Five reasons to act quickly during a cyber event

MPR

TOP 5 TIPS

Incident response providers have observed that a strong theme emerging, even where a cyber insurance policy in force, is poor escalation from the discovery of the cyber event to the point at which the appropriate experts are engaged. This almost always leads to the situation taking longer to resolve, introducing potential additional disruption and more costs. Hesitating with a cyber event is ill advised, and here are just five reasons why:

1

The first few hours are vital.

Early escalation allows the correct experts to engage quickly, triage the incident and organise a tailored action plan for the organisation. It is widely accepted that the first 48 hours following discovery is the period which ultimately dictates the eventual outcomes. So, make sure that the cyber policy not only has access to these crucial vendors, but also helps to coordinate the organisation through the process.

2

The ICO. To notify or not to notify?

The ICO has been (and will continue to be) very busy post GDPR implementation, yet their notification advice might not be what one might expect:

"You need to consider the likelihood and severity of any risk to people's rights and freedoms… if it's unlikely then you don't have to report it.

Having a cyber policy, with access to experts, will place the buyer in a much stronger position to make that initial assessment and establish any notification requirements.

3

If the breach event does qualify for notification, then speed is of the essence.

The organisation must:

"notify ICO without undue delay (within 72 hours); give a description of nature of breach & number affected; provide specific categories of data subjects (gender, age etc..); and detail the likely implications of the breach and what measures have been taken to mitigate."

So, it becomes clear that engaging experts immediately (such as forensics, crisis response and legal services) could prove vital, particularly in relation to the mitigation of any potential fine that may be levied by the ICO.

4

A black mark on the claims record?

Some policyholders may hesitate because they fear it will form part of their claims experience (i.e. a call to a helpline may be taken as a circumstance or notification to the insurer). Look for a cyber policy that allows an immediate incident response scenario without incurring a claims notification.

5

Worried about the retention/excess?

Another potential reason for delay might be that a policyholder would opt to handle the event in-house rather than incurring lawyer or vendor costs (as part of their excess/deductible), believing the matter is under control. Look for a cyber policy that has a zero deductible for the immediate incident response service, taking away that potential obstacle to the expedient handling of a cyber event.

MPR's CIRI policy specifically has an 'Immediate Incident Response Expenses' definition, because we want the policyholder to act without hesitation, even if they feel they may be able to handle it themselves. To facilitate this, we deliberately apply a £0 deductible applicable to this service, and it won't constitute a notification to MPR unless the severity means that it progresses to the crisis management stage.

To be solid, insurance must be flexible