February 2010

BRC

The Betterley Report

Technology Errors & Omissions Market Survey – 2010

Increased Awareness and Customer Demand Will Fuel Growth

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

Editor's Note: We are pleased to present our tenth evaluation of Technology Errors & Omissions insurance, in which we review twenty of the leading carriers active in the market. We welcome Hanover's Business Owners Program (BOP) to our Report, as well as the return of Zurich to the Survey. There are also two name changes to note: AIG is now known as Chartis, and the Darwin program is now listed under the Allied World (AWAC) Darwin name, reflecting Darwin's acquisition by AWAC.

Tech E&O is coverage for the liability of organizations and individuals that provide products and services utilizing technology. Depending upon the carrier, insureds can include manufacturers, software developers, consultants, service providers (such as systems integrators), and telecommunication companies.

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.

In most cases, we examined actual policy forms and endorsements provided by the carrier. Rather than reproduce their exact policy wording (which can be voluminous), in many cases we 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 interpretation of their policies or survey responses.

In the use of this material, 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. Professional counsel should be sought before any action or decision is made in the use of this information.

Since privacy risk is the driving force behind the growth in Technology E&O interest, we asked Matt Cullina, CEO of Identity Theft 911, to describe to our readers what actually happens after a cyber breach. Entitled **"We Had a Data Breach – Now What Do I Do?"** *we hope this article (see page 10) sheds some light on how a company or organization might respond after a data breach occurs.*

For update information on this and other *Betterley Report* coverage of specialty insurance products, please see our new blog, *The Betterley Report on Specialty Insurance Products,* at www.betterley.com/blog.

NEXT ISSUE

April 2010
Intellectual Property & Media Liability Market Survey

List of Tables

Contact Information 11
Target Markets 15
Limits, Deductibles,... 17
Policy Type, Who is Insured? 18
Data Privacy: Types of Coverage and Limits 27
Data Privacy: Coverage Provided 33
Data Privacy: Coverage Triggers 37
Data Privacy: Types of Data Covered 43
Data Privacy: Remediation Cost Covered 47
Data Privacy: Remediation Coverage Services 50
Definition of Products and Services 52
Definition of Damages 62
Other Policy Definitions 68
Definition of Defense Expenses 76
Claims Reporting 79
Prior Acts 84
Coverage Territory 85
General Insurance Exclusions 86
Product-related Exclusions 93
Service and Security-related Exclusions 98
CyberRisk-related Exclusions 102
Risk Management Services and Charges 104

INTRODUCTION

Coverage for the liability arising out of the design and manufacturing of technology-related products, the creation and implementation of software, and the provision of related services, is a growing business, with specialty coverages designed to cover the Errors and Omissions liability that may not be covered under traditional liability policies. Tech E&O coverages can be purchased for technology consultants, systems integrators, application service providers, Internet service providers, Internet retailers, network electronics manufacturers, medical technology manufacturers, and telecom companies. With a wide variety of coverages available, and each written on a non-standard form, insureds and their advisors can be confused and bewildered at the choices.

Coverage for Breach of Data Privacy is the hot topic in Tech E&O product discussions, as both service providers and site owners grow increasingly anxious about loss of data. While most of the news has been about data breaches suffered by site owners, technology service providers have been – or ought to be – concerned about their own exposures. When we surveyed our readers late last year, over ninety-five per cent of the respondents listed Cyber Risk and Technology coverage as 'highly interesting' or 'somewhat interesting'. We think that privacy risk (and coverage) drives this interest.

Data Privacy insurance comes in three basic forms: Liability, Remediation (sometimes called response costs), and Fines or Penalties coverage. To illustrate the types of coverage offered by each insurer, we have developed six *Data Privacy* tables:

- Types of Coverage and Limits Available
- Coverage Provided
- Coverage Triggers
- Types of Data Covered
- Remediation Costs Covered
- Remediation Coverage Services

There is confusion in the marketplace about Data Privacy coverage and how it is provided for service providers (Tech E&O) and site owners (Cyber Risk [see our June 2009 Report]); we have tried to rationalize this discussion by asking our participants broad questions about their coverages, recognizing that a service provider's risk can arise from a breach of their own data, their failure to prevent a breach of their client's data, and/or their own loss of client data while in its possession. We hope this approach brings some coherence to the discussion.

Please see our discussion under Data Privacy on page 5 (and the tables) for details.

Insureds looking for Tech E&O coverage are presented with a choice of buying individual policies that supplement their core General Liability policy, or a policy that includes both GL and E&O. In our experience, most insureds purchase separate policies, although a handful of carriers offer a combination of the two.

Tech E&O policy provisions should always be reviewed in connection with the insured's CGL policy provisions, especially with respect to new or emerging exposures of concern. Some carrier markets offer coordinated E&O and CGL coverage, whereas other markets may offer monoline E&O only. Coverage not provided or excluded by an E&O policy may well be addressed by the CGL. Given the complexity of the coverage choices, a good insurance broker can offer a lot of useful advice to prospective insureds, and their value in negotiating coverage is not to be underestimated.

NEW AND INTERESTING

Demand by third parties is starting to drive the market—Technology product and services providers, the audience for this coverage, is seeing greatly increased demand for proof of privacy insurance by their business partners. These clients are concerned about technology risk, and want proof that their vendors are covered. Proper coverage and significant limits are required by new or existing vendors if they want to do business with many organizations.

We think that this demand will be a strong force in growing the market for Technology E&O products. While historically many technology companies have been reluctant to buy coverage, the demand by clients to buy it or perhaps lose a valuable business relationship will greatly expand this market. As more and more data is held by multiple parties, the desire for protection is increasing—a positive for the market segment.

Options for the small- to middle-market insured are increasing—Hanover Insurance Group, a company that is expanding its role in the specialty lines area, has hired Anthony (Toby) Levy, formerly of The Hartford, to build their technology insurance capabilities, including new E&O products. Although not the only carrier entering this market space, Hanover represents a trend of hiring experienced technology underwriters to add specialized capabilities to their Main Street insureds. We included Hanover's new BOP product as an example of how carriers might offer cost-effective coverage to their smaller insureds.

To be fair, we should note that this product is intended to be a cost effective option for insureds that may not be interested in securing a standalone policy, and so should be judged a bit differently than the higher-end products. Hanover intends to bring out more specialized Technology E&O products later this summer.

Increased interest by risk management service providers in supporting Technology E&O insurers—Much like the Employment Practices Liability market segment, risk management service providers are seeing that they can greatly extend their reach by providing their services through an insurance policy. We think that it is a natural fit for carriers to identify quality vendors that can help the insureds avoid data breaches, and to provide cost-effective responses if a breach occurs.

STATE OF THE MARKET

Annual premium volume information about the Tech E&O market is hard to come by. As in years past, we surveyed participating Tech E&O product managers, asking them for a range of gross written premiums for U.S.-based insureds and for non-U.S.-based insureds. While there was a fairly wide range in the U.S. responses, there seemed to be some consensus in the $800 to $900 million range. There seems to be a bit of growth happening as insureds and their business partners see the need for coverage in a world where data breach is all too common.

Unfortunately, non-U.S. premium estimates were very hard to come by. Our participants mostly answered 'don't know,' although of those that did respond, $100 to $200 million was estimated. Although we have very little confidence in this estimate.

Individual carriers reported reasonable growth rates, considering the dismal state of the U.S. economy during 2009, and the significant rate competition as carriers fought to retain their existing insureds. Individual carriers reported changes in gross written premium ranging from nil to as much as a 25 percent increase.

As mentioned earlier, there should be significant growth from new insureds that finally 'bite the bullet' and buy coverage, driven by their increasing concern about data breach, privacy risk, and client demands for coverage.

It is also likely that there is much more premium to be found in the more traditional markets, but it is not being reported as Tech E&O. We continue to expect that there are many more potential insureds that need Tech E&O, but are either not aware of its existence, or underestimate its value. This is likely to be true for the smaller service firms.

We asked carriers about the health and interest of the reinsurance market that supports Tech E&O products, and they generally reported that reinsurers still like the product. Stable or increasing interest in Tech E&O product support was reported by the responding carriers.

State of the Market—Rates and Retentions

We asked the carriers whether, or not, they planned rate decreases (or increases) during the upcoming year, and what they expected of their competitors. Most offered their thoughts.

The level of retentions or deductibles that carriers are willing to write continues to be flat. None of the carriers reported plans to increase retentions, and that was mostly to bring them into line with their competitors. Isolated prospective insureds may be able to achieve lower retentions but we don't believe that it represents any type of trend.

Last year we saw rate decreases, but indications that rates would firm; this apparently never happened, as the slowdown in the economy exacerbated rate competition. For 2010, we are hearing of rate decreases of nil to 10 to 15 percent. There seems little likelihood of a rate turnaround anytime soon.

It is exceedingly difficult to predict the direction of Tech E&O rates in the coming year; insurance industry leaders, both in the Tech E&O segment and commercial lines in general, are promoting an increase in rates. This is to be expected, as the carriers would very much like to raise their rates. Whether the market will let them is another story.

The saga of AIG, now Chartis, continues to preoccupy the market, with staff changes, alleged price sharpening to retain business, and the overhanging influence of Washington. However, they continue to be a serious force in the market, apparently retaining most of its book of business. Whether Chartis is underpricing its renewals to retain business, as has been alleged by some carriers, or they are simply acting like any other rational insurer (refusing to lose good customers because of price), is unknown to us. We do know—or at least surmise—that the threat of retention pricing in and of itself helps keep the market soft.

We expect this to continue, as they need to give their customers a good reason to stay with them. Attractive premiums, and possibly coverage enhancements, are the only way they will be able to get their insureds to justify the perceived risk of continuing to insure with them.

So, while carrier executives are promoting the idea of higher rates and an end to the soft market, we don't think that the individual carrier problems are going to be the driving force. In fact, those problems may well dampen the push for higher rates. It seems that the Technology E&O product, like most commercial insurance products, is mired in a continuing (slightly) soft market. Although, unlike many other products, there is the prospect for significant growth in total premium written as new insureds sign on in significant numbers.

Target Markets and Prohibited Insureds

Unlike most of our surveys, there are significant classes of business that some carriers indicate are prohibited. Problem classes seem to include financial transaction systems, Internet Service providers, and security-focused risks.

Read the *Target Markets* table carefully as a guide to which carriers like (or don't like) certain classes of business, but also keep in mind that these can change, and are often subject to reconsideration.

Capacity and Retentions

Significant liability-limits capacity remains, and reasonable (account appropriate) retentions or deductibles are available. $25 million can be arranged by ACE, Chartis, Chubb, OneBeacon, Safeonline, and Travelers. Up to $20 million is available from Axis, Beazley, and Hiscox, while $15 million can be bought from CNA, The Hartford, and Philadelphia, with up to $10 million from Allied World/Darwin, Euclid, and Zurich.

Lower limits can be arranged with Evanston, NAS, and PLIS ($5 million), $3 million from Admiral, and $2 million from the new Hanover product.

Most carriers can secure limits above those indicated when necessary, noting in particular Euclid's interest in writing excess limits.

Deductibles or retentions can be quite competitive; the *Limits, Deductibles, Coinsurance and Commissions* table shows minimums. Lower deductibles are generally available from the carriers offering lower limits, those that may best appeal to the smaller insureds that desire low deductibles.

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

DATA PRIVACY

We are often asked whether, or not, coverage in a Tech E&O policy includes losses arising out of data breaches. For the acts, errors, or omissions of the service provider, they often do. If the provider's services fail(ed) to protect the client's systems such that a data breach occurs, then it may well find coverage in its E&O policy even if there is no specific reference to privacy concerns.

However, policies are evolving to specifically address privacy-breach claims, in part so the coverage may be more specific to such claims, and in part because the worry about liability shouldn't be the only concern.

We also note that electronic data breaches are generally everyone's first concern, but nonelectronic data losses are also a worry. Some Tech E&O carriers have addressed these concerns by including affirmative coverage grants.

As a result of our research into privacy exposures and coverage, we have identified six key areas that should be considered.

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, unauthorized access to a client's 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, though 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 now commonly accepted coverage for Tech E&O; this coverage is for the costs of responding to a loss of data. Organizations that suffer a data loss may be required to notify their customers and clients 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 costs can be covered by most of the insurers, though we predict that the rest will have to start offering these coverages in order to compete. We now think that, for service providers, it is just as important as it is for site owners. Either way, most prospective or actual insureds have not experienced a breach that required remediation; when it happens, it may well be the first time they have seen it. Knowing what to do, which vendors to use, and how to control costs, will be a serious challenge. Having a carrier with prearranged remediation plans and vendors will be a huge benefit to the breached organization. We think it's a lot like the Kidnap and Ransom line; when a kidnapping occurs, the insured needs to make fast and correct decisions—the right insurance policy can significantly improve the prospects of a successful response.

Remediation costs can include:

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

We spoke with Mark Greisiger about the magnitude of risk for organizations that keep customer data. Mark is the President of NetDiligence, a leading cyber security assurance services company with extensive experience in protecting companies against privacy beach (www.NetDiligence.com).

According to Mark, external post-breach expenses (not all of these are necessarily insured) can be thought of as:

- Cyber-crime attorney services: fees run $400 per hour (note: A lawyer knowledgeable on security/ privacy standards and the 46+ state laws that require customer notice following a data breach notice is important). Also important is guidance on any Federal regulation such as HITECH and FACTA). This initial legal assistance fee may be approximately $2k to $10k for an average national breach. This does not include future defense counsel costs.
- Investigation: This part of the process can get expensive. A lot of factors come into play here. For example, was the data breach centralized, or was it decentralized across many store (Point of Sale terminal) locations. The cost could be millions of dollars for a significant breach. Computer forensics fees ranging from $300 to $700 per hour to:
  - Stop the attack or close the security hole.
  - Determine whether there was a breach, how, when, on what machine, and did they access and steal client data.
  - Which customer's NPI data was impacted & where do they reside?
  - What type of data was breached (i.e., credit card alone; name/ address; more sensitive data such as SS#, drivers license, date of birth, medical records)?
    - Determine – source and method of attack.
    - Gather e-discovery evidence properly for criminal and civil litigation.
    - Purchase & install new software/hardware to strengthen defenses.
- Notification Costs: Set up a Website with FAQ notice information, set up a customer hot line support number, and mail a breach event notice letter to affected customers at as much as $9 per customer.
- Credit Monitoring: post breach package - $10 to $60 per year per person (depending on size of breach records) Note that there are some 37 varieties of 'identity theft' types, and only a few situations in which the data ill gotten may trigger the credit monitoring agency databases. Thus a credit monitoring service alone as a remedy may be more value to those data breach victims whose Social Security #s was the data type involved in the breach. But on the other hand the same monitoring service might not be the most effective service if, for example, only credit card #s or medical information was breached.
- Public Relations Experts: to deal with the media with charges running perhaps $10,000/month billed at rates at $400 per hour

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. A few of these services have a time limit for use, especially credit monitoring.

POLICY FEATURES

With the wide variance in coverages included in Tech E&O products, paying close attention to key features is important.

Coverage for liability arising out of the actions of subcontractors while working on behalf of the named insured is generally included in the basic policy form. However, most will not include coverage for the subcontractor itself, unless special arrangements are made.

The definition of Products and Services is critical for proper coverage; the policies define the products and/or services that are covered. There are two different ways this can be done: either the declarations page specifies the products and/or services covered (which comes from the application) or the policy definition itself defines the activities covered. Almost all of the carriers use policy definitions.

Either way, it is critical that the products and/or services of the insured be listed properly or defined as included in the policy. Wording is shown under Definition of Products and/or Services Defined in Policy included in the table *Definition of Products and Services.*

CLAIMS REPORTING, ERP OPTIONS, AND COUNSEL

Each Liability policy reviewed is a claims-made form so Extended Reporting Period (ERP) options are important. All carriers offer a Supplemental Extended Reporting Provision, but they range in length. Carriers will sometimes negotiate additional optional periods and/or cost.

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. In practice, carriers are generally willing to use legal counsel that is satisfactory to both the insured and the insurer.

Carriers offer varying levels of control (or at least, influence) in the selection of counsel, ranging from selection exclusively by the insurer, to the choice of counsel by the insured. 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; as an example, several carriers reserve the right to choose counsel, but indicate prenegotiated counsel will be considered on a case-by-case basis.

Generally, carriers can impose the infamous "hammer clause" on lawsuits that an insured may not want to settle. The use of "soft" hammer clauses has not penetrated this product as it has in Employment Practices and Management Liability products. An important exception to this is Allied World/Darwin, which provides a 50 percent soft hammer clause. They were joined in 2008 by Philadelphia, indicating, we thought, a trend in offering soft hammer protection. However, none of the carriers in this survey have added a soft hammer for 2009 or 2010.

PRIOR ACTS COVERAGE AND TERRITORY

All carriers offer Prior Acts coverage, with previous coverage usually required by all carriers, although many may require previous coverage based upon underwriting criteria. Technology is a worldwide business, and one of the liability problems is that the legal standards of many countries differ from those of the U.S.

All carriers offer worldwide coverage if a suit is brought in the U.S., Canada, or possessions. True worldwide coverage (suit brought anywhere) is available from each of the carriers reviewed except Admiral.

EXCLUSIONS

Rather than try to recite them here, the information for each carrier is found in the *Exclusions* table. Exclusions are many and varied, as would be expected; please read those tables carefully.

Unlike our other Reports, we have categorized the exclusions into:

- General Insurance exclusions (bankruptcy, dishonesty, intentional acts, expected or intended damages, SEC, unfair competition, piracy, and punitive damages).

- Product-related (product recall, cessation of support, direct property damage, direct bodily injury, loss of property, contingent bodily injury/property damage, prior to customer's acceptance of your work, breach of warranty, and hardware)

- Service and Security-related (contractual liability, cost estimates exceeded, performance delay, security breach, failure to prevent virus passing or data theft)

- Cyber Risk-related (personal injury, advertising injury, intellectual property, and Public Key Infrastructure)

A few comments on some of the exclusions that are specific to Tech E&O:

- Cost estimates exceeded – this refers to exclusions for claims by customers that the cost of a project exceeded the estimate or proposed fee. Carriers do not want to pay claims for poor pricing decisions of their insureds.

- Performance delay – this arises out of the insured's failure to meet project time deadlines, and is included in policies to protect carriers against an insured's overly optimistic promises.

- Security breach or unauthorized access – this is a very important set of exclusions for any insured that offers services related to secure data, including ecommerce. Some carriers will provide coverage if the insured is providing services related to security, while others will include coverage as long as the breach is on the system of others (i. e., not the insured), which is after all the intent of E&O coverage.

- Intellectual property – infringement of patents, copyrights, or trademarks is a source of much litigation, and coverage is rarely available when an insured is sued. Each carrier handles this very differently; read this portion of the *Exclusions* table carefully.

- Public Key Infrastructure (PKI) – the term used to describe technology that enables secure online transactions.

RISK MANAGEMENT SERVICES

Supplemental loss avoidance and control services are now much more prevalent in Technology E&O, which we approve of, considering the ability of such services to reduce or eliminate losses, for the benefit of both insureds and insurers. Please see our *Risk Management Services* table for a description of the many services that carriers are including in their offerings to insureds.

Generally, the range of Risk Management Services offered is increasing, a trend we welcome.

SUMMARY

Technology E&O is an important coverage line, supporting the risk strategies of a key component of the U.S. (and world) economy. Marketing (smaller tech companies may not buy E&O, large tech companies may not think they need it) and product design (exploding privacy risk the most important) present challenges, as does rate adequacy. Sharp underwriting skills are needed in this line of coverage, as numerous types of business segments seek coverage.

We are seeing signs that the middle market is getting serious about this coverage – carriers are starting to move down market, and are beginning to encounter smaller competitors. This presents a real opportunity for significant growth in premium, as well as a way for middle market insureds to economically obtain expertise on how to handle a breach.

Privacy risk is now well recognized and insurance should be seriously considered. While some form of self insurance or self retention might make sense for large organizations, especially those with existing captives, the high costs of a breach and the unpredictability of data loss may make risk transfer appealing. Combined with increasing pressure by business partners to show evidence of real coverage, the days of self-funding this risk may be about over.

We always encourage readers and their advisors to carefully consider the type of coverage that they need and whether or not the policy they are considering is really the right answer to their needs. The large carrier offering may not be the best one for them, but then again, the smaller carriers may not offer enough capacity.

Innovation, driven in part by privacy risk concerns, is having a major impact on this line; we look forward to examining its continuing evolution.

We Had a Data Breach – Now What Do I Do?

By Matthew Cullina

With more and more companies being asked to handle vast amounts of personal information from customers, clients and employees, privacy-related risk is becoming a bigger concern every day. Whether this data is medical, financial or employee personal information, privacy and the risks associated with data breaches should actively be on the minds of businesses and their insurers.

While initiating best practices concerning security and privacy is the perfect way to minimize these risks, proactively putting the proper Remediation coverage and associated remediation services in place is the ideal scenario. Equally important from an insurer and insured perspective, is making sure that the required remediation vendors are chosen carefully as well.

But what happens when a data breach occurs? When it comes to remediating such a breach, the main goal should be to avoid liability and regulatory sanctions by "doing the right thing," immediately following the discovery of a data breach that releases personally identifiable information (PII) and/or protected health information (PHI). This attitude will also serve a company well with respect to the harshest aspect of a data breach – the loss in consumer confidence and company reputation that can often be the most damaging aspect of such a data breach.

Thus, by insuring the costs of remediation with carriers that offer services that provide: (1) Investigatory and forensic consulting; (2) Notification; (3) Credit Monitoring; and (4) Identity Theft/Fraud Resolution Services, organizations can meaningfully protect themselves from reputational damage and the potential liability associated with data breaches.

If breach incidents are handled in a predetermined and systematic manner, with determinations and responses formulated as the facts are gathered, the process goes considerably smoother and the most meaningful and cost-effective remediation solutions can be implemented. While each incident and organization is different, the ideal process followed by any organization that experiences a data breach generally goes something like this:

First, a predetermined internal breach team is called together to determine whether or not a breach incident actually has occurred. This is typically made up of the company security, IT and/or privacy personnel and often includes outside legal counsel. Outside counsel can be called to assist in, if not lead the investigation in preparation for future litigation. Involving outside legal counsel can be important in order for an organization to best encompass an attorney's ethical obligation of confidentiality and privilege surrounding any of the attorney's analysis or mental impressions of the situation. Outside counsel should usually also be utilized to hire outside investigators such as computer forensic staff or private investigators based on this same reasoning. At this point, of course, law enforcement and/or any relevant regulators should be contacted to document and (hopefully) investigate any criminal, regulatory or procedural aspects of the breach.

The next step is to have the breach team carry out fact-finding and make additional determinations regarding:

- the method or manner of the breach;
- the type of information exposed;
- the states affected; and
- whether the data was password-protected and/or encrypted.

By evaluating the above key areas, outside counsel and the internal breach team can most accurately estimate and evaluate the risk to the affected individuals and set up the most cost effective and realistic remediation solutions – and help avoid liability and future regulatory enforcement or legal claims. These solutions can then be offered up in the mandatory breach notification letters sent out, allowing affected individuals to opt for the additional tools or assistance being provided.

Again, the level of assistance and types of tools made available will depend on the situation.

For instance, in cases where only credit card numbers and PINs, but nothing else have been lost or stolen, making credit monitoring tools available simply doesn't make any sense. If any fraud were to result, it would not be picked up by credit monitoring but would be noticed when affected individuals looked at their monthly credit card bills. But if a breach incident releases people's Social Security number, date of birth, driver's license number and mother's maiden name, credit monitoring alone may not be enough. A more robust monitoring solution that offers both credit monitoring and public records monitoring, along with fraud resolution services would be the best response. Again, the remediation to a breach is going to be highly dependent on the situation.

In fact, the response to data breaches from a remediation perspective has evolved considerably since the passage of the country's first breach notification law in California back in 2003. Infamously known as "SB-1386," this regulation required that notice be provided to any person whose electronic PII has been disclosed by a business or agency. Soon after, other states, D.C., Puerto Rico and New York City passed similar laws. This established a baseline requirement across the nation that if an entity loses the PII of consumers, there is a duty and legal obligation to notify those individuals, typically by mail, of the loss of such data.

However, the public, state attorneys general and consumer/privacy advocates expect more. The general consensus has been: "thanks for telling me you lost my information, now what?" This has led to the increasingly common data breach remediation response of offering credit and/or fraud monitoring to all people affected by a data breach. While this too has been a step in the right direction, since it provides early notice of the misuse and/or misappropriation of a consumer's PII, the increasing attitude of consumers to breach remediation is that mere monitoring is STILL not enough.

The general attitude of the public, state attorneys general and consumer/privacy advocates when taken to the extreme can be summarized as: "Thanks for telling me you lost my personal information and thanks for giving me the credit monitoring to recognize when someone is using my information, but what am I supposed to do to clean up the mess they make with my credit and or identity once it's been misused?"

This has resulted in the clear recognition that the most powerful aspect of breach remediation when it comes to alleviating both the potential for civil and regulatory liability and protecting a company's reputation and goodwill, is to offer a solution that will provide BOTH a complete monitoring and identity theft/fraud resolution solution to the affected breach notification recipients. By providing both monitoring and identity fraud resolution services, it then becomes extremely difficult for an individual, class, or even a state or federal regulator to point to a legally cognizable harm to the consumer. Even more important is that by providing these identity fraud resolution services in conjunction with credit/fraud monitoring, the notification recipients have a duty to mitigate any of their potential damages (using the tools and services provided). If at a later date a lawsuit or regulatory action is filed claiming harm to the data breach notification recipients, a company can point out three simple remediation steps taken, that if the consumer had followed, would have substantially mitigated if not completely eliminated the damages and any harm caused to the consumer(s) in question.

The simple fact is that the mere fear or apprehension that one may become a victim of identity theft or fraud at a later date has yet to be enough to support a successful legal claim. By keeping the key components of breach remediation in mind, organizations can meaningfully protect themselves from reputational damage and the potential liability associated with these incidents.

An insurance industry veteran, Matthew Cullina is CEO of Identity Theft 911. He can be reached at (888) 682-5911 ext 3001 or mcullina@identitytheft911.com.

BRC

The Betterley Report is a series of six comprehensive Reports published annually. Each Report exhaustively reviews a single hot insurance product, covering topics such as:

- The leading carriers and complete contact information
- Target and prohibited markets
- Capacity, deductibles and commission ranges
- Sample premiums (where available)
- Critical coverage and claims differences
- Risk Management services

Most *Betterley Reports* are produced annually, and range from 25 to 75 pages in length. Current analyses include:

- Cyber Risk Policies
- Technology Risk Insurance
- Employment Practices Liability Insurance (EPLI)
- Private Company Management Liability
- Side A D & O
- Intellectual Property (First- and Third-party, as well as offense coverage)—*biennial*
- Pollution Liability—*biennial*

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 all the 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 insurance products.

To order, go to: http://www.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

For additional information or to order a subscription go to: www.betterley.com

ISSN 1089-0513