HARBOUR HR ESCAPE RANSOMEWARE DISASTER THROUGH DATAFORT BACKUP AND RECOVERY SERVICE

By Steven Birch

The recent news of the Hollywood Presbyterian Medical Center, a Los Angeles hospital, faced with a disastrous ransomware attack and forced to pay hackers $17,000 of bitcoin to regain access to critical files, perfectly demonstrates just why ransomware is becoming the attack of choice for cyber criminals worldwide. Hackers demand ransoms just low enough that organisations, facing potentially disastrous and costly disruption to their operations, give in and pay up.

Experts expect this type of security attack to increase rapidly in the next six months as more hackers realise the potential ransomware has to make them serious financial gains.

Harbour HR found themselves victims of just such a ransomware attack in December 2015. The ransomware encrypted their files and threatened serious disruption to their business functions, unless a fee was paid.

As a DATAFORT customer, the end of the story for Harbour HR was significantly different, and very much happier, than that of the Hollywood Medical Centre.
Read the full case study below to see how DATAFORT's services saved the day and Harbour HR the need for a big payoff!

BACKGROUND:

Harbour HR is an established consultancy providing bespoke domestic and international HR solutions. From one off projects to ongoing long term support, Harbour's expertise ranges from HR support, immigration assistance and employer risk assessment to special project assignments.

Harbour HR specialise in the delivery of bespoke Human Resource, Immigration and International Assignment advice, with a service provided by a team of highly qualified consultants with years of experience. Their goal being to provide professional, expert knowledge and exceptional services levels.

The company's IT is managed by Capital Support who partner with DATAFORT for the provision of data backup and recovery services.

CHALLENGES:

On the 2nd December 2015 Harbour HR suddenly realised that they had been attacked by a ransomeware virus.

Nigel Sellens, Managing Director reflected "the first thing we noticed was that we were being locked-out of some of our files. Then a message came up that said all our files had been locked and would only be released on the payment of a ransome fee".

This is a situation that is being faced by many organisations as the ramsomeware attackers are becoming increasingly cunning in their methods. They trap many unsuspecting email users who inadvertently click on a file within an email that appears at face value to be perfectly genuine.

"This was a serious problem, we faced the possibility of losing all our data and not being able to access or use IT which would significantly harm our business" said Nigel Sellens. "Not only were they asking for a ransome in excess of £1500, we would also always be in doubt as to whether the virus was really cleared from our servers."

Harbour called our support provider at Capital Support who told them to shut everything down before triggering their data backup partner DATAFORT into action.

HARBOUR HR'S DATAFORT BACKUP SERVICE

Harbour were using DATAFORT's Core Care Managed service that stored data on a dedicated backup appliances held both in the Harbour HR office and enterprise class data centres. The service is based on a continuous backup process which takes snapshots of the data every 15 minutes throughout the business day. This means the data can be restored back to any point going back in 15 minute intervals over the previous 2 days as well as providing read-only archives for each end of day for 5 days, end of weeks for 5 weeks and end of month's snapshots for a full 7 years.

This method of backup is particularly useful in the situation that Harbour HR faced. The key challenge with conventional daily backup is knowing when the servers were infected as data is backed up on a version basis, rather than by date. So determining which file version to restore requires a very time consuming process as you'd have to go through the entire server making sure to restore only files saved prior to the infection. In addition, a day or more of data could be lost depending on the relative timing between the daily backup and the time of the infection.

In Harbour HR's situation, DATAFORT service engineers were able to go back in 15 minute slots and identify when the virus was received, then restore the entire server to the point minutes just before it happened, so enabling Harbour HR to continue working with minimal loss of data. This is a much faster cleaner process than traditional daily backup.

Outcome

DATAFORT were able to restore Harbour HR to a virus free environment within a few hours of them noticing the problem.

Nigel Sellens commented "This was amazing, we were back up and running within hours. I've not experienced this kind of issue before and it's great to know it works and that we are secure!"

DATAFORT has a range of complete server protection services that will protect your data from a full range of risks for a fixed monthly fee. Contact our sales team for more information.