# Five answers to cyber insurance doubts

MPR

TOP 5 TIPS

During the many conversations around the challenges of selling cyber insurance, some common themes emerge, but these are often easily answered:

## 1

### It's too expensive.

It very probably isn't. Consider how much it might cost to have; a dedicated incident response manager (24 hours a day, 365 days a year) with forensic experts, extortion specialists, PR representation, call centre facilities/staff, legal experts, restoration services. All of this is effectively in-house and available on tap. Not to mention the additional 1st party costs of potential notification, credit monitoring, further crisis response, and so on.

And don't forget the financial backstop for any 3rd party liabilities and potential regulatory action, all of which may ultimately be determined by the immediacy and professionalism of expert response in the early stages of an event.

Still too expensive…?

## 2

### There are too many exclusions.

That depends on the policy and how it's underwritten. Streamlined and 'statement of fact' insurer approaches have, naturally, been known to build protection into products (exclusions or certain IT security requirements), so look for insurers who like to understand the risk and actually do ask questions. The reason they do this might be because their policy provides stronger cover with fewer exclusions and caveats.

## 3

### We don't have many customers or personal records, so it's not for us.

Personally identifiable information (PII) and data breaches are just one area of cover, but what about extortion attempts (ransomware attacks), crisis response, interruptions to business operations, loss of corporate information, dealing with regulation or online media liability? Cyber is not just about PII.

## 4

### Our IT director is very sceptical of the benefits.

It's certainly not always the case that they are, but it's hardly surprising if they were. Insurance is part of a strong cyber strategy, not a substitute for one.

Cyber is a business risk and a board level issue. Poor handling of a cyber event can be far-reaching and fatal to the business, so the IT director needs support.

## 5

### We have good IT security and procedures, so we think our risk is already fully mitigated.

Nothing is fully defendable.

Cyber insurance is not designed to replace the mitigation already in place – it works hand in hand to ensure that there is a solution should the worst happen. The mind-set needs to shift from upfront defence as the main priority to a heavier emphasis on preparing for swift recovery and response. Good existing mitigation will mean you can access a quality product at competitive prices.

*Drawing a parallel with building and contents. There may be locks on the doors, sprinkler systems and alarms, but you still buy the insurance policy. The same should be the case for cyber, with better deals available by demonstrating strong risk protection.*

## To be solid, insurance must be flexible