June 2013

BRC

THE BETTERLEY REPORT

CYBER/PRIVACY INSURANCE MARKET SURVEY – 2013:

Carriers Deepen Their Risk Management Services Benefits - Insureds Grow Increasingly Concerned with Coverage Limitations

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

Highlights of This Issue

- *More Analysis of Risk Management Services for Insureds*
- *More Detail on Coverage for Hostile Acts (State and non-State Actors)*
- *Zooming Growth and Competitive Rates*
- *Reinsurance Activity with Commentary by Mike Brown of Guy Carpenter*
- *Two Bonus Articles:*
  - *David Kruger of Absio Corp. on self-protecting data*
  - *Rick Betterley (BRC) and Sandy Hauserman (Digital Risk Resources) on Cyber Endorsements for Traditional Policies: the next wave in Cyber insurance*

Next Issue

August
Private Company Management Liability Insurance Market Survey 2013

Like What You See in this Executive Summary?

IRMI Risk & Insurance KnowledgeBase • Education • Community

You won't believe the value in the full reports. Now Available on **IRMI Online**® and **ReferenceConnect**™

The Betterley Report provides insightful insurer analysis on these six markets and coverage lines:

- Cyber/Privacy Insurance Market Survey
- Technology Errors & Omissions
- Employment Practices Liability Insurance
- Side A D&O Liability Insurance
- Private Company Management Liability Insurance
- Intellectual Property and Media Liability Insurance

Each annual report provides a comprehensive review (50 to 175 pages) with numerous exhibits of the critical differences in insurers' coverage, market appetite, and capacity. **You save valuable time** because *The Betterley Report* has done the groundwork for you, providing practical information in a fully searchable online format.

What do you think this dedicated research team and related market analysis is worth to you and your team? Well, you are going to be pleasantly surprised when you see how we've priced it for you.

Agents and Brokers—Sell more and grow revenue by pinpointing errors in competitors' policies/proposals.

Risk Managers and Insurance Buyers—Identify, eliminate, or avoid coverage gaps with coverage comparison charts.

Underwriters—Research competitors with quick policy comparisons.

Attorneys—Keep up with year-to-year trends in policy form development.

Consultants—Identify markets and match them up to your clients' needs.

See more benefits and read Executive Summaries of each report at **www.IRMI.com/Go/3.**

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 security for organizations. Risks could include the breach of security by a hacker intent on stealing valuable data, or simple release of data through the carelessness of an employee or vendor.*

We have noted several broad trends in the Cyber insurance market and decided to dive deeper into them in this Summary and the accompanying tables:

- Insureds' concerns over Cyber exposures from attacks by state and non-state actors (i.e., state sponsored hacking for the purposes of damaging infrastructure and/or industrial espionage)
- Insureds' concerns over Cyber-based theft of Intellectual Property
- Deeper and richer value-added risk management services to help insureds avoid and cope with exposures and loss

List of Tables

Note that this Report does not focus on coverage for 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 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. The insurance industry continues to help brokers understand the exposures, coverage, and services of Cyber Risk, so that they can better

serve their clients. The products are complicated, making these educational efforts are worthwhile and necessary investment.

We have tried to present a variety of coverages to illustrate what is available in the market. Twenty-six sources of insurance are included in this survey. These carriers (and in a few instances, Managing General Underwriters) represent the core of the Cyber Risk insurance market. Safeonline's entries are now listed under their new name - Ascent Underwriting.

Last year's survey covered thirty-one; we eliminated several carriers that were unresponsive to several attempts to gather information about their products or were primarily focused on the Technology E&O market (covered in our February Report).

We did not add any new sources this year, and instead focused on further discussion of the spreading of Cyber coverages to traditional P&C policies such as BOPs (this is covered in the attached subscriber-only bonus article that Rick Betterley and Sandy Hauserman researched for the May issue of The Risk Report). It can also be found at www.irmi.com/products/store/the-risk-report.aspx

We also welcome David Kruger, Senior Architect at Absio Corporation (www.absio.com), who provided background on the availability of data protection that follows electronic data wherever it is located. This is particularly important as Bring Your Own Device becomes a common way organizations allow their employees to access and use data in the workplace. His article is entitled Data Breaches are Inevitable—But Reportable Breaches are Not.

Finally, a reminder that, 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**.

Companies in This Survey

The full report includes a list of 26 markets for this coverage, along with underwriter contact information, and gives you a detailed analysis of distinctive features of each carrier's offerings. Learn more about *The Betterley Report*, and subscribe on IRMI.com.

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 and other Intellectual Property 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.

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.

Carriers are offering Cyber Risk enhancements to existing policies, such as Business Owners, Management Liability, and other policies. These products take the form of a services-only product (no risk transfer), services plus breach response coverage, and services plus breach response plus liability. Limits are typically low and options are few, but the low additional premium can make them quite appealing to insureds. Whether they should buy these products or should consider standalone Cyber policies requires careful analysis and consideration or exposure, risk tolerance, and client/customer requirements.

As noted, a much deeper discussion is in the attached article Cyber Add-ons for Traditional Insurance policies.

State of The Market

The market continues to broaden, especially in health care and the small- to mid-sized insureds segments. Health care systems and their vendors in particular are buying Cyber Risk (and in the case of vendors, often buying it as a part of a Technology E&O policy) at a rapid clip. Carriers are offering specialized products to these insureds.

In addition to health care, carriers report much of their growth coming from small- to mid-sized companies newly aware of the possibilities of liability, and especially a breach and resulting response costs, arising out of the possession of private data. This is leading to a large increase in policy count, but far less in new premium written.

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 $1.3 billion range (up from $1 billion in last year's Report). Insurance broker Marsh reports a similar figure, lending further credence to our estimates.

The industry is divided by size (gross written premium) as follows:

- A few very large writers, with premiums in excess of $50 million
- Another few in the $25-50 million range
- A number of carriers writing $10-25 million
- Several writing in the $5-10 million and $1-5 million ranges

No carrier reported negative growth, nor did any report growth in the 1-10% range. The majority reported premium growth between 10-25%, and several reported growth of 25-50% or more.

The above information is from confidential sources and is intentionally generalized.

Growth has been dampened by some rate competition as new carriers try to gain market share, and much of the growth has come from smaller insureds. A lot more business is being written, but at slightly lower rates and for much smaller insureds.

Still, we think that this market has nowhere to go but up – as long as carriers can still write at a profit. The proliferation of data breaches and the increasing sensitivity of the public to protection of their private data surely means increasing levels of claims. Perhaps offsetting this increase in claims will be the opportunity to respond to breaches more cost effectively, as carriers negotiate lower response costs and law firms get more competitive in their pricing.

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. 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 continue at a disturbingly frequent rate. We are unsure if this is a result of increased reporting (breaches happened before but were not disclosed) or increased activity by, and effectiveness of, hackers, but it is eventually 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 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.

Pre-breach services in the past were less likely to be a compelling reason for insureds to buy

Cyber policies, although excellent information and tools have been available. An exciting new trend to expand pre-breach services may provide additional reasons to buy the coverage. We think these services could alter the competitive landscape for Cyber insurers as well as improve their claims experience. As Cyber further penetrates the smaller and medium-sized account market, such services will be increasingly appealing to Insureds and valuable to insurers.

We 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 a great deal of 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. With much data moving to the cloud, this accumulation risk is becoming more severe, a trend that concerns us greatly.

We spoke with Mike Brown of reinsurance intermediary Guy Carpenter at the May 2013 Cyber Liability meeting of the Reinsurance Association of America about support. He summarized the reinsurance market for Cyber coverages in this way:

- There are very few stand-alone Cyber-only Reinsurance Treaties
- Most reinsurance of Cyber is embedded in E&O/D&O treaties
  - 20+ reinsurers currently supporting Cyber business as part of a larger treaty
  - Under 10 reinsurers support a limited number of stand-alone Cyber treaties
- Quota share is most common structure
  - Excess of loss possible, if part of a broader treaty
- Treaty features
  - Sub-limited coverage when part of broader treaty (understanding of loss potential still evolving, technology rapidly changing and lack of premium-to-limit balance)
  - Attachment point restrictions (claims handling knowledge and resources important for primary layers)
  - Event limits (aggregation concerns for 1st party exposure- especially business interruption/increasing exposure from Cloud Computing)
  - Industry Restrictions/Exclusions (Social networking, Online gaming, Public Entities, Universities)

Most carriers report 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 25% to over 100%. Only one of these carriers reports growth of over 100%, but several others report between 50% and 100%. Most were in the 10-25% range, and only two were under 10%. This is impressive, considering the difficult economic conditions many insureds were operating in.

Newer carriers are reporting strong 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. In our consulting, we have seen several instances where incumbent carriers greatly expanded their limits only as a result of the threat of being replaced by

newer entrants to the Cyber Risk insurance market.

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

State of the Market – Trends in 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 similar to what we heard in 2011 and 2012, despite the continuing slow rise in commercial insurance rates.

Rates for Cyber Risk insurance, unlike the traditional commercial insurance lines, are still showing some signs of softness. Although there were a few reports of plans to reduce rates on the order of 5%, the predominant mood was to hold rates within a range of stable to an increase of 1-5%.

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.

We also asked about trends in deductibles and self-insured retentions – the overwhelming sentiment was to keep them as they are now.

Capacity and Deductibles

Significant liability capacity exists, and higher limits can probably be stacked up if desired. Several of the carriers in this survey are willing to sit as excess over primary coverages.

Reasonable (account appropriate) retentions or deductibles are available. Deductibles or retentions can be quite competitive; the table shows minimums, of course. Large retentions ($500,000+) should be expected for larger insureds. We are not seeing carriers changing their deductible or retention strategy, generally willing to continue the levels of retentions they have been offering. The exception might be the smaller-sized insureds, which are being offered even lower deductibles than before.

An Overview of Data Privacy Coverage

In the data security business, there is a phrase: there are organizations that have breaches and

know it and there are organizations that have breaches and don't know it - yet.

We find that most prospective insureds (and their agents and brokers) are most interested in coverage for data breaches. This coverage is found (or is available) in almost all Cyber policies.

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
- 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 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
- Non-electronic 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 notify 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

Are there more breaches than insurers realize? And will the prevalence of Cyber insurance make breaches more visible? We think the answer to this is yes, even though governmental breach reporting requirements have taken hold.

Remediation Coverage Services

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

Carriers often offer prepackaged and pre-negotiated 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 may 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.

We find that insureds are increasingly concerned about the theft of the economic value of Intellectual Property. This comes from reports, we believe, of increasing levels of industrial espionage by competitors and by governments acting in support of their economic and defense interests.

We have added a new column to the Theft table as well as to the Exclusions 2 table to capture the insurer's coverage position regarding theft of IP. In asking the insurers about this coverage, we emphasized that it references the economic value of IP. Unfortunately, we don't think that the responses are always accurate and will attempt to refine them in our next Report.

For insureds interested in coverage for the theft of the economic value of their IP, further investigation is suggested.

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 includes a table that summarizes the (optional) Media Liability coverage that they might offer a Cyber Risk insured. It includes information as to whether:

- Coverage applies to all types of media, or is restricted to social media only, 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 re-

serve 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 becoming more prevalent in this product line

Specific Coverages Included in Policy

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

- 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 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 2013).

Exclusions

Exclusions are many and varied, as would be expected; please read those tables carefully. The tables have been simplified by removing exclusions primarily related to Technology E&O.

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

Risk Management Services

2013 is the year in which Cyber-related Risk Management services began to reach their full potential – a very positive development for the insureds, their intermediaries, and for the carriers themselves.

We have been describing the parallels in services between the Cyber insurance line and other lines, especially Employment Practices and Property (Highly Protected Risk particularly). Cyber-related Risk Management services, while helpful, have been relatively weak when compared with these other lines. This is certainly understandable for this still-relatively new line of insurance, especially considering the wide array of potential services (and potentially high cost).

To try to capture more information about the services that are available to insureds via their insurance purchase (and frankly, to encourage further development of the product), we have changed our approach in the Risk Management Services table.

This table now asks for information on the following types of services:

- Active Avoidance – which indicates whether the carrier includes products and/or services that help the insured actively protect data from breach or other covered loss (the property analogy would be sprinklers. This is intended to indicate capabilities that act independently to protect against activities that lead to breaches.
- Pre-breach Planning – services and/or tools that help the insured to prepare a contingency plan for use in the event of a breach (think of disaster recovery)
- Helpline – a staffed resource that fields questions via telephone or email (think of an EPLI helpline)
- Information Portal – a source for information and possibly tools to help in the management and response to data protection and breach

The column 'Other' allows the carrier to describe additional types of services.

Summary

Cyber/Privacy insurance products are evolving rapidly, especially in terms of market segmentation and value-added Risk Management services. Pricing remains competitive, but there is no extensive rate cutting to gain market share. Carriers are no longer pouring into the market, but instead are improving their products as they learn more about what insureds need (and desire) from their insurance purchase.

We also see carriers building out their underwriting and claims staffs to meet the needs of the many insureds and potential insureds. Underwriting discipline seems to be intact.

But there is a worrying trend - insureds are concerned about coverage for exposures beyond the criminal activity that has been the dominant exposure to date. They are worried about attacks by hostile parties such as state actors (foreign nations), non-state actors (terrorist organizations or individuals), hacktivists that seek to embarrass or damage the victimized organization, and industrial espionage that seeks to gain economic advantage via data theft, damage or disruption.

We wonder to what extent the Cyber insurance industry will be able to provide protection against such acts. Clearly war and terrorist-based claims have been difficult or impossible to insure without governmental intervention. What about these risks in the Cyber area?

* *

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

Data Breaches are Inevitable—But Reportable Breaches are Not

David A. Kruger

Senior Architect, Absio Corporation

As the title implies, this is a bad news/good news story. The purpose of this article is twofold. The first purpose is to dispel two common and potentially costly myths about data breach prevention and mitigation. The second purpose is to show how data breaches can be made reliably non-reportable.

Myth #1—The Perimeter can be Secured

When most people talk about securing their data, they speak in terms of building a wall around it so only those with the proper permissions access it. You can tell because the conversation about protecting data is usually framed as "protecting our network", with the "our network" part being the operating definition of what must be secured. Protecting the network, commonly called perimeter defense, is vital and necessary, but by itself it can only prevent some breaches some of the time. Perimeter defense plays no role in mitigating the damage from breaches.

The problem is that the perimeter has become impossible to define, much less protect. Defining the perimeter was easy when the IT department was a mainframe with directly attached dumb terminals accessible only by authorized persons. Now, the perimeter is a complex collection of hardware comprised of servers, routers, desktops, laptops, tablets, phones, and peripheral devices such as printers, scanners, and cameras, some owned by the organization, but many not. This mass of hardware, any of which may contain data the organization is required by law to protect, is continuously being connected, disconnected, and reconnected to each other in varying configurations via an uncountable number of internet, web, wireless, cloud, or physical connections. Some of those connections endure but most are ephemeral. These connections are made and managed by an ocean of users, some human but others that are not, i.e. any software that connects to your network. Some users are known, but many are anonymous.

Additionally, there are an ever-present malicious few disguised as good people/good hardware/good applications. They are always probing for that one vulnerability which will allow them entrance. Imagine if you will a fortress with infinitely long walls, with an infinite number of doors opening or closing thousands of times a second, each letting in or excluding someone or something that may or may not be good—that's the perimeter. An attacker only needs to get through one door, one time, to initiate a breach.

Perimeter security assumes that everyone you've let inside is trustworthy but unfortunately that's just not so. Some insiders are honest but untrustworthy; they simply may not understand or remember information security policies and procedures, especially when those policies and proce-

dures are complex, burdensome, and ever-changing. Good people need only to be conned once by a malicious outsider (human or malware) or use a compromised computer one time for data to be breached. And of course, not all insiders are honest.

To validate the limitations of perimeter security, scan the daily news to find examples of sophisticated, diligent, security-conscious organizations suffering major data breaches. Somebody and/or something got into their network and smuggled out supposedly protected data despite the organization's best efforts.

Safe Harbor—Easy to See, Hard to Get To

The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), The Gramm-Leach-Bliley Act (GLBA), the Federal Trade Commission (FTC), forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands exempt encrypted information from breach notification requirements[1]. Collectively, these are commonly called "safe harbor" exemptions. If safe harbor cannot be claimed, breach notification is required; fines, penalties, and damage awards in the millions of dollars are possible. Note that there are two requirements for claiming safe harbor and they are distinct: 1) encrypting data and 2) and being able to defend the claim to safe harbor; that is, provide credible evidence that data was encrypted when it was breached. Meeting these requirements is not as easy as it may appear. The reason is the mechanics of breach.

[1] Congressional Research Service, "Data Security Breach Notification Laws", Report R42475, April 10, 2012, Gina Stevens, Legislative Attorney

The Mechanics of Breach

When data is breached, it is not like a stolen can of peas whose absence can be identified and quantified because there is exactly one can of peas missing from the pantry. Unlike the singular and distinct stolen can of peas, data cannot be recovered and returned to its place in the pantry. Data is breached by making perfect copies and exfiltrating them; the originals never leave. Most breaches are discovered days to months after the breach occurs. It is usually impossible to know exactly what subset of data out of the whole, i.e. which particular can out of all possible cans, was taken. Breached data can be endlessly copied and redistributed to any number of persons at any time after the breach.

Breaches are unpredictable; it is impossible predict what subset of data might be breached or when it might be breached—it is only possible to predict that it is highly likely some data will be breached at some time in the future. Since it cannot be known in advance what data might be breached, the solution is continuous encryption, that is, to encrypt all data all the time.

Data must be momentarily decrypted so it can be viewed or edited. For example, there may be thousands of Microsoft Office files, video, audio, images, and datasets (extractions from a database) on a computer; only the ones in use need to be decrypted. In order to make certain all the data not in use remains encrypted, each bit of data must be separately and distinctly encrypted, that is, each given its own lock and key. That way, it can be

unlocked (decrypted) for use without decrypting, and thereby jeopardizing, all the other data that is not in use. This is called granular encryption.

Furthermore, since breached data is, by definition, already outside the network, the means to assure that it cannot be decrypted by either authorized or unauthorized users on an unauthorized device or with an unauthorized application is required; otherwise, encrypted data could easily be emailed or downloaded to removable media and decrypted outside the network. These requirements lead us to the second myth.

Myth #2— We Encrypt, therefore our Data is in Safe Harbor

Unfortunately, that may or may not be true. Breach mechanics complicate defending claims of safe harbor. Said another way, proving that a door is lockable is simple; one need only show the lock is present and that it works. However, proving that a door was locked at one particular moment in time is complicated. It requires the means to continuously monitor and log the lock's status (locked-unlocked-relocked).

The most commonly used encryption solution for edge devices such as desktops, laptops, tablets and phones is called Full Disk Encryption (FDE). FDE *only protects data when the computer is turned off,* which is great if the computer is lost or stolen. The problem is that 99% of breached data is exfiltrated from operating devices[2]. When FDE-protected devices are operating, unencrypted data can be breached at will.

[2] "2012 Data Breach Investigations Report", Verizon

There are encryption solutions for devices in operation but most require users to manually select which files or folders to encrypt. Depending on busy, forgetful, or malicious human beings to always encrypt the data they should, when they should, practically guarantees some data will go unprotected. When data has to be decrypted to be worked on and manually encrypted when the work is done, it is all too easy to forget or get distracted and leave it unprotected. Many encryption solutions can be turned off by users or administrators—which means someone also has to turn them back on. To make safe harbor requires that encryption is automatic and cannot be turned off by users.

Finally, many encryption solutions lack the logging capability to provide evidence to a regulator or jury that breached data was encrypted when it was:

- exfiltrated by a careless or socially engineered (conned) or malicious insider, or
- exfiltrated by malware or by some other hack, or
- exfiltrated when it was intercepted in transit, or
- on a device or storage media that was lost or stolen.

Further complicating matters are regulations that potentially impute liability for a single breach to multiple organizations that move and store protected data amongst themselves. A case in point is the recent HIPAA/HITECH Omnibus where the federal common law of agency can be applied to healthcare organizations that send electronic protected health information "downstream" to other organizations for further processing (such as third party payers or billing firms).

If the downstream organization has a breach, the upstream organization can be held liable. It is reasonable to expect the federal common law of agency to be more broadly applied to those who store, share, and send protected information of all sorts as regulators seek larger fines to enforce compliance, and in some cases, seek larger fines to increase revenues to fund themselves. The proactive solution is to enable organizations to maintain visibility and control of the downstream movement, storage, and use of data they are responsible to protect.

To ensure that claims of safe harbor are defensible, what is required is a solution that provides automatic continuous granular encryption, can't be turned off, provides an audit trail, and enables the persistent control of the downstream movement, storage, and use of protected data.

Information that Controls Itself

These requirements can be met by binding encryption, distribution, and audit controls to the information itself so the controls stay with the data as it moves.

Advancements in technology have only recently made this type of solution possible. Edge devices now have sufficient computational power to allow those responsible for protecting data to control the encryption, distribution, and audit trails of individual *content objects*. Content objects are discrete sets of digital content stored or transmitted by a computer, such as files, emails, audio, videos, images, or datasets.

Let's give these information objects a name: Secure Extensible Global Content Objects (SEGCOs).

- *Secure* means that objects can only be decrypted by specified users, applications, and devices.
- *Extensible* means that the capabilities of objects can be extended to meet new requirements and changes in the computing environment, making it straightforward to maintain "backward compatibility" as systems evolve.
- *Global* means that applications running on different operating systems and device types can all use the same content object.
- *Content Objects*—files, emails, audio, videos, photographs, datasets, et al.

Most organizations have multiple applications handling the information they need to protect. Fortunately, SEGCOs can be incorporated into just about any type of software application.

As we stated earlier, breaches are inevitable, but reportable breaches don't have to be. If the breached data is in a SEGCO, claims of safe harbor can be readily defended. And that should be good for data holders, their Cyber insurers, and society in general.

About the Author

David A. Kruger is Senior Architect for Absio Corporation, which provides persistent information ownership and control for business, government, developers and consumers. Mr. Kruger can be reached at David.Kruger@Absio.com or 972.814.5015

Like What You See in this Executive Summary?

IRMI Risk & Insurance KnowledgeBase • Education • Community

You won't believe the value in the full reports. Now Available on **IRMI Online**® and **ReferenceConnect**™

The Betterley Report provides insightful insurer analysis on these six markets and coverage lines:

- Cyber/Privacy Insurance Market Survey
- Technology Errors & Omissions
- Employment Practices Liability Insurance
- Side A D&O Liability Insurance
- Private Company Management Liability Insurance
- Intellectual Property and Media Liability Insurance

Each annual report provides a comprehensive review (50 to 175 pages) with numerous exhibits of the critical differences in insurers' coverage, market appetite, and capacity. **You save valuable time** because *The Betterley Report* has done the groundwork for you, providing practical information in a fully searchable online format.

What do you think this dedicated research team and related market analysis is worth to you and your team? Well, you are going to be pleasantly surprised when you see how we've priced it for you.

Agents and Brokers—Sell more and grow revenue by pinpointing errors in competitors' policies/proposals.

Risk Managers and Insurance Buyers—Identify, eliminate, or avoid coverage gaps with coverage comparison charts.

Underwriters—Research competitors with quick policy comparisons.

Attorneys—Keep up with year-to-year trends in policy form development.

Consultants—Identify markets and match them up to your clients' needs.

See more benefits and read Executive Summaries of each report at **www.IRMI.com/Go/3.**

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

The Betterley Reports are produced annually, and range from 50 to 175 pages in length. Current analyses include:

- Cyber and Privacy 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? Need the best analysis of leading edge insurance products? We've done the ground work for you!

The Betterley Report is distributed by International Risk Management Institute, Inc. (IRMI) and may be accessed by subscribers on IRMI Online. To purchase a subscription, call IRMI Client Services at (800) 827-4242 or learn more on IRMI.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.

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

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