Negotiating key cyber exclusions

Differences in policies make understanding what is and is not covered very difficult

Thomas Bentz
Holland & Knight

There is no shortage of stories about data breaches. According to the Washington Post, federal agents notified more than 3,000 US companies their computer systems had been hacked in 2013. It seems like a new cyber event is reported nearly every week. As these stories continue to grow in number, corporate America has started to explore ways to insure against this risk.

Unfortunately, cyber policies are both complicated and rapidly changing. There is no standard policy form, which means the coverage offered by one insurer can (and often does) differ dramatically from that offered by another. There is little agreement between insurers on what should be covered, when the coverage should be triggered or even how basic terms should be defined.

These differences make understanding what is and is not covered very difficult. It also makes it nearly impossible (or at least foolish) to purchase this coverage based on price alone. Insureds need to negotiate improvements to their policies, but knowing what to negotiate is a formidable challenge.

The following is intended to offer some tips on how to negotiate the exclusion section of a cyber liability insurance policy. Although the tips below are limited to the exclusions section, it is not the only section of a cyber policy that must be negotiated.

Bodily injury/property damage exclusion

Some cyber policies exclude coverage for any claim “arising out of, based upon or attributable to” property damage and bodily injury. This is too broad. Instead, the quoted language should be replaced with the word “for”. This addresses the situation when there is an injury that is followed by a secondary lawsuit claiming a failure to supervise.

A company’s general liability policy might cover the direct liability associated with the injury but may not cover the subsequent lawsuit. With the change to “for,” the firm’s cyber liability insurance policy could provide coverage.

The bodily injury/property damage exclusion should also include a carve-back clause for mental anguish, emotional distress and shock caused by a cyber event. Many plaintiffs will allege these types of damages after a breach. Many insurers will only provide this coverage upon request.

Mechanical/electronic failure exclusion

The mechanical/electrical failure exclusion removes cover for claims caused by a mechanical shutdown such as when your computer stops working. This exclusion needs to be limited so if a cyber criminal causes the failure by means of a virus or spam attack, for example, the policy may respond.

Acts of war, invasion and insurrection exclusion

Many cyber policies have an exclusion for acts of war, invasion, insurrection and so on. Some policies also exclude acts of terrorism. This can be problematic in the cyber context, as almost all cyber attacks could be considered acts of terrorism. A strong cyber policy should not reference terrorism in this exclusion.

Laptop exclusion

Some cyber liability policies exclude coverage for portable electronic devices. This can severely limit the coverage provided by a cyber policy. Insureds are well advised to remove this exclusion if at all possible. Some insurers will only remove this exclusion if an insured agrees to encrypt the data contained on the portable devices.

Illegal/fraudulent conduct exclusions

Most cyber policies include exclusions for fraud, intentional and illegal misconduct. How a policy determines whether a conduct exclusion applies, when that determination may be made and what gets to make this determination is extremely important.

For this reason, many insureds prefer a “final, non-appealable adjudication in the underlying action to establish the alleged wrongful conduct occurred. Without such a final non-appealable adjudication of wrongful conduct, the exclusion does not apply (ie, there is coverage available from the policy).”

It is very important the conduct exclusions only apply to intentional/fraudulent acts committed by the insureds. Intentional/fraudulent acts by others should be covered.

Prior acts exclusion

A typical prior acts exclusion excludes coverage for any claims based upon wrongful acts that occurred before a certain date – often the inception date of the policy. Given the claims made nature of the cyber liability insurance policy, a prior acts exclusion has the potential to strip the cyber liability policy of all or most of its value and insureds should avoid such an exclusion whenever possible. This is particularly important for cyber liability policies because cyber criminals and hackers may install spyware, viruses and other malware long before a breach is discovered and the policy incepts.

The insured v insured exclusion

The insured v insured exclusion states the policy will not cover a claim made by one insured against another insured. However, many cyber liability insurers will agree to “carve out” certain insured v insured claims for various reasons, including the following:

- failure to protect confidential information;
- failure to disclose a breach event in violation of law;
- the unintentional failure to comply with the insured’s privacy policy; and
- violations of privacy statutes.

Often these carve-backs only relate to a specific coverage grant, so it is important to review each coverage grant separately.

Exclusion severability

Finally, to ensure the acts of one insured person do not affect coverage for other insureds, a cyber liability insurance policy should contain an exclusion severability provision. An exclusion severability provision states no wrongful act committed by any one insured shall be imputed to any other insured for purposes of determining the applicability of any of the exclusions.

There are a number of cyber liability insurance policies available today and they are highly negotiable. By taking the time to negotiate improvements, companies can greatly improve the chances their cyber liability policy will protect them when they need it most.

Thomas Bentz leads Holland & Knight’s D&O and management liability insurance team.