More cyber insurance myths debunked

[policy wording edition!]

For buyers of cyber insurance, these are confusing times. The news is peppered with stories purporting that cyber policies aren't fit for purpose and even worse, that cyber insurance claims aren't getting paid.

We're here to set the record straight. This is an incredibly important line of cover for modern businesses of all types and sizes, and cyber policies are evolving rapidly to meet their needs. Below you'll find some of the main policy coverage misconceptions we've encountered, and our response to them.

Myth 1

"Cyber events caused by human oversight or error won't be covered"

The reality

While it's true that cyber insurance was primarily developed to deal with malicious cyber events, policies go far beyond this today, covering a wide range of losses caused by human error or oversight, such as lost laptops or social engineering scams. In fact, about 75% of the cyber claims that CFC pays are for events originally caused by some kind of human error.

Myth 2

"Only the legally required costs associated with a data breach will be covered"

The reality

Cover for data breaches is actually incredibly mature, having been an established part of cyber insurance policies for the last decade. Should a cyber event lead to a privacy breach, nearly every policy will pick up the costs associated with regulatory fines and penalties, breach management like the production and posting of letters, post-breach remediation, and crisis communications, even if you are voluntarily notifying costumers.

Myth 3

"System interruption cover will only cover the period of actual system downtime"

The reality

Recognising that business interruption can be felt well beyond the period of actual system downtime, cyber insurance providers have developed this cover considerably over the last few years. CFC's policy, for example, automatically provides a 12-month indemnity period to pick up losses incurred in the long aftermath of a cyber event, and most other providers offer 3-6 months as standard with the option to extend.

Myth 4

"If an outsourced technology provider experiences an issue that leads to a cyber event, it won't be covered"

The reality

This is a relatively outdated concern. Today, any established cyber insurance policy will cover cyber events and system downtime experienced by the insured themselves and at least their third party technology service providers, if not the full supply chain encompassing non-technology service providers too. In addition, data hosted with third parties is also typically covered.

Myth 5

"If a system has been recently updated, it won't be covered"

The reality

Not only are systems updates part and parcel of most business' operations, but it is not in the interests of cyber insurers to discourage businesses from bringing their systems up to date. After all, updates and new system implementation can improve security. For that reason, reputable cyber policies will not look to exclude events arising out of systems that are new or recently updated.

Myth 6

"If a contractor causes a cyber event, such as a data breach, it won't be covered"

The reality

The majority of cyber policies are designed to cover the entirety of business operations. Just as with outsourced technology providers, CFC's policy is designed to cover claims caused by third party contractors. In fact, we take it one step further and cover our policyholders' data wherever it is hosted and whomever it is breached by.

Myth 7

"It's difficult to get cyber incident support and notify claims"

The reality

It's in the interests of insurers to encourage quick and easy engagement with policyholders if a cyber event occurs. If the last two decades of underwriting this class has taught us anything, it's that good incident response is key in containing the loss to a business and the subsequent cost of a claim. CFC – along with much of the industry – is taking steps to make reporting a claim as easy as possible through 24/7 hotlines or innovations like our cyber incident response app.

Myth 8

"In the event of a cyber incident, businesses cannot choose the IT, legal, or PR specialists they work with"

The reality

While we can't speak for the entirety of the market on this matter, this is certainly untrue for CFC. While we offer policyholders quick and easy access to a global panel of high-quality incident response partners, we understand that some businesses have their own providers and therefore don't typically limit our policyholders to working with our panel alone.

Myth 9

"Cyber insurance doesn't pay out"

The reality

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 2018, we paid over 1,000 cyber claims and we expect that number to increase by 50% in 2019. In short, the number of these claims continues to rise and insurers are paying them.