Cyber Insurance: A Complicated Necessity

Authors: Doug Tait

published 05/03/2018

Whether an organization suffers a cyber incident is no longer a question of “if” but “when” and as such, cyber security is a risk to be managed not solved.

The basic game plan of cyber risk management is to minimize risk. However, no amount of technology, policies or training can guarantee that an organization will not suffer a cyber security incident. Accordingly, once an organization has minimized its risk using technology, policies or training, it should consider transferring the risk that cannot be removed through investment in further security measures, to a cyber insurance policy. In fact, due to the increasingly high costs associated with a cyber incident, many consider cyber insurance not as a mere consideration but rather as an absolute necessity.

Unfortunately, organizations can easily become confused about the cyber insurance that may best suit their needs. Cyber insurance is a relatively new insurance product and policies are developing and evolving as the cyber threat landscape shifts. Unlike many insurance products which are now fairly standardized, cyber insurance policies currently have very little standardization and policy wording may vary greatly between policies. While all the policies may be called cyber insurance policies, not all insurance providers offer the same thing. The subtleties between policies may not be readily apparent but there could be very important difference. It is therefore critical that an organization carefully and closely read, or have a trusted advisor accustomed to dealing with cyber insurance policies review and advise as to, the policy fine print to ensure that the organization is actually getting the coverages it is expecting. Which costs are covered and which costs are not, is not the kind of information an organization wants to learn after a cyber incident occurs.

At a fundamental level every cyber insurance policy on the market provides coverage for a data breach. Two types of coverage are typically involved; first party and third party.

First party coverage covers expenses the insured itself incurs in the event of a cyber incident - forensic costs, notification costs where a party has to be notified, credit card monitoring costs, etc.

Third party coverage is what the insured would rely on if it was sued by third parties - claims, class action lawsuits, some regulatory coverage, etc.

Another type of coverage typically found in a cyber insurance policy is network security coverage. This provides coverage if something happens with an organization’s network as a

result of a covered cause and an organization's data is damaged or its customers can't access the network, etc.

Some coverages that an organization may think it has coverage for but may not, depending on the policy wording, are:

1. Social Engineering - losses resulting from social engineering attacks are not typically covered under cyber insurance policies as social engineering is generally not considered computer fraud. This however is an emerging area and in the meantime coverage for social engineering may be obtainable under commercial crime coverage. If social engineering coverage is available it will typically take one of two forms, one of which will only cover social engineering in the event someone is impersonating an employee within the insured's organization. This form would not cover a fraudulent e-mail purportedly sent on behalf of a service provider, vendor or client.

2. New Hardware - in a cyber insurance policy, digital assets coverage typically addresses corruption or destruction of data or software and not property damage or hardware replacement. So if a ransomware attack corrupted an organization's computers to the point that replacement was necessary, digital assets coverage would not cover that loss.

3. Software upgrades - cyber insurance policies typically don't cover new versions of software. So if, at the time of an attack, an organization is using legacy software like Windows XP, the insurance will not replace that with Windows 10.

4. Third-party errors - some cyber insurance policies extend coverage to third-party providers others do not. It's important for an organization to ensure that its coverage includes any service providers or other third parties the organization uses. If something was done improperly not by the organization but rather by a service provider or other third party the organization uses, and that causes the organization to suffer damage, the organization wants its coverage to extend to the service provider or other third party error. Typically this kind of error would be excluded from policies but there is separate cyber insurance coverages that address this type error.

5. Bodily injury - if a cyberattack hits a connected vehicle or piece of medical equipment or a bug in manufacturing or industrial equipment leads to bodily injury, most cyber insurance policies won't cover medical costs.

6. Intellectual property theft and reputation damage - this is a difficult area for insurers because it's hard to quantify the loss. Currently coverage is limited but demand is growing so it's something insurers will need to address.

Other costs which are typically not covered in a cyber insurance policy include public relations coverage, data breach law compliance/notification costs, regulatory investigations costs, including subsequent fines and penalties.

Cyber insurance is expensive and the deductibles are high. Therefore organizations need be sure that any cyber insurance policy purchased provides coverages that are tailored to their business requirements and designed to fit their cyber risk profile. In that regard, as the cyber insurance market is still relatively new and far from standardized, insurers are somewhat open to negotiating policy provisions or narrowing or eliminating exclusion. This willingness to negotiate can lead to an organization getting coverages that best suit its particular needs.

When an organization applies for cyber insurance coverage the questions an insurer will want answered before providing a quote may vary from a few questions to multiple pages of questions. While the information sought will vary depending on the insurer, aside from the usual questions about whether the organization has ever experienced a cybersecurity incident, ever made an insurance claim involving cybersecurity, ever had an insurer cancel a cyber insurance policy or refused to renew one or aware of any facts which may give rise to a possible claim, typically questions will focus on:

(a) the kind of data the organization holds;

(b) the kind of security software and hardware the organization utilizes;

(c) whether encryption is being utilized;

(d) a description of the organization's backup system and processes;

(e) whether the organization has and follows written security policies;

(f) whether there is mobile device security in place;

(g) whether the organization follows general best practices regarding passwords, access control, patching and upgrading;

(h) whether the organization complies with any specific cybersecurity standards;

(i) whether employees are trained in cybersecurity and how often they train; and

(j) what steps are taken to secure data when an employee leaves the organization.

It is extremely important that the application for coverage be carefully completed. If a policy is issued the application becomes part of the policy and any misrepresentation, even made inadvertently, could, at worst, invalidate the coverage or, in the very least, create a coverage dispute. Accordingly, when filling out the application an organization needs to have the right expertise, HR, IT and Legal, around the table. They can assist in not only ensuring that there is a full understanding of the questions but also in the development of the answers. If a question is not fully understood, then clarification from the insurance company should be sought before the question is answered. There may even be a need to talk to service providers or vendors if questions pertain to what they are doing and the organization does

not have internal knowledge to answer that.

Once a cyber insurance policy is purchased an organization cannot just put it away and forget about it. It is important to have a full grasp of what the policy may require. For example, if representations were made in the application that the organization was doing certain things, like encrypting data, then the organization needs to make sure it's doing that. Policies can have strict requirements around whose knowledge of a claim is relevant in terms of giving notice or who has to be given notice in the event of a claim and when that notice has to be given. Its critical then that individuals within the organization are identified and tasked with managing these requirements and conditions.

Organizations should also amend their incident response and other similar plans to ensure that they reflect the need to give notice to the insurer and particulars around the giving of that notice. Without such an amendment, when an incident occurs and everyone is running around, it's easy to forget to provide the notice.

Finally, it's important that an organization maintain awareness of emerging threat risks and what insurance coverages may be available to address these new risks. If appropriate these coverages should be added to the policy.

If your organization already has a cyber insurance policy you should review it carefully to see if it contains the coverage your organization actually requires. If your organization does not already have a cyber insurance policy now is the time to start considering one. Remember though, cyber insurance is only one part of an overall cyber risk management strategy and is not a replacement for that strategy.

---

articles, you should seek and be guided by legal advice based on your specific circumstances. We would be pleased to provide you with our assistance on any of the issues raised in these articles.

