



BETTERLEY
RISK RESEARCH

**Understanding the Cyber Risk Insurance and
Remediation Services Marketplace:
A Report on the Experiences and Opinions of Middle Market CFOs**

September 2010

**Betterley Risk Research – Insight for the Insurance Industry Driven by
Real World Market Research**

About Betterley Risk Research

Betterley Risk Research provides product research and consulting services to commercial lines insurance companies and service providers. Driven by a desire to couple its ‘in the flow’ knowledge of commercial insureds and their needs with a desire to improve insurance-related products and services, Betterley Risk Research strives to provide information, understanding, and (we hope) wisdom.

Our work includes consulting on the design and distribution of products and services, competitor analysis, market analysis, and surveys of insureds and prospective insureds. Clients include leading insurance and reinsurance companies as well as service providers.

For more information, please contact:

Richard S. Betterley, CMC
President
Betterley Risk Consultants, Inc.
Thirteen Loring Way
Sterling, MA 01564
P: 978/422-3366 E: rbetterley@betterley.com

* * * * *

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.

www.betterley.com/blog

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

Table of Contents

Introduction.....	4
Research Methodology.....	5
Summary of Findings.....	6
Market Penetration and Product Awareness	6
Opinions on Product Features.....	6
Perceptions of Insurance Companies, Brokers, and Risk Management Service Providers.....	7
Conclusion	8
Data Included in the Complete Report	9
Study Sponsors	10

Introduction

The Specialty Insurance market has rarely – if ever – seen a new product in as much demand as Cyber Risk and Privacy. A coverage that is designed to meet the needs of commercial insureds (whether for profit or not-for-profit, as well as public entities), this type of insurance can perhaps be considered necessary by almost all insureds. Large or small, high tech or low tech, most organizations have at least some exposure to cyber and privacy risk.

Cyber and privacy risk exposures are real - according to the Ponemon Institute's fifth annual *U.S. Cost of a Data Breach Study* (<http://www.ponemon.org/news-2/23>), "data breach incidents cost U.S. companies \$204 per compromised customer record in 2009, compared to \$202 in 2008. Despite an overall drop in the number of reported breaches (498 in 2009 vs. 657 in 2008 according to the Identity Theft Resource Center), the average total per-incident costs in 2009 were \$6.75 million, compared to an average per-incident cost of \$6.65 million in 2008."

Various governmental Red Flag initiatives require U.S. organizations to respond to data breaches by alerting the victims of the breach, triggering extensive and expensive remediation services. Regulatory fines can be imposed for failure to properly notify affected persons or organizations.

To protect against this risk, organizations can buy Cyber Risk and Privacy insurance. This type of insurance has been around for some years, especially the damages and loss of income portion, but liability and remediation cost coverage is relatively new (we started writing about it in [The Betterley Report](#) in 2003). Although only a few insurance companies initially offered coverage, there are now many more in the marketplace.

Typically, larger companies were the purchasers of Cyber Risk and Privacy insurance; middle market and smaller companies, and not-for profit institutions and governmental organizations, were far less likely to buy coverage.

This seems to be changing; the insurance companies and brokers in this market expect that the real growth opportunities for Cyber Risk and Privacy coverage are in the middle market. Insureds that are too small to self assume their losses but too big to ignore them are the likely next wave of buyers.

We have spent much of our career evaluating (and participating in) the rollout of new types of insurance policies. D&O, Environmental, Management Liability, Employment Practices Liability – we've seen a lot of new products.

But after looking into Cyber Risk and Privacy insurance for a couple of years, we began to realize that this line of insurance could represent the biggest new product opportunity that we had ever seen.

How to Obtain the Complete Report

The entire Report includes 43 charts and 52 pages of discussion about the survey findings.

To obtain a copy, please visit www.betterley.com and click on Ordering Info. Select Order Single Issues

Or, call Betterley Risk Consultants at 877/422-3366 or email rbetterley@betterley.com

Why so big? The combination of widespread concern by the public over data breaches, difficulty in measuring the true risk, continuing and creative efforts by hackers, difficulties in containing the risk, political support for regulatory action, and an insurance industry eager to find new sources of revenue made this an almost perfect situation for new product opportunity.

In response to this high level of interest, we created this study to examine the attitudes of U.S. middle market companies toward Cyber Risk and Privacy insurance.

How many of them already have insurance, and how many are expecting to buy it in the next 18 months? What do they want to buy? Who are the insurance companies and brokers, as well as risk avoidance and response service providers, that they recognize? And finally, what are the coverage features that they want to see in a policy? We decided to ask.

Research Methodology

We determined that a relatively small, in-depth survey would allow us to best determine and understand the attitudes of middle management companies about Cyber Risk and Privacy insurance. Since we wanted to really dig in to the thinking and opinions of senior executives responsible for insurance decisions, we commissioned a study to interview 51 executives of middle market companies (annual sales between \$10 million and \$500 million).

Responses were analyzed where appropriate by size of company, whether or not they carry Cyber Risk and Privacy insurance, if not, whether they planned to buy insurance within the next eighteen months, and if not, why not.

Very specific questions were asked about product features, the role of insurance brokers as sources of guidance, and their perceptions of the various insurance companies, brokers, and service providers.

Each executive was interviewed for approximately 15-20 minutes. The interviewee was required to be an executive responsible for purchasing insurance, and was generally a CFO or Treasurer. All responses were confidential and individual company names were not known to us or our the study sponsors.

Participants were included from the full spectrum of middle market companies, not only as to size but also the location of their headquarters. While not a statistically meaningful sample, we believe that the interview process accurately captured the opinions of the market.

Survey questions were developed by Betterley Risk Consultants; study sponsors had input on the questions asked, but final control of the questions and of this study was maintained by Betterley.

We are grateful to our study sponsors, CNA, Identity Theft 911, Munich Re, and USI for funding the interview expenses and for their input on the survey questions. We would also like to thank Synovate, Inc., which helped with the final design of the interview questions and conducted the actual interviews.

Further demographic information about the interviewees are included in the accompanying tables.

Summary of Findings

This Report includes over 40 charts presenting the results of the interviews and our commentary on their meaning. These charts are listed in the Table of Contents above. They are separated into 3 key areas:

- Market Penetration and Product Awareness
- Opinions on Product Features
- Perceptions of Insurance Companies, Brokers, and Risk Management Service Providers

We will summarize the findings here; the accompanying charts provide substantially more information and greater detail.

Market Penetration and Product Awareness

In this section we asked executives responsible for insurance at middle market companies about:

- Their awareness of Cyber Risk and Privacy insurance
- Whether their company was currently insured for cyber and privacy risk
- If not currently insured, whether they planned to purchase coverage within the next 18 months
- If not planning to buy coverage, their reasons why not

Approximately one-third of the respondents indicated that they currently buy Cyber Risk and Privacy insurance, and another 25 per cent plan to buy coverage within the next 18 months.

The largest companies (\$250 – \$500 million in sales) were more likely to already have coverage, but the next most likely was the \$50 – \$100 million group (higher than both the \$100 – \$250 million and \$10 – \$50 million groups).

For those that do not have coverage, ‘too expensive’ was not as big a reason as we expected, but was still important. Keep in mind that, for many of these companies, the Great Recession’s effects aren’t yet over.

Respondents heard about Cyber Risk and Privacy insurance from many sources; their insurance broker was one important source, but far from dominant. Audit firms, news reports, and experiencing their own data breach were also sources.

Opinions on Product Features

We asked a number of detailed questions about the types of products that the respondents were interested in, the specific product features and how they ranked them, and the value of the various risk avoidance and loss mitigation services that often are an integral part of a cyber policy.

Respondents were quite interested in buying coverage as a part of their existing Commercial General Liability or similar policy. We don’t think that this is realistic; standalone cyber coverage will still dominate the market for this group of insureds.

We asked about the Two Most Important Coverages in a cyber policy; there were clear distinctions between the insureds and those not yet covered. The uninsured did not see Fines and Penalties coverage as being as important as did those that already have coverage. This may be a function of product knowledge; the uninsured are not as knowledgeable as the insureds.

Policies that include services to help avoid losses and those that minimize losses that still occur were very attractive, especially to those not yet insured. This indicates that the availability of services could be a strong but underutilized selling point. Brokers should make more of an effort to educate their prospects about the availability and value of these services in cyber policies.

Cost was important but coverage quality ranked high for many companies. There was a clear distinction amongst companies, where cost was the most important factor for many, and for others, it was coverage quality. Marketing coverage quality to this group should pay dividends.

Most insureds bought coverage from their existing brokers, and most of the prospective insureds expect to as well. At the same time, respondents did not place much emphasis on the broker's product knowledge, which indicates that brokers with specialized knowledge might do well in this market. Insurers could do more to support the expertise of their brokers.

Existing insureds reported that they would be willing to pay higher premiums if their primary coverage objectives were included in the cyber policy; fewer prospects agreed. Interesting, as it implies there is a market for high quality coverages if the insured or prospective insured understands that they are included.

Perceptions of Insurance Companies, Brokers, and Risk Management Service Providers

This section includes information about the middle markets:

- Awareness of various insurance companies, brokers, and service providers
- Satisfaction with those organizations
- Claims experiences and satisfaction

Insurance companies in the Cyber Risk and Privacy area are not widely known; respondents listed a limited number of carriers compared with the many that are in this space. Understandably middle market executives that are responsible for insurance on a part time basis (none reported that they employed a Risk Manager) are not astute about who is in the market.

Current insureds knew of more carriers than the prospective insureds. This is perhaps because they had been introduced to some of the companies through the application and proposal process.

Most of the insured companies were satisfied or very satisfied with their carrier. This speaks well of the cyber risk product design and especially of the performance of the service providers, which are likely to have more contact with the insured than any party except the broker.

There were no brokers dominant in their cyber risk presence; respondents were likely to stay with their current broker when considering the purchase of cyber coverage. Middle markets also expected to remain with their current broker when renewing their coverage.

Service providers can be an important component in a cyber risk policy, both in the risk avoidance and mitigation value they bring and in their potential to sway a prospective insured to buy a policy (or particular policy) because of the service provider involved.

Existing insureds knew of a number of different providers, but there was no dominant name. Many did not know a single provider's name.

Prospective insureds were even less likely to know of specific providers. This indicates to us that there is much to be done about educating and influencing insureds and especially prospective insureds about the presence and value brought by the service providers. Service providers need to greatly elevate their profile amongst cyber risk insurance prospects in the middle market.

Finally, we asked about claims experience of the companies. Not surprisingly, quite a few had experienced a claim. Of those willing to speak about their claims experience, all were either very or somewhat satisfied. This is probably higher than in most lines of insurance, and speaks well toward the expectations they have of the coverage and of the performance of the claims personnel of the insurance company. We need to be cautious, though, as this very small group of insureds may not be representative.

Conclusion

Cyber Risk and Privacy is such a new product for the middle market that there is a great deal of variation in coverage quality, broker knowledge, and customer expectations. Insurance companies are striving to figure out the right mix of coverage quality, price, and services. Brokers are trying to learn about which products best fit their client's needs. And service providers are figuring out how they can best be involved in the insurance process.

This study shows that middle market insureds recognize the need for coverage and accompanying services, but are not clear on which products are the best for them.

Making clear to the middle market that there are distinct differences between the products offered, and even different products from the same insurers, seems to be an approach that has merit. When we see respondents indicating that they will pay more to buy the right policy, we are confident that the marketplace will provide them with that option, and that insurance brokers will help them find it.

It is clear to us that our original assumption, that there is a lot of room for growth in the middle market for cyber risk products, is correct. Designing the right products, educating and motivating brokers to encourage insureds to add coverage to their protection, and using service providers wisely, will be a challenge. We are confident that the cyber risk insurance industry will meet it.

Data Included in the Complete Report

You are reading the Executive Summary of our study of the Cyber Risk insurance experiences and opinions of financial executives of companies in the U.S. Middle Market. The full study, which can be purchased for \$900 at www.betterley.com, includes 43 charts that analyze responses to the following categories of questions:

- **Market Penetration and Product Awareness**

- % of respondents that carry Cyber Risk insurance

- Reasons why they don't buy this insurance

- Do they intend to buy it in the next 18 months?

- How they learned of Cyber Risk insurance

- **Opinions on Product Features**

- Opinions about specific product features for both coverage and services

- Satisfaction with premium cost

- Willingness to pay more premium for key product features

- Satisfaction with limits and deductible options

- The value of underwriter and broker knowledge

- **Opinions about Cyber Risk Insurers, Brokers, and Service Providers**

- Which insurers and brokers are insureds and prospective insureds familiar with?

- Satisfaction with current insurer? Broker?

- Which service providers are insureds and prospective insureds familiar with?

- Number of respondents that have had a claim? How satisfied are they with claims handling?

Study Sponsors



As one of the most trusted names in commercial insurance, CNA offers a family of information risk products to address the cyber liability and information risk needs of businesses across a variety of industries. CNA NetProtect®, sets a high industry standard for network security, content and privacy liability protection, and offers the ability to tailor both first- and third-party coverage based on each business' individual information risk assessment. Visit www.cna.com to learn more or to contact a local branch office.



Identity Theft 911™ data breach solution provides comprehensive data risk management services for insurance carriers to help their commercial policyholders appropriately prepare for, respond to and resolve a potential data breach. We help business policyholders design an incident response plan, do regulatory consulting, training and education, and we can carry out consumer notification assistance and identity theft resolution to all parties impacted by the breach. Our security and privacy experts, in addition to our Breach Team, provide unlimited product development assistance, endorsement review and consultation to our carrier partners in the preparation of their data breach programs.

[Identity Theft 911](#)



Munich Re: Always one step ahead

Addressing the key challenges of the future – that is what we have been doing successfully for 130 years. As a reinsurer, we work across borders and disciplines to devise cutting-edge solutions and render tomorrow's world insurable. Our recipe for success: we anticipate risks early on and deliver solutions tailored to clients' needs, providing impetus for sustainable profitable growth.

This is especially true for the field of cyber risks: Munich Re extended its coverage of cyber risks in the last few years. We now offer the most capacity in this field and are also able to reinsure accumulation perils such as virus losses. Thanks to our international set-up, we are familiar with the solutions used in different markets and are able to help our clients get to grips with the new legal parameters and devise suitable products.



USI is the Single Source for Innovative Design, Strategic Perspectives and Informed Decisions.

The liability of business leaders in today's changing world is a volatile area filled with cyber liability as well as privacy and network security issues. USI's dedicated Management and Professional Services Practice specializes in helping clients make informed decisions to mitigate loss and avoid devastating damages and expenses resulting from these evolving exposures.