NYMITY

Privacy Interviews with Experts
June 2014

Toronto / Washington DC / Brussels
www.nymity.com

Rick Betterley

President
Betterley Risk Consultants, Inc.
United States

What is Cyber Insurance, anyway? A Checklist for the Privacy Office

Insurance can be a bit of a mystery, especially Cyber/Privacy insurance, where no two policies are alike. When selecting a policy, there are many options, and a few things to watch out for. Rick Betterley helps explain the options so organizations can obtain the coverage they want.

Rick Betterley, the President of Betterley Risk Consultants, consults with clients about their insurance risks, types of insurance needed, and assists in negotiation. Betterley Risk Consultants is an independent risk management consulting firm providing expertise and objectivity in property & casualty insurance and alternative risk financing mechanisms. It does not sell insurance products or related services.

Betterley is also the author of Cyber/Privacy Insurance Market Survey, published annually in The Betterley Report (www.betterley.com).

Nymity: What is Cyber Insurance?

Betterley: Cyber insurance is a specialized type of insurance that covers the risk of a data loss by the insured. Whether loss is the result of a data breach caused by a computer hacker or a simple theft of a laptop, the theft of funds via computer, or a business interruption caused by a virus, Cyber insurance policies can help.

Despite its name, Cyber insurance isn't just for insureds that do business via the Internet – many potential insureds think that they don't need the coverage because they aren't a target or don't sell online. But Cyber insurance can actually cover data loss in any form – including paper!

Nymity: What can cyber insurance cover?

Betterley: Each insurance company's policy form is different, and not all provide the same types of coverage. But generally the following types of coverage can be included in a Cyber policy:

- Liability insurance:
  - To protect against lawsuits that allege a failure to protect confidential information
  - Will pay for the legal costs, and if needed, judgments or settlements
- Breach Response Costs – incurred by the insured following a breach, which may include:

  - Notifying the affected persons – an obligation imposed by law or regulation
  - Credit monitoring for the affected persons – which helps make the affected person feel taken care of, and can help reduce the likelihood of lawsuit
  - Breach coach/legal services – to guide the insured through the process of responding to a breach
  - Public relations – to help the insured minimize damage to its reputation
  - Forensics – to pay for the cost of technology consultants to identify the source of the breach and how to fix it
  - Repair – to pay for the cost of fixing the weakness that allowed the breach (this coverage is rarely offered)
- Fines and Penalties:
  - Imposed by regulators
  - Imposed by credit card processors
- Extortion:
  - To cover the cost of ransom-type payments to cyber criminals that threaten to release private data, shut down websites, or corrupt data (similar to kidnap and ransom insurance)
- Theft:
  - Of the economic value of funds, goods, and services
- Business Interruption/Extra Expense and Damage to Data – a much more traditional coverage often found in property policies, but sometimes offered by Cyber insurers:
  - Loss of income minus non-continuing expenses arising out of the inability to operate
  - Extra Expense to continue or more quickly resume operations
    - i.e., a network, website, etc.
- Optional coverages:
  - Media Liability

Nymity: What are the risks to organizations in not purchasing cyber insurance or in purchasing the wrong type of cyber insurance?

Betterley: Not being covered; cyber breaches are surprisingly expensive, easily reaching $50/record breached for the expenses that might be insured. We expect that many victims of cyber breaches will find that the cost of the breach and the damage to their reputation will doom the company.

Nymity: What are the biggest barriers to an organization's purchase of cyber insurance?

Betterley: Great question; lack of knowledge by both the organization and their insurance broker, the belief that 'it can't happen here', and the hope that they are not a target. Organizations often resist new types of insurance, and when they aren't aware of it or don't have confidence in their knowledge, tend not to buy.

Nymity: What should an organization watch out for when purchasing cyber insurance?

Betterley: Things to watch out for:

In general:

- Be sure that data is covered anywhere, not just while on your network or in your possession. You should be sure it is covered while in the hands of others, such as your vendors. And this should be worldwide, not just in, say, North America.

- Be sure that the definition of the data being covered includes all types of data, not just electronic data. Many data losses still include paper files.
- Don't accept a policy that excludes breaches that arise from a failure to patch (or update) software. After all, if your cyber security was perfect, you wouldn't need the coverage.
- Only buy from insurers that have been offering cyber coverage for at least a few years; there are many new entrants into this space, and not all of them will have a profitable experience. You don't want to be nonrenewed by a Cyber insurer that has decided to no longer offer this coverage.
- And don't buy from an insurance broker that doesn't have substantial experience in Cyber coverage

Sublimits:

- Policies typically have a lower limit (i.e., sublimit) for certain types of claims, including the type you are most likely to have – Breach Response costs. Make sure that sublimit is high enough to cover your foreseeable exposure. Breach Response cost limits of up to $10 million (or more) can be purchased.

Liability coverages:

- Should include class action lawsuits, not just lawsuits by individuals
- Be sure it covers Intentional Acts, at least until a finding of intent is rendered by a court
- Punitive and exemplary damages should be included, at least where insurable by law (look for so-called Most Favored Venue wording)

Breach Response coverages:

- Make sure that you can select the services provider handling the response. Some vendors have low prices but try to upsell your customers/clients while they are alerting them to the breach.
- Make sure that the service providers include those that you want to work with; not all insurers include all possible providers, and may not include one that is acceptable to you. This is especially important for Notification and for Legal (breach coach) services.

Fines and Penalties coverages:

- Make sure that this coverage is offered
- Try to include the actual cost of the penalty, not just legal services related to the penalty
- If you accept credit card payments, PCI fines and penalties are a real threat and coverage for them is valuable

Nymity: What other services are offered by insurers that organizations may benefit from?

Betterley: Most policies offer valuable services that help you prevent or minimize a breach. These are offered, usually for free, to most insureds, but not all services are equal. Many are simple self-audits or education materials easily available for free on the Internet. The better services provide personalized services to answer questions, offer tools to help assess and measure risk, and community support for IT Security professionals.

Since Cyber insurance doesn't cover many of the losses that result, including injury to reputation and management's time, to say nothing of hits to the insured's market cap, these services may well be as important as the actual insurance.

Nymity: What are the top 5 recommendations you would give organizations considering the purchase of cyber insurance?

Betterley: 1) Don’t put off looking into cyber insurance 2) Make sure your broker has substantial experience in cyber, ideally in your industry; if not, retain an expert who is 3) Be careful about buying insufficient limits; insurance is important, enough insurance is critical 4) Only buy from an insurer with substantial experience in cyber 5) Don’t ignore the value of value-added risk management services