Cyber Insurance Making its Mark

Privacy Breach Regulation is Tightening

SMEs are increasingly realising the need to better manage the risks posed by the growing digital environment especially since the emergence and publicity of large scale, worldwide cyber attacks, notably WannaCry and NotPetya.

As many in our broker market will have realised VL took a measured approach in developing and launching its Cyber product in March last year. This approach has proved to be successful with a steady stream of placements and enquiries. We have found in many cases that Cyber can be quoted simply by utilising the information on a LegalEdge proposal form.

The VL policy is primarily aimed at the SME and professional services sectors however VL does have the appetite to consider larger more complex risks on a case by case basis.

Apart from the obvious risks of replacing hardware and software and the attendant business interruption losses there is a growing risk of failing to comply with regulatory reporting requirements in the aftermath of a data breach. Whilst there are not yet any mandatory data breach notification laws in New Zealand, businesses which trade into territories with such legislation are potentially exposed. Two significant markets, Australia and the European Union have tightened their privacy breach laws:

1. From 22 February 2018 Australia's Notifiable Data Breaches Scheme under Part IIIC of the Privacy Act 1998 came into effect. In the event of an 'eligible data breach' the entity must notify the Office of the Australian Information Commissioner and all individuals affected. Breaches can attract penalties up to AUD$1.8million. An 'eligible data breach' occurs where there has been:

   (a) unauthorised access or disclosure, or loss of information where unauthorised access or disclosure is likely; and
   (b) a reasonable person would conclude that the access or disclosure would likely result in serious harm to the individuals to whom the information relates.

   For more information on whether this might apply to your client see the Office of the Australian Information Commissioner website.

2. In the EU the General Data Protection Regulation (GDPR) comes into effect on 25 May 2018. The GDPR applies to all companies worldwide processing the personal data of EU citizens. Organisations can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). Breach notification will become mandatory where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This mandatory notification must take place within 72 hours of having first become aware of the breach. See EU General Data Protection Regulation website for more information.

As well in the USA, whilst there is no single specific federal 'privacy breach' legislation. There are innumerable state and federal acts which embrace the principles of privacy and data breach reporting. The main federal law which traverses this is the Federal Trade Practices Act. It prohibits unfair or deceptive acts or practices involving practices that fail to safeguard consumers' personal information with significant financial penalties at its disposal.

The VL policy caters for these exposures with specific cover for costs arising from a breach of privacy obligations.

Talk to your VL underwriter who will be happy to assist with any queries.