

RANSOMWARE – THE RISK IS REAL - WHAT DOES THIS MEAN FOR YOUR BUSINESS?

By Heidi Bruce, PRINCIPAL – MANAGING DIRECTOR, SYDNEY

29 JUNE 2017

You will have seen in the press the cyber attacks that have been impacting businesses worldwide, with a recent wave of attacks affecting international businesses. These are not isolated incidents by any stretch, and this is a serious concern that all businesses need to consider. The experts have been warning for some months that the risks of these attacks hitting Australian businesses are very real. The risks include not only critical impacts on business operations, but serious adverse legal and reputational consequences.

Ransomware – what is it?

Ransomware is a form of cyber attack that typically encrypts files on a server, and offers to give a key to unlock the data for a fee. This will generally come in the form of a rudimentary request for a set amount of Bitcoin, a form of digital currency, which can represent a very substantial sum of money. If you or your clients rely on this data and there is no backup, then the decision whether to pay the ransom will be one you don't want to have to make. Even if the ransom is paid there is no guarantee that the attackers will follow through with their offer to unlock the data, so there is no certainty that the files will be recovered. It can often be impossible to verify whether there has been any actual transfer or sharing of the data so it may be very difficult to know the extent of the problem you are dealing with.

How can it really impact advertising, media, PR, digital and promotional agencies?

Such agencies are increasingly holding or managing some form of client data on their systems, and this may include personal information such as names and contact details or sensitive information such as health or religious details. Agencies can also be involved in the processing of credit card payments, which is extremely valuable.

Many of these agencies will often use the most advanced technologies and processes to ensure the protection of their systems and the data they hold. However in some cases there may be systems that are overlooked for whatever reason, they may be seen as low risk, or they may be old legacy systems that have not been updated or reviewed for some time. These can be especially vulnerable to cyber attackers and even with the best measures in place across the board, there may be hidden weaknesses.

These sorts of attacks are predicted to increase in sophistication and in prevalence, and the valuable nature of the data held by agencies can set them up as high risk targets for these sorts of attacks.

What are the legal consequences?

With [new data breach notification laws](#) set to become mandatory in Australia in February 2018, this will carry even heavier consequences. For an eligible data breach, ie one that is likely to result in 'serious harm' to an individual, a business will need to notify the Privacy Commissioner and affected individuals.

Under current Australian privacy laws, there is an obligation on APP entities to take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Most contracts that agencies have with their clients will have a clause that requires the agency to comply with Australian privacy laws including the above, and can also include a whole raft of obligations on security, back-up of data, restricting access to personal information, and procedures for management of personal information. If security measures are not up to scratch, a ransomware attack could expose flaws and lead to claims that the agency has not fulfilled its obligations.

Client contracts can also include an express requirement for the agency to notify the client if there has been a data breach. So this can mean the agency is obligated to inform the client immediately of the issue and the steps it is taking to resolve it. The client may pressure for notification to consumers, and may claim breach of contract or negligence under the client contract.

What steps should be taken now?

It is critical that agencies take the time now to do a thorough investigation of their systems including servers and applications especially those with access to the internet, and ensure that security settings are in place and up to date, the relevant support is being provided and crucially, patches are installed regularly. As cyber criminals find new vulnerabilities, the technology providers come out with patches, so the longer you take to patch a system, the higher the vulnerability. It is also recommended to consider a routine of penetration testing, and whether adequate data back-up and recovery processes are in place. Training is also prudent, to advise staff not to open certain files and to take other preventative measures.

If a data breach or cyber attack does occur, and these are becoming more inevitable in this environment, the agency will need a robust response process to ensure the agency can react quickly and confidently to fix the issue and reassure any affected clients. It is important that a robust response and escalation procedure is in place, so that staff know exactly what to do and who should be contacted to investigate and manage the issue. It can help to have experts appointed to roles in the technical response and data protection fields, for this purpose. A strong response procedure when properly executed, can help to resolve and shut down an issue successfully before it escalates.

Contact us

If you would like further information on data security related issues, please contact one of our experts below.

Heidi Bruce
02 8935 8806
Heidi.bruce@anisimoff.com.au

Tony Anisimoff
02 9460 6611
tony@anisimoff.com.au



www.anisimoff.com.au



<https://www.facebook.com/AnisimoffLegal>



<https://twitter.com/AnisimoffLegal>



<http://www.linkedin.com/company/anisimoff-legal>