Hacked Off – Cyber Attacks and Cyber Risk

The issue of IT failure and cyber security has never been a greater risk factor for businesses.

Cyber Crime

Cyber crime is on the rise: we hear that from our clients and we see it every day in the news. As an example, the records of over 215,000,000 individuals were leaked in August 2018, including data from a Chinese hotel chain that related to up to 130,000,000 customers.

In May 2017, elements of the NHS were effectively crippled by the "WannaCry" ransomware attack, which locked computers, encrypted files and demanded payment in cryptocurrency. WannaCry attacks were directed at other high profile targets, such as the Russian Interior Ministry, FedEx (the international shipper) and Telefónica (the Spanish telco).

To put it simply, all companies are at risk of a targeted cyber attack. However, not all companies have large resources to spend on IT security measures. All organisations, including mutual companies, are required by the ICO to have in place breach response plans[1]. Under the General Data Protection Regulation, there is a requirement to report to the regulator within 72 hours of an organisation having become aware of an issue. That is a tough deadline to meet and requires organisations effectively to frontload work by considering it would work in practice and building a plan around it to help things run as swiftly as possible if organisations need to "hit the red button".

Incident response plan

Many organisations will not have such plans in place, but it matters from a risk reduction perspective. Consider the issues that a response plan would require and whether organisations will know the answers immediately:

- What does the business consider a "breach"?
- What guidance do employees have on what to report and who to tell?
- Who gives the initial analysis of whether something is an issue of concern?
- How does the business define what needs to be reported to the regulator?
- How does the business define what needs to be reported to the individuals affected?
- How does the business define what needs to be reported to the police?
- How does the business define what requires a public statement?
- Who drafts those reports?
- Who signs off on those reports?
- When are third parties like solicitors or forensic IT investigators brought in?
- How is the board kept informed of what has occurred?

It is, therefore, fairly uncontentious to say that every business should have an incident response plan. It makes business sense and legal sense. It may, therefore, come as a surprise that only about 30% of organisations actually have an incident response plan[2]. 70% of organisations are, therefore, at risk of a sub-optimal response in the event of a cyber incident. Unsurprisingly, therefore, we are seeing a lot of client interest in our offering around cyber incident response plans and we are seeing businesses across all sectors begin to put in place the tools that they will need should the worst-case scenario arise.

Insurance

Due to the risks, it is no surprise that this is an area for which insurance coverage is being sought. However, this is a developing area. As part of their risk management programme, organisations need to consider the value of obtaining cyber insurance. If insurance is obtained, knowing when to call the insurer, who to make the call and what is covered is crucial to the cyber incident response plan. Needless to say, considering this for the first time when an organisation is in the middle of an incident is unlikely to reduce stress.

---

1 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

2 PwC Global Economic Crime and Fraud Survey 2018

The specialist cyber policies typically cover the following which may occur following a cyber breach:

- the costs of notifying relevant regulators and affected individuals;
- the PR costs of responding to an incident;
- the legal costs of dealing with third party civil claims by affected individuals;
- damages payable to third parties;
- the costs relating to regulatory investigations;
- the IT costs of restoring damaged data and of investigating the cause of the breach;
- business interruption costs; and
- the costs of paying ransom to hackers (e.g. ransomware) following a hack.

Some of the above losses may be insured under an existing insurance programme e.g. business interruption or financial crime policies. However, care needs to be taken in relying on such policies due to their limitations in relation to cyber losses.

Terrorism

War exclusion clauses in insurance policies typically exclude coverage for acts of war; including but not limited to invasion, revolution and acts of terrorism. However, as state-sponsored cyber-attacks appear to be on the increase, is has to be considered whether insurance against such cyber-attacks can be effective. Are these attacks actually acts of terrorism?

An act of terrorism is defined under Section 1(2)(e) of the Terrorism Act 2000 as an action *"designed to influence the government or an international governmental organisation…and the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause…and it is designed seriously to interfere with or seriously disrupt an electronic system".* This definition would potentially cover many of the high profile attacks that we read about every day in the newspapers, especially as S1(4)(a) states that the requisite *"action includes action outside the United Kingdom"*

An insurer seeking to rely on an exclusion in a policy subject to English law would need to prove, on the balance of probabilities, that the loss fell within the exclusion. This could present difficulties given that with state-sponsored attacks, the state where the attack took place will not publish all the evidence relating to the event, merely its conclusions that an attack has taken place.

Whilst it may be possible to infer what the motives of a hacker are from the known facts - for example in relation to the attacks on the Organisation for the Prohibition of Chemical Weapons - it is highly unlikely that there will be any direct evidence from the alleged hackers. This will problematic if it is necessary to decide whether a particular act was an act of terrorism or merely a hack for commercial purposes, which is less likely to be excluded.

Nevertheless, from a policyholder's point of view, a policy which excludes state sponsored attacks is of questionable worth, given that this is perhaps the area of greatest risk. Ideally an insured would be able to agree with insurers that the wording of an exclusion is as limited as possible.

For further information, contact Paula Gaddum, Partner, insurance and Reinsurance, Eversheds Sutherland: PaulaGaddum@eversheds-sutherland.com