Browne Jacobson

‘Big Game Hunting’ – the new face of cyber extortion?

11 December 2022

Previous
(Another) case on insurers’ duty to defend

Next
Comply with policy terms – or pay the price

According to a recent article by cyber response firm Storm Guidance, ransom attack methods have been steadily moving away from widespread attacks towards ‘Big Game Hunting’. But what is it, and why does it matter to insurers?

What is ‘Big Game Hunting’?

Big Game Hunting is a general term used to describe cyber attacks (and, in particular, ransomware attacks) which attack specific high value targets who have a higher ransom potential. That ransom value may be driven by the particular harm - financially, operationally or reputationally – that could be caused to that particular target. Cyber criminals have calculated that such victims are not only more likely to pay a ransom, but are also likely to be prepared to pay a higher ransom, than other victims.

One particular method of big game hunting which is increasing in frequency is the use of ‘data extortion attacks’. In a data extortion attack, cyber criminals will access data belonging that is particularly sensitive or of extra value to the victim. The cyber criminals will then charge a ransom for the data to be released. In some cases, where the data may also be of value to others, the data will be sold by the cyber attackers at an auction to which anyone who may be interested in the data will be invited. The invitees will include the victim, who must outbid everyone else in order to buy back their own data.

According to Storm Guidance the data being stolen can take many forms including trade secrets, client databases, political and military secrets.

Why does this matter to underwriters?

It is important for cyber underwriters to stay up to date with ever-changing attack methods used by cyber criminals. The potential move towards ‘big game hunting’ as an attack vector may require more specific and detailed underwriting for businesses or individuals who may be particularly valuable to cyber criminals.

Additionally, the increased focus on data as the target for ransomware attacks may necessitate additional underwriting questions as to the amount and nature of data held by a proposer, together with information as to how that data is protected. In some cases, additional wordings protections may be required in the form of more specific exclusions and obligations.

Contents

Contact

Tim Johnson

Partner

tim.johnson@brownejacobson.com

+44 (0)115 976 6557

Our expertise

Services

Cyber liability and data security insurance

Policy drafting and distribution