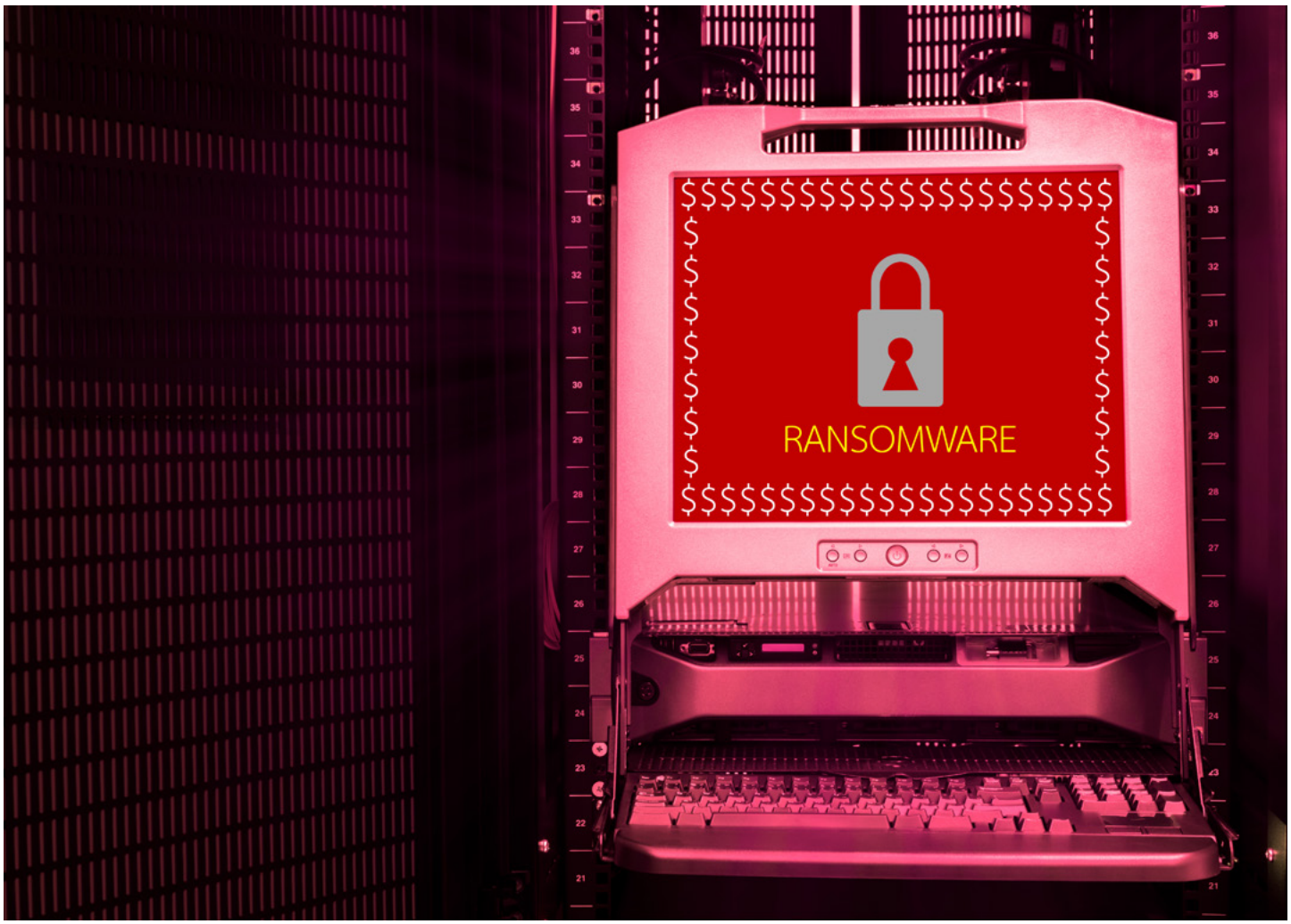

What should law firms do about **ransomware**?

BY MATT TORRENS

Ransomware is a now a very serious and consistent threat to business. This article explains what ransomware is, how best to defend your firm against it and what your firm can do if it suffers an infection.

Ransomware is a piece of software that encrypts or blocks access to the victim's data. In some cases, there is a threat to delete that data. In return for a decryption key or to regain access to the data, the victim is asked to pay a ransom. Most commonly, the ransom is demanded in the form of Bitcoin, an innovative digital payment system based on cryptocurrency.

Malware extortion dates back to 1989, but the notion of ransomware became highly prominent in 2013 with the now infamous CryptoLocker strain. More recently, 2017 saw the international spread of the WannaCry ransomware attack, which infected more than 230,000 computers in 150 countries and crippled much of the UK's national health service.

The total value of all ransomware payments is unknown, but in just three months during 2013, CryptoLocker saw returns of $27 million from infected users. Conversely, 2017's massive WannaCry outbreak netted a paltry $128,000 – thanks to the actions of Marcus Hutchins, the 'accidental hero' who found a way to slow the spread of the malware.

Figures from the SonicWall Global Response Intelligence Defense (GRID) Threat Network suggest that there were 266 million ransomware attack attempts in the fourth quarter of 2016. This was a sharp increase compared to previous quarters:

Ransomware is not going away any time soon. We need to do two things: improve our defences, and better understand our options if we become victims.

How can law firms avoid falling victim to ransomware?

I'm sure we'd all agree that not becoming a victim at all is the best option. Who wants to have to pay a ransom, or try to recover systems back into operation? And if you accept that brand awareness and reputation is key to the survival and growth of your practice, then you might also want to consider how to build reputational resilience in the form of a cyber-strategy.

Here are five 'quick wins' that can instantly make your practice safer and more resilient.

1. Software patching

- Automate your patching and cover as many vendors as possible. WannaCry exploited a Microsoft vulnerability, but often it is Java or Adobe.
- Install patches regularly – as soon as possible after release.

2. Email security

- Employ email security to scan traffic and particularly URLs (web addresses) within emails. This technology keeps you safe regardless of the device or location from which you access emails and click on any links.

3. Perimeter security

- Configure your perimeter security to analyse your traffic in real time. If you accidentally visit a nefarious website, this technology will detect, and drop, any malicious payloads. A well configured firewall will also prevent your machine from 'calling home' back out to the internet, should you somehow get infected.

4. Back up

- Have a robust and well tested backup process. If the worst happens and you are 'ransomwared', you can simply recover your data from a backup. This is still painful, but much less costly!

5. Train, train, train

- People don't like to hear it, but we are the weakest links – the humans. Train yourself and your colleagues to spot threats and avoid traps. The Law Society and the Information Commissioner's Office (a government agency) tell us we should all complete annual awareness training. Start now, and you will also be ticking a GDPR box (the General Data Protection Regulation is an EU measure that comes into force in 2018). There is probably no more effective countermeasure, pound for pound, than a good security awareness program. As the security technologist Bruce Schneier has noted, 'only amateurs attack machines; professionals target people'. The notion of 'the human firewall' should be at the forefront of any cyber resilience strategy.

The notion of 'the human firewall' should be at the forefront of any cyber resilience strategy

My firm is infected – what are the options?

According to the SonicWall 2017 Annual Threat Report, companies in the UK were three times as likely as those in the US to be targeted by ransomware. This means that a critical element of any successful cyber resilience strategy is to predetermine how your business will respond in the face of an attack and/or a ransomware infection.

Of equal importance is to plan how your organization will recover from the incident. The specifics will vary from business to business, but remember, the ultimate objective is to respond and recover with minimal financial or reputational loss. From a UK legal perspective, organizations should be closely considering the impact an incident may have on their clients, whose data they hold.

A significant goal is to have the right response to any breach to ensure that any data loss does not become a reputational crisis. If you have the right systems in place, you should not have to pay the ransom.

1. Mobilize incident response teams

- Early and accurate communication, both internal and external, is critical during the earliest stages of a breach or attack.

2. Contain

- Where possible, contain and isolate the threat and/or engage business continuity systems.

3. Retain

- Ensure that log files (e.g. system, application and firewall) remain intact/ ▸

stored for later forensic use. Where possible, safeguard all affected assets and establish a chain of custody.

4. Identify
- Identify the threat source and remove the weakness or vulnerability – permanently, if possible.

5. Recover
- Return your systems back to normal service as soon as is practicable.

6. Re-test
- Carefully review the threat vector and test new systems, processes or technology as required to ensure mitigation.

7. Review
- Take care to review your cyber resilience strategy in its totality.

How to deal with communication if you become a victim of ransomware

Throughout the response and recovery stages, communication is vital. We have seen many high-profile incidents where poor communication from the breached company has led to confusion both for clients and for staff. Ultimately, the most significant cost of a poor communication strategy is likely to be borne by the business itself. Poor communication throughout the incident teams, both internally and externally, can easily lead to additional and unnecessary technical work, data loss, loss of productivity and client goodwill – and ultimately, a public relations disaster.

Conclusion

A true cyber resilience approach blends protection, detection, response and recovery to form an organization-wide, collaborative strategy. In order to protect itself from cyber threats, a business must first be able to recognize its risks (combining threats and vulnerabilities) and go on to define solutions to help manage those risks. Response and recovery plans may then take many differing forms but should always have the aim of enabling the organization to recover with minimal financial or reputational damage.

Matt Torrens is managing director at legal IT specialist SproutIT, which seeks to help law firms and barristers' chambers to achieve competitive advantage and peace of mind through the innovative use of best-of-breed technology; focused cyber security and resilience; award-winning services; and passion for service excellence.

LEGAL IT TODAY
COMMENTARY, STRATEGY AND MARKET INTELLIGENCE FOR THE GLOBAL LEGAL TECHNOLOGY COMMUNITY
18 JUN 2017