GOLDMAN JUDIN INC.
ATTORNEYS
Reg No. 1998/011/368/21

Wanders Office Park
Pavilion Building Second Floor
52 Corlette Drive
Illova

PO Box 78662 Sandton 2146
Docex 264 Randburg

e-mail: law@elawnet.co.za
website : www.gji.co.za
tel : (+27 11) 595 2300

Cyber Risk Insurance and Cyberattacks

14 August 2013 - In his excellent article leading US attorney Jose Umbert, under the rubric New Trends To Watch In Cyber Risk Insurance, writes as follows:

"Although specific cyber risk insurance policies are becoming increasingly common, claims related to data breaches continue to be submitted under commercial general liability policies. Some recent decisions addressing these claims provide helpful guidance for practitioners in this area.

It is well known that over the last few years, there has been a significant increase of data breaches, that is, incidents compromising the security of data stored electronically by an organization. This has been accompanied by the development and growth of specialty cyber insurance products specifically designed to address these, and other, cyber-related risks confronting businesses today.

Notwithstanding the expansion of cyber risk insurance, policyholders continue to submit claims arising out of data breaches under their traditional CGL policies. This is due to a variety of reasons, including that the agreed-upon limits of liability under the insured's cyber risk policy turn out to be insufficient to cover the losses resulting from the data breach; an exclusion or other provision precludes or limits coverage for the particular claim; or the company simply did not purchase cyber liability coverage.

Therefore, CGL policies continue to play a significant role in ascertaining the scope of coverage available for third-party claims arising out of data breaches. Indeed, some recent, high-profile coverage disputes in this area have involved claims brought by large corporate policyholders seeking coverage under the "personal and advertising injury" provisions of their CGL policies for the class action and other claims brought against them after computer hackers stole their customers' personal information.

In analyzing the legal issues involved in these types of claims, several recent court decisions involving claims brought under a CGL policy for the insured's alleged liability for the loss or misappropriation of the claimant's electronic data may be relevant to practitioners as this is often the basis of at least some of the claims asserted against companies affected by a data breach.

A critical issue in these cases is whether the third-party claims against the insured involve physical injury to, or loss of use of, "tangible property" so as to trigger coverage under the "property damage" section of the CGL policy. Several recent decisions have concluded that electronic data,

such as a third party's customers' email addresses, employees' personal information and even electronic funds in a bank account, do not constitute tangible property and therefore fall outside the scope of this coverage grant.[1] Some of the CGL policies at issue in these decisions expressly excluded electronic data from the definition of "property damage."

However, in contrast, another court held that where the loss alleged in the underlying lawsuit involves the medium on which data was stored (in that case, a CD-ROM containing third parties' personal information), there is a potentially covered claim for "property damage" under a CGL policy.[2]

It should be noted that even if the coverage for "property damage" is potentially triggered, other provisions in the policy may apply to limit or preclude coverage. Indeed, in this same case, the Seventh Circuit affirmed summary judgment for the insurer on the ground that the exclusion for property "in care of" the insured applied to the insured's loss of the CD-ROM, thus barring any recovery under the insured's CGL policy.[3]

Policyholders may also seek coverage for data-breach losses under the "personal or advertising injury" coverage parts of standard CGL policies. With respect to a claim against an insured for loss or disclosure of third parties' personal information, the relevant insuring clause is the coverage grant for alleged injuries arising out of the "publication of material that violates a person's right of privacy."

Coverage for such claims may depend on the interpretation given to the term "publication" in the relevant jurisdiction. As recent decisions show, in some states, a "publication" requires dissemination of the personal information to the general public,[4] and in others, there must be a communication to a third party.[5]

Other courts, however, have taken a more expansive view of the term "publication." The choice-of-law issue may thus be outcome-determinative in these types of claims.

Case law involving liability insurance coverage for claims arising out of electronic data breaches continues to develop. The decisions mentioned in this article signal some important issues and trends, which practitioners in this area need to consider when analyzing these types of claims.

[1] See Liberty Corporate Capital Ltd. v. Security Safe Outlet Inc. (E.D. Ky. Mar. 27, 2013); Recall Total Info. Mgmt., Inc. v. Federal Ins. Co. (Conn. Super. Ct. Jan. 17, 2012); Carlon Co. v. Delaget, LLC (W.D. Wis. May 21, 2012).

[2] Nationwide Ins. Co. v. Hentz (S.D. Ill. Mar. 6, 2012).

[3] Nationwide Ins. Co. v. Central Laborers' Pension Fund, 704 F.3d 522, 525-26 (7th Cir. 2013).

[4] Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co., 444 Fed.Appx. 370, 375-76 (11th Cir. 2011) (applying Florida law).

[5] Recall Total, 2012 WL 469988 at *6-7"

In an equally excellent article, and again by a leading US attorney, namely, Vincent Morgan, he writes, under the rubric Help Clients Insure Against Cyberattacks:

The constant threat of cyberattacks presents many and varying challenges for businesses. Insurance provides one way to deal with them. Because the market for insurance covering these risks and the law interpreting these policies both continue to develop, this is an area in which attorneys can help clients by maximizing their opportunity to secure the broadest possible coverage.

A look at federal and state action on cybersecurity risks provides some critical background. President Obama issued his Executive Order on Improving Critical Infrastructure Cybersecurity in February. In October 2011, the U.S. Securities and Exchange Commissions Division on Corporate Finance issued relevant guidance on financial-disclosure obligations concerning cybersecurity issues in CF Disclosure Guidance Topic No. 2 - Cybersecurity.

Texas law also imposes some key legal requirements on businesses. Texas Business & Commerce Code Chapter 521 imposes duties on companies to protect sensitive personal information collected or maintained in a company's regular course of business and to notify affected individuals if the security of a computerized system containing that data is breached.

A look at cyberattackers also provides important perspective. Wrongdoers can target a company's trade secrets or product-development pipeline for competitive, nationalistic or societal reasons. In addition, certain industries with a strong presence in Texas, such as energy, petrochemicals, transportation and technology, face particularly frequent attacks due to their unique characteristics and vulnerabilities.

When prevention efforts are insufficient, a data security breach often imposes first-party losses in the form of response costs and impacts on the company's revenue stream. These can include expenses for detecting, investigating and eliminating the intrusion, notifying those affected by it, managing the company's reputation and dealing with revenue impacts from damaged customer relationships. Third-party claims also can result, in the form of lawsuits and regulatory actions.

Because these issues touch on so many aspects of a company's business, from negotiating vendor agreements to compliance to litigation, lawyers have many opportunities to help clients address these risks. Insurance coverage provides one such opportunity.

A company's traditional insurance policies may offer at least some protection. In Retail Ventures Inc. v. National Union Fire Insurance Co. of Pittsburgh, PA (2012), the 6th U.S. Circuit Court of Appeals held that a "computer fraud" endorsement to a crime insurance policy covered more than $5 million in losses arising out of the illicit access to customer accounts stored in a retailer's database. These losses included expenses for customer communications, public relations, customer claims, and investigations by multiple states and the Federal Trade Commission, as well as chargebacks, card reissuance costs, account monitoring and fines imposed by the credit card issuers.

The insurance industry's offerings for specific cybersecurity policies also have grown rapidly in response to this threat. Just going through the process of applying for cyberinsurance can improve a company's risk awareness. Large insurance brokers often use illuminating self-assessment questionnaires that pose dozens of queries on topics such as background checks, employee and contractor training, network security protocols, prior incidents and crisis-management procedures.

Attorneys will need to guide clients through varying policy options. Current cyberinsurance offerings lack the standardization that develops after court challenges refine policy language and the marketplace comes to accept that language.

Given the lack of industry-wide agreement on policy language, an "off the shelf" policy may be ill-suited to a particular business. Because the market is still developing, lawyers can have a greater impact in negotiating more favorable terms for a specific client's unique needs. The policy should cover both first-party and third-party losses, as a cyberattack often triggers both.

Here is a list of some other issues to consider when purchasing a cyberinsurance policy:

A simulated cyberattack can create an opportunity for detailed analysis. Several publicly available sources track costs associated with data security breaches. Because of the wide-ranging impacts a cyberattack can have, the total costs of these incidents are often significantly higher than the largest individual component. On the other hand, some aspects of a cyberattack may be relatively minor for a particular company.Gaining a thorough understanding of the company's risk profile through a simulated cyberattack will help guide decisions on issues such as the amount of overall limits, particular sublimits and deductibles.

Does the policy cover acts of third parties with access? If the company provides confidential data to third parties or allows vendors access to its secure systems, the policy should offer coverage for that exposure. Recent headlines involving rogue employees at third-party contractors demonstrate the importance of closing off this potential gap.

Seek coverage for unknown breaches that may have occurred already. A recent fraud summit revealed that early detection of cyberattacks remains a significant challenge. Accordingly, policyholders should seek retroactive coverage to protect against intrusions that began prior to the policy but only caused losses during the policy period.

Broad exclusions can have unintended consequences. Suppose a cyberattack leads to an environmental liability. Is there a pollution exclusion geared towards more traditional risks that would preclude coverage for the cyberattack? Counsel should address these issues and narrow relevant exclusions, if possible.

The right to choose counsel is critical. Choice-of-counsel provisions may matter here more than other areas. A company's comprehensive cybersecurity plan may already have designated counsel as part of a crisis-response team.

This is something a business typically can negotiate with the insurer before a loss occurs. Left unaddressed, a company may find itself arguing about selection of counsel at a time when it most needs the help of trusted lawyers who know the company well.

For companies involved in significant technology outsourcing arrangements, it is important to examine vendor agreements for cybersecurity issues, as well as for insurance and indemnity provisions that a cyberattack involving the vendor may trigger. That analysis may suggest needed modifications to these agreements for more robust protections.

Managing cyberattacks may be a more achievable goal than preventing them. Fortunately, paying close attention to insurance issues is one way lawyers can help companies with that effort.

South African entities must wake up to the looming danger of cyberattacks and the importance of cyber risk insurance. It is hoped that the above article will assist.

Prepared by J. Michael Judin of Goldman Judin Inc.

Michael may be contacted on

+27 (0) 83 300 5000 or at michael@elawnet.co.za