



THE BETTERLEY REPORT

CYBER/PRIVACY/MEDIA LIABILITY MARKET SURVEY – 2011:

Many More Carriers in This Market, and Numerous Recent Data Breaches:

Will Coverage Remain Available?

Richard S. Betterley, CMC
President
Betterley Risk Consultants, Inc.

Highlights of This Issue

- *New Carriers Pour Into the Market*
- *Carriers Add Media Liability Coverage Options*
- *Frequent Data Breaches – Will They Increase or Decrease the Use of Breach Notification Services?*

Next Issue

August

Private Company Management Liability Insurance Market Survey 2011

The Betterley Report

Editor's Note: In this issue of *The Betterley Report*, we present our annual review and evaluation of insurance products designed to protect against the unique risks of data for organizations. This activity could be customer/client records, e-commerce (selling products, services, or content), or social networking.

Social media has become a focus of liability for some insureds and their advisors; although there are few claims arising out of social media, the dramatic rise in Facebook, LinkedIn, Twitter, and others is fueling interest in coverage. For many insureds and their brokers, 'cyber' means the Internet, so cyber coverage must mean insurance for bad things that happen on the Internet.

Cyber carriers are responding to this interest

by offering media liability coverage options in their policies. In order to try to sort through these coverages, we have added three new Media Liability tables for our readers.

Cloud computing is a rapidly-emerging cyber risk - we asked attorney Paul Paray of Wilson Elser for his thoughts on exposures and coverage; his article follows this article.

Note that this Report does not focus on coverage for organizations that are simply using the internet for tasks such as e-mail, or on technology providers that support e-commerce, such as internet service providers, technology consultants, and software developers. That market is reviewed in our February issue, *Technology E&O* market survey.

One thing we would like to point out is the difficulty in separating Technology products from Cyber Risk products; for many carriers, the same base product is used, then adapted to fit the technology service provider insured or the Cyber Risk insured. Where the carrier has a separate product, we reviewed here their Cyber Risk product; if it is a common base product, we included information about both.

In looking at our information, if you see that a certain carrier's policy does not include, for example, Errors & Omissions coverage, keep in mind that this coverage is most important to a service provider and that the same carrier might have a separate product for those insureds. You will probably find that product reviewed in our February issue.

The types of coverage offered by Cyber Risk insurers vary dramatically. Some carriers offer coverage for a wide range of business activities, while others

List of Tables

Contact and Product Information	17
Product Description	26
Market Information	37
Limits, Deductibles, Coinsurance, and Commissions	42
Data Privacy: Types of Coverage and Limits	45
Data Privacy: Coverage Provided	56
Data Privacy: Coverage Triggers	61
Data Privacy: Types of Data Covered	65
Data Privacy: Remediation Costs Covered	70
Data Privacy: Remediation Coverage Services	74
Media Liability – Business Activity Coverage Limitations	78
Media Liability – Personal Injury Rights	83
Media Liability – Intellectual Property Rights	86
Security Assessment Requirements	93
First-party Coverage	95
Terrorism Coverage	100
Theft Coverage	102
Third-Party Liability Coverage	107
Claims Reporting, ERP, Selection of Counsel, Consent to Settle	124
Prior Acts	132
Territory	134
Definition of Covered Services	136
Specific Coverages Included in Policy	141
Exclusions	155
Risk Management Services	180

The Betterley Report

are more limited. For the insured (or its advisors) looking for proper coverage, choosing the right product is a challenge.

Most of the carriers offer multiple Cyber Risk products, so crafting the coverage for each insured requires the best in risk identification and knowledge of the individual covers. More than most insurance policies, Cyber Risk requires experienced risk professionals to craft the proper coverage.

We have tried to present a variety of coverages to illustrate what is available in the market. Twenty-nine sources of insurance are included in this survey. These sources represent the core of the Cyber Risk insurance market. Last year's survey only included nineteen sources of product; as the market has greatly expanded, we decided to include more insurers.

There continues to be substantial interest in privacy and data protection coverages; in fact, it isn't going too far to say that privacy risk is driving the market for Cyber Risk coverage. Carriers are tweaking the products to improve coverage, while in some instances adding protection against adverse claims experience, especially in the remediation costs area. This is interesting to us, as our clients generally seem to feel that a liability loss is not likely, but that the remediation coverage is useful. As carriers tweak their remediation coverages, they face a challenge of continuing to offer obviously helpful protection without incurring excessive losses.

As always, while each insurance carrier was contacted in order to obtain this information, we have tested their responses against our own experience and knowledge. Where they conflict, we have reviewed the

inconsistencies with the carriers. However, the evaluation and conclusions are our own.

Rather than reproduce the carriers' exact policy wording (which of course can be voluminous), we in many cases have paraphrased their wording, in the interest of space and simplicity. Of course, the insurance policies govern the coverage provided, and the carriers are not responsible for our summary of their policies or survey responses.

In the use of this information, the reader should understand that the information applies to the standard products of the carriers, and that special arrangements of coverage, cost, and other variables may be available on a negotiated basis.

For updated information on this and other Betterley Report coverage of specialty insurance products, please see our blog, *The Betterley Report on Specialty Insurance Products*, which can be found at: www.betterley.com/blog.

Finally, we regret that The Hartford could not respond to this survey; we have included their

Companies in This Survey

Ace	Admiral
Allied World	Arch
Axis	Beazley
Brit	CFC
Chartis	Chubb
CNA	Crum & Forster
Digital Risk	Euclid
The Hartford	Hiscox
Ironshore	Liberty International
Markel	NAS
Navigators	OneBeacon
Philadelphia	RLI
Safeonline	ThinkRisk
Travelers	XL
Zurich	

The Betterley Report

2010 information.

Introduction

As with all of our Market Surveys, Cyber Risk coverage represents a new or recently developed form of coverage designed to address the needs of new risks confronting organizations. Cyber Risk coverage epitomizes new insurance products, presenting insurance product managers with challenges as they learn what their insured's need, and what the carriers can prudently cover.

Most carriers were convinced that their best opportunities are to sell Cyber Risk coverage to mainstream companies that have significant Cyber Risk exposures. Many of those prospective insureds are already the carrier's customers, looking for coverage not present in traditional policies. The experience of a distressingly large number of major companies in the past few years is perhaps only the tip of the iceberg representing the threat of data theft facing businesses worldwide. Insurance protection to backstop IT security safeguards must be carefully considered for businesses and institutions such as hospitals, educational institutions, and public entities.

Often, these policies are adapted to cover the special risks of Cyber Risk activity. Carriers have developed very different products to address what they think Cyber Risk companies need; we have provided a Product Description table that lets the carrier describe in its own words the coverage it is offering. This table is vital to the reader's understanding of the various - and varied - products offered.

Specialized Cyber Risk insurance comes in a variety of forms, but we find it most helpful to divide coverage into property, theft, or liability for surveying purposes. Some carriers offer liability only products, while others offer a combination of property, theft, and liability cover.

The market is now broadening, as small to mid-sized companies become aware of the possibilities of liability, and especially a breach and resulting response costs, arising out of the possession of private data. Carriers are offering specialized Cyber Risk policies to these potential insureds, as well as enhancements to existing policies, such as Business Owners, Management Liability, and other policies. We don't cover that product segment in this Report, although we do cover it in our Private Company Management Liability Report (August).

State of The market

Annual premium volume information about the U.S. Cyber Risk market is hard to come by, but in reviewing the market, we have concluded that the annual gross written premium is in the \$800 million range (up from \$600 million in last year's Report). We suspect that the market will continue to grow, as protection against privacy breaches and the growing importance of post-breach response (also known as remediation) services drives the market.

Privacy coverage is clearly driving the market; Cyber Risk seminars and conferences are packed with prospective customers, carriers, brokers, and attorneys interested in privacy risk, coverage, and services. Interest is translating into purchases, which we (and many others) have been predicting.

The Betterley Report

Management may still be thinking ‘it can’t happen here’ but as more events occur that would be covered, more Cyber Risk insurance is being bought.

Data breaches have become disturbingly frequent, especially over the past few months. We are unsure if this is a result of increased reporting (breaches happened before but were not disclosed) or increase activity by, and effectiveness of, hackers, but it is going to have an impact on the insurance market.

What might those impacts be? Possibly higher interest in coverage as more potential insureds see the frequency of breaches, but also higher premium rates and/or retentions, as the increasing frequency of claims are paid for (and as insurance company leadership sees breaches occurring even at “good” risks).

We can imagine the conversations in insurance company management meetings about cyber insurance after reading about breaches at companies such as Lockheed Martin, Sony, and Citibank. And even worse - RSA SecureID token breaches.

We think that a strong influence on the purchase of Cyber Risk insurance is the increasing awareness of the value of post-breach response coverage. We have spoken with many CFOs, Treasurers, and Risk Managers who are not so sure that the case for liability protection has been made, but that can easily see how post-breach costs would be a burden.

We also asked carriers about the health and interest of the reinsurance market that supports Cyber Risk products, and they generally reported that reinsurers still like the product. Increasing interest

in Cyber Risk product support was reported by the responding carriers. There is concern over accumulation risk (that is, the same cause of loss affecting multiple insureds, leading to massive claims), which has caused reinsurers to limit their exposure.

Many carriers are reporting strong growth in premium. Although we must maintain confidentiality about the details, carriers that have been significant players in the Cyber Risk market for at least several years indicate premium growth ranged from flat to over 100%. More than one of these carriers reports growth of over 100%, while several others report between 50% and 100%. A few were in the 10-25% range, and the others were under 10%. This is remarkable, considering how difficult it has been for commercial property and casualty insurers to grow their top line revenue in the severe economic downturn.

Newer carriers are reporting high rates of growth, but this is off of relatively small base premiums, of course. These newer carriers are helping expand the market with innovative product features as they seek to create a presence in what has become a crowded segment.

Premium volumes were well reported to us in this survey. We know that at least two carriers are writing a relatively large amount of business (well over \$50 million), with other carriers writing in the \$10-25 million range. Others are fairly far behind; there are several markets writing under \$5 million.

Finally, as noted, there are a number of carriers that are offering Cyber Risk coverages as an option to another policy, such as a package policy,

The Betterley Report

Management Liability policy, or some other mainstream product. We did not include these products in this Report but have added more specific questions to our Private Company Management Liability Market Survey 2011 (August release).

State of the Market – Rates and Retentions

We asked the carriers whether they planned rate increases (or decreases) during the upcoming year, and what they expected of their competitors. Most offered their thoughts, which were remarkably similar to what we heard in 2010.

Rates for Cyber Risk insurance, like the traditional commercial insurance lines, are still showing signs of softness. Some of the smaller carriers report plans to reduce rates on the order of 5-10%, while the larger carriers indicate that rates will stay flat or perhaps down a bit (5%). Several reported that they expect their competitors will reduce rates even further, a sure sign of a soft market.

The rates are soft at least in part because Cyber Risk is a new market with a great deal of growth potential; we surmise that carriers are trying to avoid missing the growth opportunity present in this still new product. Also, since new products tend to start with conservative rates, there may be room to lower them as the market learns more from its (loss) experience.

We do have some concern that the claims for post-breach response costs are turning out to be more common and more expensive than carriers might have expected. What was perhaps seen as a bit of a sweetener to the product is turning out to

be a major source of claims. These claims could drive rates up, but we suspect that they are more likely to result in tighter cost controls by the carriers. As insurers learn more about how to respond to a breach at a lower cost, there is hope that rate increases can be held down.

Capacity and Retentions

Significant liability limits capacity exists, and reasonable (account appropriate) retentions or deductibles are available. Higher limits can probably be stacked up if desired.

Deductibles or retentions can be quite competitive; the table shows minimums, of course. Large retentions (\$500,000+) should be expected for larger insureds.

Carriers are still reluctant to state commissions, but they typically are similar to those paid on traditional commercial lines products.

Data Privacy

We are often asked whether coverage in a Cyber Risk policy includes losses arising out of data breaches. Coverage for liability resulting in data breaches often existed in Cyber policies, although not specifically spelled out. Because prospective insureds (and their advisors) wanted to see coverage more clearly stated, and because underwriters wanted more control over this evolving (exploding?) risk, more specific coverage has evolved.

Based on our research into privacy exposures and coverage, we have identified six key areas that should be considered:

- Types of Coverage and Limits Available

The Betterley Report

- Coverage Provided
- Coverage Triggers
- Types of Data Covered
- Remediation Costs Covered
- Remediation Coverage Services

The Types of Coverage and Limits Available

There are three fundamental coverage types: liability for loss or breach of the data, remediation costs to respond to the breach, and coverage for fines and/or penalties imposed by law or regulation.

Liability coverage is pretty self-explanatory - protection for the insured should it be sued for negligence leading to a security breach. Often the coverage does not explicitly list data breach as covered, rather including coverage as a part of a more general coverage grant for, as an example, failing to prevent unauthorized access to a its computer system.

Some carriers offer more explicit coverage, such as an act, error, or omission that results in a theft of data from a computer system. Both methods can work, but it is very comforting to see a term like Theft of Data included in the coverage grant.

Coverage Provided

Coverages fall into three categories varying widely between the carriers:

- Liability – defense and settlement costs for the liability of the insured arising out of its failure to properly care for private data

- Remediation – response costs following a data breach, including investigation, public relations, customer notification, and credit monitoring
- Fines and/or Penalties – the costs to investigate, defend, and settle fines and penalties that may be assessed by a regulator; most carriers do not provide this coverage, although there can be coverage for defense costs.

Coverage Triggers

Coverage can be triggered by:

- Failure to secure data
- Loss caused by an employee
- Acts by persons other than insureds
- Loss resulting from the theft or disappearance of private property (such as data that resides on a stolen laptop or missing data storage media)

Types of Data Covered

Some carriers specify the types of data covered, others do not. Specific types covered can include:

- An individual's personally identifiable information
- Nonpublic data (such as corporate information)
- Nonelectronic data, such as paper records and printouts

Remediation Costs Covered

Remediation is an area that is no longer new for Cyber Risk insurance (in fact, we believe that it is the primary reason why many insureds buy Cyber Risk insurance). This coverage is for the costs of responding to a data breach. Organizations that suffer a data loss may be required to no-

The Betterley Report

tify their customers with notice of the data loss, which can be expensive. Typically, they may also want to mitigate the negative impact on their reputation by providing credit monitoring services for those same customers; this cost can also be significant.

Remediation cost coverage is now offered by most carriers. It can include:

- Crisis management services
- Notification of potentially affected customers
- Credit monitoring
- Costs to resecure (that is, make secure again) data

The Ponemon Institute is the most frequently cited source of information about the cost and extent of data breaches; their most recent report (<http://www.ponemon.org/news-2/23>) compared 2009 breaches to 2008 and noted:

- The cost of a data breach as the result of malicious attacks and botnets were more costly and severe.
- Negligent insider breaches have decreased in number and cost most likely resulting from training and awareness programs having a positive effect on employees' sensitivity and awareness about the protection of personal information. Additionally, 58 percent have expanded their use of encryption up from 44 percent last year.
- Organizations are spending more on legal defense costs which can be attributed to increasing fears of successful class actions resulting from customer, consumer or employee data loss.
- Average abnormal churn rates across all incidents in the study were slightly higher than last year (from 3.6 percent in 2008 to 3.7 percent in 2009), which was measured by the loss of customers who were directly affected by

the data breach event (i.e., typically those receiving notification). The industries with the highest churn rate were pharmaceuticals, communications and healthcare (all at 6 percent), followed by financial services and services (both at 5 percent).

- Third-party organizations accounted for 42 percent of all breach cases, dropping from 44 percent of all cases in 2008. These remain the most costly form of data breaches due to additional investigation and consulting fees.

The most expensive data breach event included in this year's study cost a company nearly \$31 million to resolve. The least expensive total cost of data breach for a company included in the study was \$750,000.

We have been seeing signs that many smaller data breaches are coming in with lower numbers; for example, a more typical cost per record breached might be in the \$100 dollar range, rather than the \$200+ often cited.

Remediation Coverage Services

There can be great benefit to the insured if the remediation services are prenegotiated and prepackaged; much like kidnap and ransom coverage, knowing how to respond to a loss can be daunting.

Carriers often offer prepackaged and prenegotiated services provided by third-party vendors. In some cases the insured is required to use designated vendors. In addition, some policies require the written consent of the carrier to use the services. Finally, a few of these services have a time limit for use, especially credit monitoring.

Security Assessment Requirements

Carrier-required assessments of the prospective insured's security policies are rare now; the details are in the accompanying table. Typically, but not always, any required assessment is free to the applicant.

Such an assessment can be very useful to the applicant, even if they do not buy the coverage. But if they do, a favorable assessment should help lower the insured's premium.

Requirements often differ depending on whether the coverage is first-party or third-party, and can also vary depending upon the type of business the insured is in. Some assessments are as simple (and easy on the applicant) as a review of its website, while others require an onsite review by third-party firms. Of course, the scale and intensity of the assessment is dependent not only on the carrier's underwriting philosophy, but also the nature and role of the applicant's business being considered.

Coverage

Property and Theft

The insurance industry offers property and theft (first-party) coverage and liability (third-party) coverage; some carriers offer liability only, while others offer all. We expect that more carriers will soon be offering combined property and liability programs.

First-party coverage protection against denial of web services (hacker attacks) is still a hot topic due to continuing attacks on leading Internet sites.

Most property products cover this risk, although subject to negotiation and individual underwriting.

Theft exposures are sometimes not well understood in Cyber Risk risk assessments. The potential for traditional theft of money or goods *via* the Internet is often recognized, but theft or destruction of data, extortion, and theft of computing resources sometimes are not.

Liability

The definition of Insured differs on many policies, but special requirements can usually be met. Many carriers do not automatically include subcontractors as insureds, although many can endorse coverage.

The definition of a claim also varies significantly, with some carriers going to great lengths to define a claim, others using wording such as "a demand seeking damages."

Coverage for liability arising out of alleged media offenses has become a popular addition to Cyber policies. As many insureds and their brokers take Cyber activities to mean "Internet" activities, accompanied by buzz about social networking, questions about coverage for libel, slander, and intellectual property are increasing. Where is the coverage, asks many an insured.

Some coverage may already exist in the Personal Injury portion of an existing General Liability policy, but more specific – and broader - coverage may be obtainable in a Cyber policy.

This Report has several new tables to address the Media Liability coverages that may be offered. They condense the information into three areas:

The Betterley Report

- Business Activity Coverage Limitations, which shows how and in what ways the carrier restricts the coverage, such as whether it is limited to the Insured's own website
- Personal Injury Rights that may be covered, and
- Intellectual Property Rights that may be covered

Claims Reporting, ERP Options, and Counsel

Each liability policy reviewed is a claims made form so Extended Reporting Period (ERP) options are important; look for bilateral extended reporting period wording.

Selection of counsel continues to be a delicate issue with insureds, but as we frequently see in other new lines of coverage, carriers typically reserve the right to select, or at least approve, counsel. However, some carriers offer an option for the insured to preselect counsel, while others allow selection from an existing panel,

As with all questions of counsel choice, we recommend that insureds discuss and agree with their carrier beforehand on the counsel they want to use.

Generally, carriers can impose the infamous "hammer clause" on lawsuits that an insured may not want to settle. The use of "soft" hammer clauses is beginning to become prevalent in this product line

Definition of Covered Services

All carriers define the services they cover, whether it is contained in "boilerplate" terminology or on the declarations page, so it is important that it match the operations of the insured. Most carriers can adapt the language to meet the needs of the insured, but carefully crafting that language is important.

This is an area where omnibus wording is much needed, since the range of e-commerce activities can be vast and ever-changing.

Optional endorsements are available, including manuscripted coverages for special requirements of insureds.

Specific Coverages Included in Policy

We have identified 11 specific coverages that may be, but are not always, included in a Cyber Risk policy. These are:

- Errors & Omissions
- Virus
- Unauthorized Access
- Security Breach
- Personal Injury
- Advertising Injury
- Loss of Use
- Resulting Business Interruption
- Copyright Infringement
- Trade or Servicemark Infringement
- Patent Infringement

Generally, insureds should be careful to review their exposures to these types of losses, and make

The Betterley Report

sure they use carriers that are willing to offer the needed protections. Coverage for Patent Infringement, for example, is rarely (if ever) offered in basic Cyber Risk forms, but can be purchased from a limited number of carriers as a separate Intellectual Property policy (as covered in Intellectual Property and Media Liability Market Survey April 2011).

Exclusions

Exclusions are many and varied, as would be expected; please read those tables carefully.

Rather than try to recite them here, the information for each carrier is found in the Exclusions table.

Risk Management Services

Carriers continue to augment the exposure identification and loss prevention services they offer their insureds. This is a tough area to operate in, because the range of e-commerce activity is extensive, not lending itself to a “one size fits all” approach.

We are pleased that carriers have identified these services as valuable to their insureds (and to their own loss ratios, we hope) and continue to broaden and strengthen their capabilities. More e-

commerce-specific exposure identification and loss services are becoming available to insureds and their brokers. Services range from underwriting assessments that are shared with insureds through self-help audits and technical information to training, seminars, and testing by third-party service providers.

Please also refer to our discussion of privacy-related remediation services earlier in this Report.

Summary

Privacy coverage and associated remediation services continue to be the big news in Cyber Risk; carriers have rolled out impressive new products, brokers have beefed up their expertise, and insureds are getting proposals.

Proposals are being sought, and policies are being bought. Companies, healthcare systems, not-for-profits, and the public sector are buying coverage, despite a shortage of funds for new insurance policies. It’s an exciting time to be thinking about cyber risk and insurance - especially because of the impact of Cloud Computing. We asked attorney Paul Paray, a well-known authority on cyber insurance and now Of Counsel with Wilson Elser, to offer his thoughts in the following article.

Does Our Network Security and Privacy Policy Cover Cloud Exposures?

By Paul E. Paray*

If risk managers and CFOs are not asking their brokers, insurance consultants or legal counsel this question they really should. Given the major impact cloud usage is having on businesses around the country – with some users readily providing sensitive data to be processed by cloud vendors – it is essential that companies get the insurance coverage they expect. Most network security and privacy (NSAP) insurance products ostensibly cover losses tied to the processing, transfer and storage of sensitive data. Companies should want to know whether their NSAP insurance, first purchased before they entered into uncharted waters, continues to provide peace of mind now that the ocean has gotten a lot wider.

By way of background, cloud providers provide easily provisioned IT resources on an “as needed” basis.¹ Cloud computing brings with it the promise of significantly lowering IT expenses over the long haul – an obvious strong lure to both business and government. A single cloud provider,

¹ See National Institute of Standards and Technology definition of “cloud computing” is as follows: “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” *NIST Special Publication (SP) 800-145* (January 11, 2011).

Amazon.com, boasts of already having hundreds of thousands of customers. It is no wonder that in his Federal Cloud Computing Strategy report released in February 2011, our first federal CIO, Vivek Kundra, estimated that \$20 billion of the federal government’s \$80 billion IT spending is a potential target for migration to the cloud.²

Unfortunately, the added risks inherent in moving to a cloud provider are not necessarily intuitive. For example, cloud providers do not offer a universal interface that allows companies to move easily among various cloud providers. If you are one of the many Silicon Valley startups that now completely avoids hardware investments by being fully reliant on a cloud provider – such as Amazon’s EC2 service – the risks inherent in porting existing software or writing entirely new applications don’t really exist. On the other hand, if you are an established company moving from your existing hardware-based system to a cloud provider, you will need to devote sufficient resources to port your applications and data. The risks of data loss and business interruption may increase during this customization process.

There is another risk inherent in jumping into the cloud: identity management. The same problem obviously exists outside the cloud but to a lesser degree. Cloud computing does not require that a client know the location and configuration of the system that is ultimately delivering its storage and software services. Firms using the cloud to process sensitive data may be at a greater risk of theft because physical security measures taken to protect data in a secure environment may no long-

² See Federal Cloud Computing Strategy (February 8, 2011) (<http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf>)

The Betterley Report

er be applicable. Indeed, according to a recent survey, only 31% of cloud providers use or will deploy within a year an ID and credentialing system.³

Another major risk – and the one that really mandates an answer to the question of whether existing NSAP insurance addresses a claim originating in the cloud – stems from the fact that cloud providers are not generally ready and able to stand behind their clients should a claim be filed. For example, in a white paper one leading cloud provider offers ways to satisfy the HIPAA Privacy Rule and Security Rule requirements, including with the use of encryption and access controls. The real value of such guidance remains to be seen given the disclaimer at the end of the paper and similar language found in its agreements makes clear that the provider offers no representations or warranties that its services “will assure compliance with applicable laws, including but not limited to HIPAA.” To drive home the point, cloud providers often limit their exposure using an exclusion of consequential damages as well as a limitation of liability.

Applicability of NSAP Coverage Grant

In some instances, an insured’s use of cloud computing does not generate much of a coverage-grant issue. That is definitely the case when a NSAP policy provides express coverage for outsourced IT services. Such a coverage grant is usually tied to an expanded definition of computer

systems, which includes third-party computer systems. Other NSAP policies tie coverage to an insured’s network and are careful to specify what that consists of – sometimes specifically stating that a “network” includes a third-party provider’s hardware and software. At the other end of the spectrum, some NSAP policies expressly state that covered computer networks do not include third-party infrastructure. Such a provision would be of obvious concern.

Some NSAP insurers have allowed a third-party service provider’s computer system to be endorsed onto the policy as being part of the insured’s computer system. Would the failure to endorse a new cloud vendor mid-term impact the coverage provided by an existing endorsement? As well, several NSAP insurers require that insureds “maintain the minimum security standards set forth in the application or better” as a condition precedent to coverage. Front loading the question of whether a particular cloud provider improves or degrades the insured’s existing security is preferable to a post-claim scenario. It should also be determined up front whether the use of a cloud provider mid-term would require underwriter approval or would impact the applicable coverage grant.

Even if the existing policy does not have an express coverage grant, an expansion to the definition of network or computer services can often be obtained by endorsement, but somebody, the applicant or its broker, has to ask for such an endorsement. Even if the language offered in the policy provides coverage for computer systems maintained by third-party service providers such as cloud providers, the language used must still be carefully scrutinized. For example, one market provides ostensible cloud provider coverage, but

³ See Ponemon Institute Survey, *Security of Cloud Computing Providers Study* (April 2011) at p. 9. Interestingly, this same survey also shows that only 43% of cloud providers use or will deploy within a year “encryption for data at rest” and only 58% use or will deploy within a year “encryption for data in motion.” *Id.*

The Betterley Report

only if the third-party computer system in question is solely for the benefit of the insured. It is likely that a cloud provider has more than one client so the language used may make handling claims difficult when questions arise regarding shared servers – configurations which are largely unknown to cloud users.

There are a number of other standard coverage provisions that need to be considered during the application process and cloud contract negotiations. Since an insured may not know exactly where its data is residing; having broad jurisdictional coverage becomes essential. Does the policy provide coverage for losses occurring anywhere in the world and for claims made anywhere in the world? NSAP policy conditions may also dictate how cloud provider agreements are negotiated. Given most such policies are claims made and reported, it is important that cloud providers be contractually bound to promptly report breaches.

Conditions and Exclusions

As referenced above, some policies may exclude coverage for the failure to “ensure that your computer system is reasonably protected by security practices and systems maintenance procedures that are equal to or superior to those disclosed in the application.” Coverage can also be excluded if the claim is based on the “failure in design or architecture of your computer system, including failure to design for adequate traffic and capacity requirements.” Given the typical lack of insight insureds have regarding their cloud providers’ IT infrastructure, if not addressed beforehand, such exclusions will become wildcards.

Business Interruption and Extra Expense

As sadly illustrated by the recent Japanese earthquake and tsunami, contingent business interruption coverage can be a crucial coverage for many businesses. In a cloud context, such coverage can be even more important – especially since most cloud providers offer very little compensation under their service level agreements (SLAs). In almost all instances, a SLA compensates based on a reimbursement policy that is tied to the return of fees. The recovery of lost profits or costs to restore a network is not typically part of standard cloud services agreements. And, assuming there is no physical damage to an insured’s computer network, the NSAP policy will most likely provide the only available insurance coverage.

Although business interruption and extra expense coverage under a NSAP policy is now widely available, there remain exclusions that might seem a bit problematic from a cloud perspective. For example, most NSAP policies exclude coverage for any failures or outages caused by a disruption in power, utility services, or telecommunications services not under your direct operational control. It should be confirmed upfront whether the NSAP policy would pick up the cloud provider’s network disruptions. For example, the April 21, 2011 “instance connectivity, latency and error rate” outage that hit Amazon Web Services for four days impacted many popular websites. It is important for insurance buyers to understand beforehand whether such outages would be covered events. And, assuming they are covered and there is no relevant exclusion, companies also need to evaluate whether all relevant conditions of the policy would be readily satisfied. Some policies pro-

The Betterley Report

vide that an insurer has the right to inspect the network to prove that business interruption costs are fair and reasonable. If a firm's cloud provider is large and geographically diverse, it is unlikely insurers will discover where the relevant servers are located, let alone be able to have forensics experts comb through them.

Conclusion

There can be no denying that cloud computing still faces some major barriers before it displaces the traditional corporate IT function. On the other hand, in only a few years time, it has been embraced in some way by much of corporate America. Gartner even predicts that by next year, 80 percent of Fortune 1000 companies will be using some form of cloud computing services with 30 percent actually using cloud computing infrastructure services – stepping that much closer to being fully in the cloud. NSAP insurance is playing and

will likely continue to play a key role in increasing this adoption rate – that is, so long as the right questions are asked and answered.

* Paul E. Paray is Of Counsel in Wilson Elser's New Jersey office. He is a commercial litigator who also counsels clients on managing technology risk. Paul previously built an insurance practice focused on addressing privacy exposures while working at several large insurance services firms. Recognized for his knowledge in the area of commercial litigation and risk management, Paul has been interviewed and quoted in Business Insurance, The Hartford Business Journal, The New York Times, The Newark Star-Ledger, The Financial Post, CFO magazine and other leading publications. Paul is admitted to practice law in New Jersey, New York and the District of Columbia and can be reached at 973-735-5977 or paul.paray@wilsonelser.com.

The Betterley Report



About The Author

Richard S. Betterley, CMC, is the President of Betterley Risk Consultants, an independent insurance and alternative risk management consulting firm. BRC, founded in 1932, provides independent advice and counsel on insurable risk, coverage, alternatives to traditional insurance, and related services to corporations, educational institutions, and other organizations throughout the U.S. It does not sell insurance or related services.

Rick is a frequent speaker, author, and expert witness on specialty insurance products and related services. He is a member of the Professional Liability Underwriting Society and the Institute of Management Consultants. He joined the firm in 1975.

Rick created The Betterley Report in 1994 to be the objective source of information about specialty insurance products. Now published 6 times annually, The Betterley Report is known for its in-depth coverage of Management Liability, Cyber Risk, Privacy, and Intellectual Property and Media insurance products.

More recently, Rick created The Betterley Report Blog on Specialty Insurance Products, which offers readers updates on and insight into insurance products such as those covered in The Betterley Report. It provides him with a platform to more frequently and informally comment on product updates and newly announced products, as well as trends in the specialty insurance industry. www.betterley.com/blog

The Betterley Report

The Betterley Report, your independent guide to specialty insurance products, is a series of six comprehensive Reports published annually. Each Report exhaustively reviews a single hot specialty insurance product, providing essential information such as:

- Who are the leading carriers?
- Complete contact information
- Target and prohibited markets
- Capacity, deductibles, and commission ranges
- Sample premiums (where available)
- Critical coverage and claims differences
- Exclusionary language
- Risk Management services

Most Betterley Reports are produced annually, and range from 25 to 100 pages in length. Current analyses include:

- Cyber/Privacy/Media Risk Policies
- Technology Risk Insurance
- Employment Practices Liability Insurance (EPLI)
- Private Company Management Liability
- Side A D & O Liability
- Intellectual Property and Media Liability

The Betterley Reports are a huge timesaver for busy Risk Management professionals who need to be up-to-date on insurance products for their clients. Need to identify and evaluate the coverage, capacity and contacts for your clients? We've done the ground work for you!

Subscribe now and, for only \$199.00 U.S., you will receive a full year of upcoming Betterley Reports plus access to our exclusive archive of reports dating back to 1999!

Only want single issues? Only \$50.00 U.S. each; you will be able to select, view, and print the back issue of your choice.

Need the best analysis of leading edge insurance products? Subscribe to The Betterley Report, your best source of objective advice on innovative specialty insurance products.

To order, or for further information, go to: betterley.com/ordering_information.html

Betterley Risk Consultants, Inc.
Thirteen Loring Way • Sterling, Massachusetts 01564- 2465
Phone (978) 422-3366 • Fax (978) 422-3365
Toll Free (877) 422-3366
e-mail rbetterley@betterley.com

Betterley Risk Consultants is an independent insurance and alternative risk management consulting firm. Founded in 1932, it provides independent advice and counsel to corporations, educational institutions, and other organizations throughout the U.S. It does not sell insurance nor provide insurance-related services.

* * * * *

The editor has attempted to ensure that the information in each issue is accurate at the time it was obtained. Opinions on insurance, financial, legal, and regulatory matters are those of the editor and others; professional counsel should be consulted before any action or decision based on this matter is taken. Note: all product names referred to herein are the properties of their respective owners.

The Betterley Report is published six times yearly by Betterley Risk Consultants, Inc. This material is copyrighted, with all rights reserved. ISSN 1089-0513
