WHY SIMPLY HAVING BASIC CYBER RISKS INSURANCE MAY NOT BE ENOUGH*

In a news story that will send a chill through almost every business that holds customer data, it was reported last month that cyber criminals had stolen the data of more than 600,000 Dominos Pizza customers in Belgium and France. An anonymous Twitter user threatened to publish the data unless the company paid a cash ransom.

Customer names, delivery addresses, phone numbers, email addresses and passwords were taken from a server used in an online ordering system that the company was in the process of replacing. Domino's spokesman Chris Brandon said that he did not know if the stolen passwords had been encrypted. According to media reports, a tweet directed at Domino's customers through an account of somebody listed as "Rex Mundi" said hackers would publish the customer data on the Internet unless the company paid them 30,000 euros. The Rex Mundi account was later suspended. Brandon said he was not familiar with the ransom demands, but that the company would not be making any such payment.

Domino's Vice President of Communications Tim McIntyre said the hacking was "isolated" to independent franchise markets of Belgium and France, where the company's online ordering system did not collect credit card orders, so no financial data had been taken.

The episode raises the issue of whether cyber risk insurance policies offer sufficient cover for the risks faced by businesses now. UK businesses increasingly understand the importance of cyber risk insurance cover for managing the impact of data breaches but this incident shows that simply having basic cyber cover may not be enough to protect against all the perils posed by cybercrime.

Almost all cyber risk insurance policies protect against liability to third parties and a good number cover an insured's own first party costs of managing a data breach and the ensuing crisis. These costs can include hiring consultants to identify and analyse the breach, legal costs, and rebuilding compromised security systems. Extortion by a third party, however, does not fit within most third party or first party covers, and extortion liability coverage tends to require a specific addition to the cover. Traditional kidnap and ransom cover may not be triggered if all that has happened is that data has been copied rather than physical assets or staff being detained.

Cyber risk insurance is a relatively new product, and the scope of its coverage can vary enormously from policy to policy. As the market for cyber risk insurance is still developing, there is no industry wide consensus on what policies should cover and the array of options and terms used for the same products can be confusing for the customer.

As the field of cyber risk insurance matures, policies are becoming more specific and customisable. Accordingly it is essential that businesses, their brokers and insurers

consider the level of cover required so that the appropriate protection is given, including ensuring that customers are not paying for unnecessary coverage.
A number of high profile companies including Sony and more recently Target in the US have found themselves in the news following the theft of personal customer information from databases. These events often hit the headlines when large companies are involved, yet the majority of data breaches occur within small companies. And while the impact on a large company can be significant, for a small or medium sized enterprise it can be devastating.

The methods used by cyber criminals are evolving and consequently so are the risks for companies. It is therefore vital that insureds and their brokers carefully consider whether obtaining extortion liability coverage is necessary.

We are grateful to Justin Tivey, Senior Manager and Fiona Pearson, Associate, at Bond Dickinson, a leading UK law firm for allowing us to reproduce the above excellent article. What they have written for the UK market is certainly of application to the South African market and whilst this communication is provided for general information only and does not constitute legal or other professional advice, we strongly recommend that you consult a suitably qualified person in order to discuss this very important issue.