Emerging Trends

Negotiating the New World of Cyber Insurance

March 2012

Q&A

Rene L. Siemens
Litigation
+1.213.488.7277
reynold.siemens@pillsburylaw.com

Mr. Siemens is a nationally recognized insurance coverage practitioner who represents policyholders in negotiations and disputes with their insurers. He also handles complex litigation matters including product liability, mass tort, environmental, and consumer litigation.

Businesses today have complex, carefully designed insurance plans to protect against physical property loss, environmental damage, defective products and other risks. Much of a company's value, though, is now tied up in its data and network systems. The growing importance and vulnerability of these IT assets is driving the popularity of a new type of insurance protection, "cyber insurance," which is specifically designed to cover many almost-inevitable data breach scenarios. While more and more companies are buying cyber insurance to mitigate their potential losses, selecting the right policy requires planning and negotiation.

In this *Emerging Trends Q&A*, Pillsbury Insurance Recovery & Advisory partner Rene L. Siemens addresses this new insurance product class. Siemens, who has helped clients recover more than $1 billion from insurers during his career, explains why the cyber insurance market is growing, what businesses should consider when studying coverage and emerging legal and regulatory issues to watch in this space.

Q: Cyber insurance is a relatively new addition to the roster of insurance policies many providers offer. Why has it emerged on the scene?

Siemens: The need for cyber security insurance has become apparent because of the constantly increasing number of successful and attempted cyber attacks and because legislators and regulators have imposed onerous new requirements on companies to protect their data and networks.

As everyone knows from the headline news, it is getting harder every day for companies to protect their data and networks from theft and data hacking, and in the current regulatory environment the stakes for even inadvertent disclosure of private data are high. Customer names, credit card information, social security numbers, passwords, employee information, and confidential commercial information and intellectual property are all at risk in a data breach. Loss or unauthorized disclosure of this data can mean lost revenue and public trust, not to mention the costs of remediating the breach or fending off lawsuits by the affected parties. An interruption in the flow of data or a disruption of one's network as a result of a breach can also bring business to a complete halt. An increasing number of companies view the need for insurance to mitigate these risks as crucial. As companies become more reliant on sophisticated networks and data flow, and have to rely more and more on third-party vendors to handle their sensitive information, the importance of cyber insurance only grows.

Over the past 15 years, data privacy statutes and regulations have also proliferated. For example, the 1996 Health Insurance Portability and Accountability Act (HIPPA) and 1999 Gramm-Leach-Bliley Act (GLBA) require healthcare providers and financial institutions to institute measures to protect the privacy of customer information. Most recently, in October, 2011, the SEC issued guidance "recommending" that public companies disclose hacking incidents and threats in the "material developments" section of their regulatory filings, as well as whether they have insurance for such losses. This new guidance is expected to further increase the demand for cyber insurance.

Q: What kinds of companies purchase cyber insurance?

Siemens: Although all companies face cyber security and data breach threats, some companies are certainly more likely to be hacked than others—and these entities are the most likely to have purchased cyber insurance policies or to be actively considering whether to buy them.

Companies in the financial services, health care, retail and hospitality, communications, media and technology sectors have tended to be early adopters of cyber insurance, for the obvious reason that they possess large amounts of private customer data and are attractive targets for data thieves. In addition, a company that manufactures or sells an extremely popular consumer product may be more likely to face hacking attempts. The same is true for companies whose leadership is high-profile, or especially outspoken on controversial issues. Big companies tended to buy cyber insurance first, but much of the growth in the cyber insurance market lately has come from smaller and middle-market companies as they come to realize the magnitude of their exposure to data security risks.

Q: What is included in cyber insurance? What should companies look for?

Siemens: There are two main types of cyber insurance—third-party and first-party.

Third-party cyber insurance is most common, and covers losses from data security breaches, other loss or unauthorized disclosure of private information, as well as the discovery of libelous or copyright-infringing content on a business' site. While no two policies are exactly the same, this kind of coverage often falls into three categories:

1. Crisis management expenses, including costs of notifying affected parties that their data has been compromised, costs of providing credit monitoring services, and the costs of public relations consultants, forensic investigation, and pursuit of indemnity rights against third parties who might be responsible for the breach;
2. Claim expenses, such as the costs of defending and settling lawsuits; and
3. Regulatory response costs, which can include compliance, investigatory and settlement costs.

First-party cyber insurance covers the cost of restoring or recollecting lost or damaged data, revenue loss caused by interruptions to data flow or network systems, and "e-vandalism" and "e-extortion."

Q: What are the top issues of legal contention within cyber insurance? Are companies actually receiving payouts?

Siemens: Because cyber insurance is a relatively new type of coverage, there aren't really reliable, publicly-available statistics on claims filings and payouts, at least not yet. I do know from personal experience, however, that claims are getting paid, and my sense is that because insurance companies are trying to build market share they are sensitive about how they will be perceived if word gets around that they are denying claims.

As with any type of insurance, of course, disputes arise between claims providers and policy holders. Areas of potential friction include adequacy of limits and size of retentions, whether the policies have retroactive coverage — that is, coverage for breaches that occurred without the policyholder's knowledge before the policy was issued — consent and panel provisions, and coverage for vendors' errors and omissions. There are many other dispute factors. For example, the issue of whether data was "lost" as opposed to being "stolen" can determine whether a claim is accepted — some policies only make provision for one or the other.

To avoid disputes, companies should proactively consider the specific type of coverage they need, and negotiate the adequate language to ensure this coverage. Unlike some other lines of insurance, there are no "standard" cyber liability policy forms. Each insurer has its own policy form, and those forms are usually highly negotiable. Because of the lack of standardization, cyber liability policies can contain surprisingly narrow insuring clauses and broad exclusions, so it's important to negotiate what you need for the scenarios your company could someday face.

Q: What should companies look for when negotiating cyber insurance?

Siemens: Businesses need to strike a balance between accepting a "one size fits all" policy that may be too broad or restrictive for the data and security breach threats they face daily—and, equally ill-advised, orchestrating a plan so specific that it results in making it harder to get coverage or more expensive than truly necessary.

Because the cyber insurance market is highly competitive right now, our clients have been able to negotiate significant coverage enhancements with their insurers, often for no additional premium.

Q: What can companies overlook when drafting their coverage requirements?

Siemens: There are literally dozens of issues I look for when a client asks me to review a cyber policy that it's considering. One of the most basic questions is whether the policy limits and sub-limits are adequate. For example, many policies try to cap the insurer's liability for the costs of responding to regulatory investigation by imposing inadequate sub-limits on that part of the coverage. Similarly, many policies impose inadequate limits on covered "crisis management" expenses. Skimping in these areas or assuming that the insurer has your best interests at heart when it makes these decisions may cost you in the long run.

Q: What are the developments to watch in the field of cyber security insurance?

Siemens: The importance of cyber insurance to the business community will grow and policies will become much more common. Right now the cyber insurance market is a bit like the "Wild West," but over time the cast of insurers offering this product will probably stabilize and a higher degree of standardization can be expected.

There's no doubt that the most notable development in the United States very recently has been the SEC's disclosure guidance, which indicates that regulators will continue to watch how public companies in particular invest in their data protection.

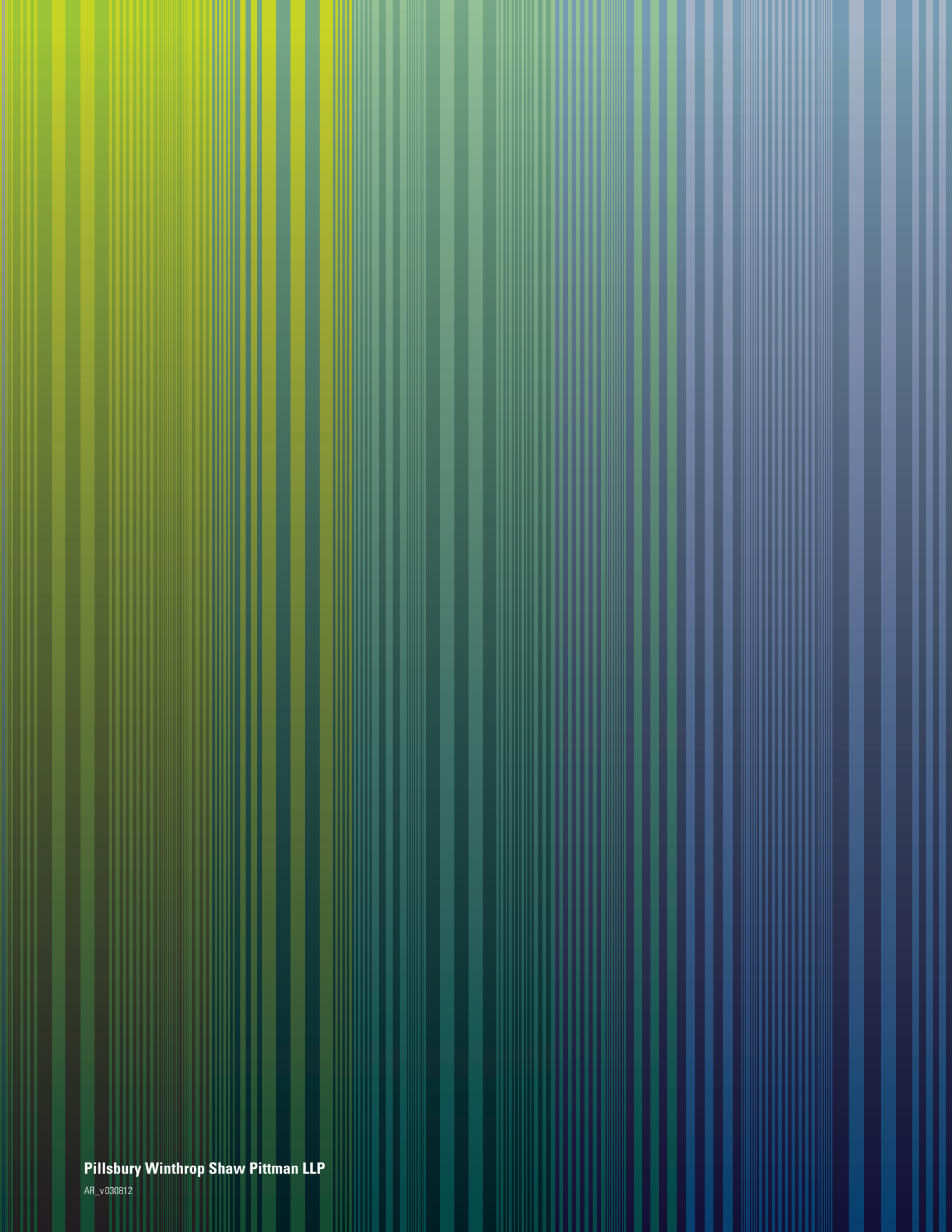
Emerging Trends *is a regular feature from Pillsbury, highlighting key issues impacting the energy, financial services, technology and real estate sectors and other industries today.*

Pillsbury's internationally recognized Insurance Recovery & Advisory practice vigorously advocates for policyholders in coverage negotiations and disputes with their insurers, helping policyholder clients recover billions of dollars from their insurance carriers. Pillsbury's insurance recovery lawyers represent corporate and institutional policyholders in every major industry—from airlines to energy companies.

Pillsbury's Privacy, Data Security & Information Use lawyers work with domestic and multinational companies to address privacy requirements, needs and issues in a way that balances thorough compliance with the flexibility to conduct and expand their businesses. In addition to addressing privacy requirements, the team works with clients on privacy issues related to data security breach preparedness and response. The Privacy, Data Security & Information Use team also provides legal advice associated with information disclosure and discovery orders in litigation proceedings and government/regulatory investigations.

For more information on cyber insurance and regulatory or legal issues around privacy and data security in general, please contact Tom Resau, Senior PR Manager, at 202-663-8236 or tom.resau@pillsburylaw.com.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | 1.877.323.4171



Pillsbury Winthrop Shaw Pittman LLP

AR_v030812