The importance of a tailored cyber insurance policy

The continuing risk of cyber attacks, which can be devastating for businesses and are impossible to defend against entirely, has brought into focus the potential of cyber insurance as a means to soften the blow in the event of a cyber attack. While the US market for cyber insurance is significant already, in the UK it is less advanced, although as Tom Webley, Peter Hardy and Eleanor Nugent of Reed Smith explain, it is developing. In this article, Tom, Peter and Eleanor discuss the response of the insurance market to the risks, what drives growth in cyber insurance policies, and the steps organisations putting cyber insurance policies into place should take in order to ensure they are adequately protected.

It is no mystery why cyber security is such a hot topic. Almost everything in our lives is becoming digitised and, for many companies, their data is now their most valuable asset. This is particularly true for any organisation that holds the personal or financial data of its customers.

Any company that holds sensitive financial data is likely to be at risk of attacks or breaches. This will naturally include companies that handle payments or hold financial information. The data held by such companies would be a tempting target for cyber thieves and any breach (whether deliberate or accidental) could have considerable knock-on effects if it results in customers’ payments not going through.

Any company’s ‘crown jewels’ need protecting. However, statistics suggest that, no matter how good an organisation’s defences, cyber attacks are almost impossible to prevent. This is where insurance should come in. Despite this, the cyber insurance market in the UK is surprisingly underdeveloped and many companies still see it as at best, an add-on to their traditional policies. However, this is beginning to change and the UK market is starting to catch up with its far more advanced US cousin.

Given the huge financial impact of any breach, it is important that organisations realise the importance of having adequate insurance cover before they become a victim of an attack or breach, rather than as an afterthought. If in doubt, companies should speak to specialist cyber insurance brokers to ensure that there is adequate cover in place.

What are the potential risks?
One of the difficulties in putting up adequate defences against cyber attacks or breaches is that cyber attacks can take many forms and evolve as rapidly, or in some cases more rapidly, than the technology used by companies.

In general terms, the risks fall into four very broad categories:
(i) Negligent acts or omissions of employees or third party providers;
(ii) Hacking;
(iii) Misuse of private data or information; and
(iv) Software issues.

Whether deliberate or accidental, the consequences can potentially be catastrophic and might include:
● Vital digital assets being lost or stolen;
● Business interruption or denial-of-service;
● Extortion or being held to ransom; or
● Reputational damage.

It is quite possible that some or all of these consequences could happen at once. Consider an example of a financial services company’s systems being attacked. The hackers get into the system and extract key personal information about that company’s customers, leaving the company unable to access it. What might be the consequences for the company?

Having lost valuable data, the company might not be able to provide any services, leading to the risk of business interruption. There could be serious public relations issues in relation to the impact that the breach has on its customers. In addition to these direct, or first party, risks there are the indirect consequences. The breach might be a sign of a lack of adequate systems and controls, which could lead to a very expensive regulatory investigation and/or fine.

Where there is blame, there is a claim. Customers might have a claim against the company as a result of the breach. The issue with cyber breaches is that they can affect any number of customers. Therefore, if one customer has a
CYBER INSURANCE

claim, all customers might.

Data malfunctions could just as easily happen as a result of an
innocent mistake by an employee
or software failure as they could
from a firm’s systems being hacked.

How tailored a company’s cyber
insurance policy should be to
ensure that both deliberate and
inadvertent attacks are covered, is a
question for insurance markets and
policyholders alike.

How has the insurance
market responded to the
risks?
The UK insurance market has
responded to cyber threats far
more slowly than the US. The US
market has embraced the concept
that cyber insurance is a necessity,
not simply an esoteric product that
only a few types of firms need. In
fact, for many organisations in the
US, having cyber insurance in
place is a regulatory obligation and
is seen as a key part of the
company’s risk management and
regulatory compliance.

While approximately 90% of
cyber insurance premiums are still
from the US, the UK market is
waking up to the importance of
specifically insuring against cyber
security breaches. As with the US,
to a certain extent, this drive is
being led by the regulators, HM
Treasury, the Prudential Regulation
Authority and the Financial
Conduct Authority are focusing
intently on the need to improve
organisations’ resilience to cyber
attacks. They are of the clear view
that cyber security is not merely a
technical issue, but something that
needs to be considered at board
level. Regulated firms should not
be in any doubt that they need to
have adequate systems in place to
defend themselves as best they can
from cyber attacks or to avoid
accidental breaches.

As with the US, there are a
number of reasons to suggest that
regulatory interest is likely to have
a knock-on effect on the cyber
insurance market. The first is a
direct consequence. If the
regulators believe that cyber
security needs to be a key part of
risk management, a natural
consequence will be that having
cyber insurance in place will
eventually be a regulatory
requirement. This will avoid the
risk that businesses will incur
enormous losses as a result of
breaches which will either leave
them financially unstable or which
they will try to pass on to their
customers.

In addition, regulated
organisations will want to insure
themselves specifically against any
consequences resulting from a
regulatory failing in relation to
cyber security and the vast amount
of back-end litigation from
customers that often follows
regulatory sanction.

Another reason to think that
regulatory interest in cyber security
could drive the cyber insurance
market is that where regulated
entities lead, others tend to follow.
If the need for cyber insurance
becomes an obligation or
commercial requirement for
regulated organisations, the range
and availability of cyber insurance
products is likely to expand for all
organisations.

However, we are not there yet in
the UK. Given the considerable
risks posed by cyber security
breaches, the number and uptake
of specific cyber policies is
surprisingly small. There has been
a dramatic rise in both the
frequency and cost of cyber
attacks. The nature and
sophistication of these attacks, as
well as the potential financial
consequences for the victim, mean
that it is impossible to put in place
impregnable defences. This creates
an obvious need for insurance.

However, until recently the UK
insurance market did not offer
dedicated cyber insurance
products, and even now such
policies are not as all-
comprising as they could be,
continuing to expose policyholders
to certain types of cyber breaches.

This is starting to change and the
UK insurance market is starting to
become alive to the need for
specific products covering these
risks. Policies are now available to
deal specifically with the direct
risks (such as the loss of valuable
data or business interruption) and
indirect risks (including claims
brought by third parties pursuant
to a cyber attack). Given the
increasing threat, this proliferation
of cyber insurance products is
likely to be a trend that continues.

What this is also likely to mean,
however, is that cyber-related issues
are going to become increasingly
excluded from traditional policies.

What steps should
organisations/risk managers
take to ensure there is
adequate protection?
As cyber insurance becomes both
more available and more necessary,
risk managers and organisations
generally will have to consider very
carefully what cover they need.
Clearly a ‘one-size-fits-all’
approach will not suffice and a
careful consideration of the specific
risks faced by each organisation
will be required. It is vital that the
insurance cover in place is tailored
to match the specific risks faced by
the business and that any potential
gaps left by the traditional policies
are filled.

This will involve a number of
considerations, including:

What are the specific risks faced
by the business?
Each business will be different and
so the risks faced will be different.
It is important to ensure that the
insurance cover is suitable and
adequate for that particular business model. This analysis will have to include an assessment of the direct risks to the business (first party risks) and the potential liability to third parties caused by any breaches (third party risks). In general terms, the areas that will need to be included in any insurance cover are likely to include:

- Any costs relating to claims and defences to regulatory action for breaches of privacy and data protection (including investigation and forensic IT costs);
- The losses suffered as a result of business interruption and distributed denial-of-service issues (inundating websites with visits, resulting in a slowed or unavailable service, particularly devastating to online retailers);
- The costs of recovering data and repairing software having been hacked; and
- Claims relating to breaches of intellectual property.

A year is a long time in the fast moving world of technology and it will be necessary for an organisation to ensure that the terms of any cyber insurance policy that it has in place are not so focussed on the current threat that they would not respond to and protect against future breaches, which might take a different form.

Will deliberate and accidental acts be covered?

When people think of cyber security breaches, people often think of hacking. This would obviously require insurance cover for losses caused by criminal acts. However, even if such a policy were in place, it will be important to ensure that there was no terrorist exclusion which would apply. Equally important is the need to make sure that there is civil cover for losses caused by innocent or negligent acts or omissions by employees or third parties, as these can have as serious consequences as a criminal attack.

Who is covered?

An organisation might be protected for cyber-related risks, but what about its management? Regulators across the globe are being vocal in their intention to hold individuals personally accountable for issues which arise, and cyber security will not be an exception. Organisations will need to ensure that Directors and Officers Liability policies offer adequate protection to senior individuals to deal with the fallout from any cyber security breach.

How will the policy respond if there is a claim?

Cyber insurance is largely untested in the UK as it is so new. It will be important for anyone considering the terms of any policy to keep an eye on developments in the US (a more established market) to see in what circumstances cover is being denied by insurers and make sure that any such issues are avoided as far as possible when the exact terms of the policy are being put together. For example, there have been cases in the US where cover has been denied on the basis that an employee accidentally downloaded malware.

Conclusion

Assessing how best to insure against cyber risk is not an easy exercise and there is a lot at stake. Risk managers and organisations should work with specialist insurance brokers to make sure that they have all of the protection that they need to avoid the position where a cyber security breach causes a massive loss to the business, only to find that it falls straight through a gap in insurance cover, even within cyber-specific policies. As with everything, adequate insurance is required to help ease the pain should the defences fail. This will become increasingly important as, with the growth of specific cyber insurance products, traditional policies are more and more likely to exclude cyber-related risks.

Tom Webley Counsel
Peter Hardy Partner
Eleanor Nugent Trainee Solicitor
Reed Smith, London
T:webley@reedsmith.com
PH:0207 334 8918
enugent@reedsmith.com

05