Cyber Insurance For Data Breach: Being Prepared If The Black Hats Come Calling

By Max H. Stern and William S. Berman, Duane Morris

Abstract: This article addresses the current business environment and the exposure companies, small and large, have to a potential data breach. Data is a resalable commodity, and traditional liability insurance generally provide businesses no or limited protection for the significant costs required to respond to a data breach. In response, an emerging market is developing of cyber insurance policies protecting network security and privacy. These policies offer firs-t and third-party coverages, and business policyholders should seek to negotiate an insurance policy on the best terms to meet their needs.

In the dynamic global economic environment, where data is a resalable, desired commodity, protecting data is increasingly important business priority. Business leaders no longer considered data security an IT function; data protection is a topic discussed in the boardroom and more companies are charging chief privacy officers with the responsibility to protect the company's and customer's data. The consequences of not doing so may result in certain data security-related issues being inadvertently overlooked or not considered.

To avoid the potential crippling costs of a data breach, companies have begun to do a better job identifying potential data breach risks and implementing internal and external mechanisms to protect such confidential data. Many focus their prophylactic efforts on ensuring that their company's technology policies are up-to-date and the encryption of confidential data. On the advice of their counsel, some business leaders have taken the additional step of expanding their insurance portfolios to include stand-alone insurance policies that cover network security and privacy breaches.

Many network security and privacy insurance policies provide protections against losses that are not otherwise insured by traditional liability policies. Few companies are able to absorb the internal and external costs associated with a data breach without material adverse effect, and even fewer businesses have a team of forensic, public relations and crisis management consultants in place and ready to spring into action should a data breach occur. A specifically tailored network security and privacy policy can provide companies with a unique set of insurance benefits and resources to assist in

the event of a data loss, including assisting a company with identifying how the breach occurred, helping to respond in the event of a data loss, and offsetting some of the costs associated with a data breach.

Identifying Potential Vulnerabilities

Regardless whether a decision is made to secure insurance protecting against a data breach, a company should identify any and all potential data breach vulnerabilities and seek to take all action to secure the data. If a decision is made to explore available insurance products, armed with information regarding the nature of the business's risks to insure, a business will be in the best position to identify and negotiate the most suitable insurance policy to protect against such risks.

The Data Commodity

Any business that collects, handles or stores confidential or private information is a potential target for those interested in profiting by selling that desirable information for nefarious uses. The size of the business is not a determinative factor in assessing whether a company may be a target or is at risk for breach; rather, if it collects, handles or stores confidential or private data, then the company potentially is at risk and would be required to respond if a breach occurs. Arguably, if a computer is connected to the Internet, a business is at potential risk for a data breach. But that is not the most common way data can be put at risk.

There are generally two common forms of data breaches. The most widely recently reported data breaches concern unauthorized computer system infiltrations that result in the taking of data. However, for years, data breaches occurred because sensitive, identifiable information was sent to the wrong recipient or devices, or documents containing sensitive, identifiable information were stolen.

The valuable data companies collect, handle or store includes: (1) personal identifiable information (PII), which may enable others to identify an individual; (2) personal health information (PHI), which may enable others to identify health conditions, treatments and payment information; and (3) personal credit and debit card information (PCI), which may enable others to utilize another's accounts.

In response to its recent data breach, the U.S. Department of Personnel Management entered into a $133 million contract to provide credit monitoring

for the roughly 21.5 million Americans whose personal identifiable data was stolen from the Department's computers. While the OPM data breach is quite significant in terms of the size of the breach and the costs, the $133 million costs solely represent the costs for credit monitoring of the affected individuals. That amount does not include other significant costs associated, which private companies (but not necessarily a governmental entity) would incur when a data breach occurs, including: computer forensics and other investigation costs, analysis of notification obligations to regulators and affected persons, notification costs, business interruption expenses, costs to defend lawsuits (including class actions) from affected third parties, costs to settle or pay damages or judgments with respect to third party lawsuits/claims, costs to respond to regulatory inquiries, costs to pay any assessed fines and penalties, and public relations/crisis communication expenses.

Breach Cost Per Record Is $217, And It Can Add Up Quickly

While most companies will not experience a data breach of the magnitude that hit the OPM, regardless of the size of the company, the global average costs per record breached is $154. The average cost per record breached in the United States is significantly higher, at $217 per record. Breaking down the averages by type of data, the costs for each PHI-related record average as high as $363, while retailers experiencing a breach of PCI average $165 per stolen record, and the public sector's average cost per breached record is approximately $63 per record.

A U.S. company with a loss of 10,000 records, depending on the nature of the record acquired, based on the average costs, likely would experience costs of over $2.1 million because of such a data breach. Because these potential costs are significant, and unless companies have the ability to pay these response costs or adequate insurance protection, a data breach could lead to jeopardizing a company's ability to continue ongoing operations.

Data Breach and Privacy Policy Should Be Included In Companies' Insurance Portfolios

Traditional insurance policies do not provide network security or privacy data breach protections. Electronic data does not meet the definition of "property damage" found in a commercial general liability policy, and most insurers issuing these policies also have added an exclusion for electronic data. In addition, personal injury coverage found in commercial general liability policies have been found not to cover loss data, because the publication requirement is not met. The Connecticut Supreme Court in *Recall Total*

Information Mgmt., Inc. v. Federal Ins. Co. , affirmed the reasoning of the appellate court's decision that the loss of tapes containing IBM past and present employees' social security numbers, birthdates, and contact information did not fall within the scope of the definition of "personal injury," because the only showing was that the tapes were lost, not that the information on the tapes was published .

This does not mean that an insured should not tender a data loss claim to its general liability insurer, particularly when a publication of the data has occurred. In *Hartford Cas. Ins. Co. v. Corcino & Associates*, the insured's motion to dismiss the insurer's declaratory judgment action asserting that an exclusion that negated coverage for "advertising and personal injury" arising out of the violation of a person's right of privacy created by any state or federal act, did not negate an insurer's duty to defend under a commercial general liability policy a hospital that experienced the release of confidential, identifiable health care information about approximately 20,000 patients whose information was published by a third party on a website.

Insurance Is Available For Data Losses

While some insurers offer endorsements providing a form of network security or privacy protection, which is added to a commercial general liability policy or a separate coverage offered in a professional liability or other errors and omissions policy, the scope of coverage is unlikely to be as broad as the stand-alone policies now available in the marketplace.

Network security and privacy policies may offer more in their protections to the extent they offer some typical first party protection, such as covering certain costs a policyholder may experience as a result of a data breach, in addition to providing an insured third party coverage protection for claims brought against the insured for a data breach.

Network security coverage typically is implicated by the happening of an "event," often referred to as a "technology event," as defined by a policy. The privacy coverage generally concerns an unauthorized disclosure, access or wrongful collection of confidential information that does not involve technology –something other than electronic data – and does not require a publication of the data in order for coverage to exist. The court's conclusion in *Total Recall*likely would have been different with respect to the insured's loss of the tapes with PII if the insured had privacy coverage.

(Source: http://www.advisen.com/tools/fpnproc/fpns/articles_new_35/P/251426402.html)

Cyber Insurance For Data Breach: Being Prepared If The Black Hats Come Calling, Part II

By Max H. Stern and William S. Berman, Duane Morris

Abstract: This article, the second of two parts (read the first part), addresses the current business environment and the exposure companies, small and large, have to a potential data breach. Data is a resalable commodity, and traditional liability insurance generally provide businesses no or limited protection for the significant costs required to respond to a data breach. In response, an emerging market is developing of cyber insurance policies protecting network security and privacy. These policies offer both first and third party coverages, and business policyholders should seek to negotiate an insurance policy on the best terms to meet their needs.

First Party Loss and Third Party Liability Protection

The advent of cyber insurance products that combine both first party (network security) and third party protection (privacy) have been welcomed. Before these products were introduced, first party coverage for loss of business income and the value of destroyed data was becoming increasingly difficult to find at affordable prices. The influx of new products has been good news for policyholders with significant potential data and privacy exposures.

First party coverages insurers may offer in the event of a data loss include: (1) legal analysis of applicable reporting and notification laws; (2) forensic consultants to determine the nature, scope, extent, and cause of the breach; (3) public relations and crisis management consultants and services; (4) notification services to affected person(s) and entity(ies); (5) call center services; (6) credit or identify monitoring; and (7) funding for direct costs resulting from the security or privacy breach.

Third party coverages an insurer may offer in the event of a data loss include coverage for: (1) breach from unauthorized access; (2) infection of system from a virus or malicious code; (3) denial of service attack; (4) defense of third party lawsuit (including class actions) from affected person(s) and entity(ies); (5) defense of regulatory proceedings including payment of fines and penalties; and (6) costs to re-issue credit cards.

Insurers continue to refine their products based on developments in the marketplace and risks identified. One insurer may be willing to offer insurance

covering a particular risk that other insurers are not. That is why when considering the purchase of an insurance policy, it is important to know the risks sought to be insured, to make sure coverage is available for such risk, and that you purchase insurance with appropriate limits/sublimits.

The Terms of Your Cyber Coverage Matter

A hospital system located in Santa Barbara, California experienced a data breach that resulted in the release of approximately 32,000 confidential medical records after either the health care system or its medical records storage vendor failed to install encryption software and/or undertake other security measures to protect health care patient information stored on a system fully accessible from the Internet. The class action lawsuit filed against the health care system resulted in a $4.1 million settlement for the data breach. While the health care system had a $10 million per claim cyber breach insurance policy, which was subject to a $100,000 self-insured retention, the insurer denied coverage because of the insured's "failure to follow minimum required practices" with respect to its computing system. If the insurer prevails on its coverage defense, the health care system will be responsible for all of the $4.1 million settlement.

This matter illustrates the importance of making sure the company's processes are compliant with its insurer's requirements, such as an insurer's "minimum required practices" in order to receive the maximum insurance benefit available. Unless IT is aware of and ensures the insurer's "minimum required practices" are in place, premium dollars spent on a network security and privacy policy with a "minimum required practices" requirement will be wasted. Some companies are empowering one person or a group of individuals with the responsibility of securing and protecting data and to be involved in obtaining data and privacy-related insurance protection.

In another insurance dispute relating to data, a federal district court in Utah concluded an insurer was not obligated under its technology errors and omissions coverage to defend its insured against a lawsuit based on the insured's alleged failure to process members' accounts and transfer member fees to the company purchasing the business. While the insurer originally agreed to defend subject to a reservation of rights, the insurer prevailed in a declaratory judgment action in convincing the district court that there is a difference between an insured withholding data because of an error, omission or negligent act and, on the other hand, knowingly withholding data and refusing to turn it over until certain demands are met.

Coverage Beyond Data Breaches

Today, many insurance products offer various forms of protection against data-related breaches. Policies often include coverage for more than computer network intrusion data breaches, so that companies without significant data vulnerabilities still may benefit from securing appropriate protection for their business. For instance, consideration also should be given to whether a business would benefit from insurance protection for risks such as destruction of data, viruses, cyber extortion, loss of (or access to) laptops with confidential or private information, the loss of physical records containing sensitive information and distribution of identifiable information sent to the wrong recipient. Other coverages often available include protection against claims of libel, slander, product disparagement and defamation.

These are risks not generally insured by many commercial general liability and/or professional liability policies, and – even if such coverage is offered by those policies – companies should carefully analyze whether the insurance adequately protects its business both in terms of the nature of the risks covered and at sufficient limits/sub-limits.

At a minimum, companies' in-house or outside counsel, risk managers, privacy officers and/or insurance brokers should assess whether a company may benefit from adding a network security and privacy insurance policy to its insurance portfolio or whether it has sufficient and appropriate insurance protection. Even if a company has an insurance policy protecting against data loss and privacy issues, if a company identifies a new potential risk, contact your insurance broker or insurance company about modifying your current insurance policy to meet your current needs.

What Businesses Can Do To Protect Against The Risk of Data Breach

There is no lockbox to protect against a data breach, particularly when 25% of all breaches are a result of human error. Slightly less than half of all data breaches are a result of criminal or malicious attack (47%), with 29% of such breaches attributable to a system glitch involving IT and business processes failures.

Businesses collecting, handling or storing confidential identifiable information should consider being proactive in protecting their data and taking all reasonable preventive steps to guard against a data breach. These may include:

- Developing and implementing stringent network and data securities policies based on risks particular to business;
- Appointing personnel responsible for data protection;
- Requiring third-parties you contract with to abide by and implement stringent network and data security policies;
- Ongoing review, assessments and updating of network and data security policies; and
- Conducting a data breach risk assessment and obtaining insurance protection that should respond in case there is a data breach from known risks.

Also, one of the most often overlooked potential liability issues is whether your insurance will protect you from acts or omissions of your business partners or a breach from a business partner.

For instance, a recent report suggests that the initial access into Target Corp.'s computer network was through malware installed on a Target contractor's computer system which enabled the thieves to use the heating and air conditioning contractor's user credentials to access Target's network. In another alleged breach event, it was recently reported that the payment processor YapStore, which handles payment for the short-term rental website VRBO, reportedly experienced a data breach.

Those who rely on business partners to handle, process or store PII, PHI, or PCI should not only ensure that its insurance provides coverage for such risk, but also should seek to allocate risk in its contracts and service agreements with its business partners and ensure that your business partners are following the required levels of privacy and securities policies.

If a decision is made to investigate potential insurance options, among the things to consider are:

- Identify key coverages that align with your potential risks and exposures;
- Assess whether proposed exclusions pose issues given the nature of the risks and exposures;
- Determine the financial risk the company is willing to assume, to seek insurance limits/sub-limits that provide the desired level of protection;
- Assess whether insurance on "occurrence" or "claims-made-and-reported" policy basis is right for you;
- If business is an ongoing concern, you may want to ask for a policy retroactive date/anniversary date as early as possible (well before the

policy's inception date) so that the insurance may apply to pre-inception unknown breach; and

- If you have agreed to indemnify others in the event of a data breach, discuss with your broker the need to have your indemnity obligation be exempted from contractual liability exclusions and to satisfy your policy's deductible or self-insured retention.

- Data security and assurance that our businesses have appropriate insurance to address the risk of a data breach requires vigilance. Helping clients through these issues should help avoid the risks that could potentially cause significant, unexpected financial hardship, reputational harm or even threaten the viability of the business.

About the authors: *Max H. Stern is a head of the Insurance Division of the Duane Morris Trial Practice Group and a partner at Duane Morris LLP, who is a resident of its San Francisco office.*

William S. Berman is Special Counsel at Duane Morris LLP, who provides advice and counsel on insurance-related issues, and is a resident of its San Francisco office.

(Source: http://www.advisen.com/tools/fpnproc/fpns/articles_new_35/P/251733946.html)