The top 6 cyber insurance myths debunked

Cyber is one of the hottest topics in insurance and, as a line of business, it's projected to experience phenomenal growth in the years ahead. But cyber is still a relatively new market, and can be made unnecessarily complex by industry jargon, buzzwords of the day, and a lack of standardization in policy wordings. As such, many companies find themselves confused about how cyber insurance actually works and are skeptical about whether it makes sense for their business to purchase a policy.

To clear up the confusion, here are six of the most common misunderstandings that businesses tend to have about cyber insurance and how to overcome them.

Myth 1

"We don't need cyber insurance. We invest in IT security..."

This might be the single most common objection to purchasing a cyber insurance policy.

Not purchasing a cyber policy because you have 'good IT security' is akin to suggesting that you don't need theft cover on a property policy because you have high quality locks on your doors, or fire cover because you have a sprinkler system in place.

There is a big difference between vulnerability and risk. And while a client that has invested heavily in IT security may be less vulnerable to certain types of cyber attack than an organisation that has invested very little, they still have a risk exposure. Cyber threats are rapidly evolving and there are a plethora of ways in which attackers can access networks. Even large corporations that spend vast amounts of money on IT security every year still get hit.

People are often the weakest link in an organisation's IT security chain. According to IBM, 95% of successful cyberattacks and incidents are the result of human error[1]. Technology and training may reduce the likelihood of an employee accidentally clicking on a malicious link in an email, or from being tricked into transferring funds to a fraudster as part of a social engineering attack, but it can't eliminate those risks completely. And no amount of investment in IT security can stop employees from leaving their laptops on a train or a rogue employee from releasing sensitive data on the internet.

The short answer

No matter how much a company invests in IT security, they will never be 100% secure. The purpose of an insurance policy is to respond in the event that the worst happens.

Myth 2

"We outsource all of our IT, so we don't have an exposure..."

Using a third party for IT might change your exposure, but it doesn't eliminate it.

Consider what happens in the event of a data breach. If an organisation outsources their data storage to a third party and that third party is breached, they could be forgiven for thinking that responsibility for notifying affected individuals and dealing with any subsequent regulatory actions that may arise would rest with the breached third party.

But that's generally not the case.

If an individual has entrusted their personal data to an organisation, it is the organisation that is responsible for looking after that data, regardless of whether or not a third party is utilised to look after it. If that data is lost or stolen, then it is the organisation that will be accountable for any notification requirements, regulatory investigations, fines or penalties that do arise, and it will be their reputation that suffers, not the third party's.

Of course, it isn't just breaches of data at outsourced IT providers that could leave businesses exposed. Many businesses rely on third parties for business critical operations, and should those providers experience a system failure, it could have a catastrophic effect on the company's ability to trade, resulting in a business interruption loss and additional costs incurred to continue trading.

Claiming back these losses from a third party can also prove to be easier said than done. Most third party technology service providers tend to have standard terms of service that completely limit their liability in the event that a breach or system outage causes financial harm to one of their clients.

The short answer

Even if you outsource your IT, the chances are you're still liable. Assuming you'll be successful in claiming back damages from a third-party is a risky gamble.

Myth 3

"We don't collect any sensitive data, so we don't need cyber insurance..."

Cyber insurance is about much more than data breach and privacy risk. In fact, two of the most common sources of cyber claims are funds transfer fraud and system damage or business interruption as a result of ransomware.

Funds transfer fraud is often carried out by criminals using fraudulent emails or conducting social engineering over the phone to request the transfer of funds from a legitimate account to their own. In many cases, fraudsters will pose as a senior executive appearing to give urgent instructions to a junior employee. Any business that wires money to and from a business bank account is susceptible to funds transfer fraud, and many of the victims of these losses hold next to no sensitive personal data.

Additionally, 2017 saw the WannaCry and NotPetya ransomware outbreaks cripple many organisations within the manufacturing and logistics industries. These attacks did not involve the theft of data, but rather the freezing or damage of business-critical computer systems. NotPetya alone is estimated to have cost businesses over £1 billion[2], and nearly all of that loss was due to operational disruption leading to large drops in turnover and the significant cost of rebuilding or replacing systems. The core exposure in both cases was not data breach but system business interruption and system damage.

The short answer

Any business that relies on a computer system to operate, whether for business-critical activities or simply electronic banking, has a very real cyber exposure.

[1] IBM Cyber Security Intelligence Index 2013

[2] Fred O'Connor, Cybereason (https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue)

Myth 4

"Cyber attacks only affect big business. We're too small to be a target..."

We've all heard about major corporations falling victim to cyber attacks because they're reported in the news. But what you don't often hear about is the small law firm that transfers £100,000 to a fraudster as part of a social engineering scam or the private hospital unable to use their computer systems for days because of a destructive malware attack. Just because events like these aren't reported in the mainstream media doesn't mean they aren't happening.

In fact, attacks against smaller organisations are now so frequent they are no longer newsworthy. A recent Verizon report found that 58% of victims were categorised as small businesses[3]. Looking at our own CFC data shows that 95% of funds transfer fraud claims, our largest source of claims by number, come from businesses with revenues under £100 million.

Cybercriminals see smaller organisations as low hanging fruit because they often lack the resources necessary to invest in IT security or provide cyber security training for their staff, making them an easier target.

The short answer

Cyber criminals target the most vulnerable companies, not just the most valuable.

Myth 5

"Cyber is already covered by other lines of insurance..."

Cyber insurance emerged as a standalone product specifically to fill the gaps that more traditional insurance products have been unable to fill.

Property, crime and professional liability are three of the most common lines of insurance assumed to include some form of cyber cover, but they often fall well short of the cover found in a standalone policy.

Property insurance policies, for example, have often included some form of sub-limit for data restoration costs, but it was developed as an add-on with narrow cover and property insurers have often lacked the expertise to deal with a claim involving data theft or damage.

Likewise, crime insurance policies have only recently started to give cover for social engineering attacks, but generally speaking, the social engineering coverage on cyber policies is broader and has less onerous terms than a traditional crime policy.

Similarly, some professional liability policies offer limited cover for suits arising from data theft, but these policies do not tend to cover any of the first party costs associated with responding to an event, which can be the most important part in determining how the event unfolds.

So, while there may be elements of cyber cover existing within traditional insurance policies, it tends to be only partial cover at best. Standalone cyber policies will generally provide broader cover with less onerous terms and are purpose-built for true cyber exposures.

Most importantly, standalone cyber policies provide access to an incident response service, while traditional policies won't. A property policy does not generally give you access to technically qualified incident response specialists who know what to do when ransomware has encrypted your systems. A traditional crime insurer is unlikely to be able to help when cybercriminals have stolen your data and are holding you to ransom to prevent them from publicly releasing it. A typical professional liability policy won't be able to effectively manage the notification and crisis management costs associated with responding to a rogue employee posting confidential data online.

A standalone cyber policy does all this and more, and brings a level of expertise to handle cyber events effectively and efficiently, with minimum disruption and financial impact to the business.

The short answer

Some overlaps exist (as they do with all lines of insurance) but traditional insurance policies lack the depth and breadth of standalone cyber cover, and won't come with experienced cyber claims and incident response capabilities.

Myth 6

"Cyber insurance doesn't pay out..."

Cyber insurance most certainly does pay out. At CFC, cyber insurance actually has a lower claims declinature rate than most other lines of insurance. In fact, CFC paid more cyber claims in 2017 than ever before and 2018 is on track to eclipse prior years by a substantial amount.

Skepticism around whether cyber insurance pays out often stems from how the product first developed. Cyber insurance was a new and largely untested market and insurers were naturally nervous and wanted to protect themselves. As a result, early cyber policies had risk management warranties in place that required insureds to maintain certain controls for the policy to remain valid. These warranties were often difficult to understand and even harder to comply with, particularly for small business owners, and they would put clients off.

But the market has changed a lot since then. A good cyber policy will now tend to be free from risk management warranties and control-based conditions, meaning that there are unlikely to be any unpleasant surprises when insureds make a claim.

The short answer

The number of cyber claims continues to rise, in terms of both frequency and severity, and insurers are paying them.

[3] Verizon 2018 Data Breach Investigations Report