LEGAL EXPERT CONNECTIONS, INC.

1-866-417-7025
www.LegalExpertConnections.com
www.InsuranceDefenseMarketing.com
MG@LegalExpertConnections.com

Legal Marketing Strategies

Cybersecurity Draws Attention in Insurance Defense Market

By Margaret Grisdela

Highlights of this Article

- Insurance defense panel counsel opportunities will expand in cybersecurity
- Insurance companies and law firms are launching new cybersecurity services
- Legal counsel can get in on ground floor by being named in an insured's policy
- Legal fees and investigations can run millions of dollars for a single breach

Cybersecurity Draws Attention in Insurance Defense Market

A Cybersecurity Council led by the Department of Homeland Security is a central element of a national data security plan under consideration by the White House, according to a recent Washington Post article titled "White House drafting standards to guard U.S. against cyberattack, officials say."

A uniform set of national cyber security standards may result if an interagency government council evolves to the point of establishing minimum guidelines. The goal would be to protect against data breaches in the nation's network for communications and major utilities.

Insurance coverage for cybersecurity policies may potentially benefit from national standards, suggests the reporter, by contributing to a framework for insurance policy provisions.

Consideration of national cybersecurity policies follows the SEC's October 13, 2011 release of the "CF Disclosure Guidance: Topic No. 2" relating to cyber-security risks. "Registrants should address cybersecurity risks and cyber incidents in their MD&A if … costs … represent a material event, trend, or uncertainty …," according to the SEC.

Also of interest is an undated paper titled "Cyber-Insurance Metrics and Impact on Cyber-Security" available on the White House website.

A Definition of Cybersecurity

You might be asking, what exactly is cybersecurity? According to the Congressional Research Service:

> *Cybersecurity might best be described as measures intended to protect information systems—including technology (such as devices, networks, and software), information, and associated personnel—from various forms of attack.*

Putting this in context, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23) defines "cyberspace" as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.

A White House a report titled the Cyberspace Policy Review references the following as key elements of U.S. cyber structure:

- Broadband networks and wireless signals
- Local networks in schools, hospitals, and businesses
- National, regional, and local energy grids
- Transportation systems
- Classified military and intelligence networks
- Proprietary business information
- E-commerce
- Global financial services
- Intellectual property

Cyber incidents can result from malicious activity, accident, or natural disaster.

Insurance Companies Continue to Launch Cybersecurity Insurance

NAS Insurance Services, Inc. recently announced the availability of BrandGuard™ insurance coverage that pays companies for lost revenue in the event of a cyber breach. The expanded cyber liability insurance is designed to provide organizations with an extra layer of financial support while they work to restore their customers' trust following a data security breach.

NAS policies will provide protection for privacy-related data breaches and recovery efforts, including the cost of legal support, IT forensics, public relations, customer notification, credit monitoring, identity restoration, and compensation for lost income.

Chubb, Chartis, and Philadelphia Insurance Companies are a few of the leading insurance companies offering cybersecurity coverage.

Insurance Defense Law Firm Opportunities with Insureds and Self-Insureds

While data security is increasingly recognized as a major risk factor in our world of "big data," many companies are not yet seeking insurance coverage.

According to the 2012 Risk and Finance Manager Survey conducted by Towers Watson and released in April 2012,

> *Nearly three in four respondents (72%) are not purchasing a network security/privacy liability policy, virtually unchanged from last year. And those that did purchase policies (28%) opted for limits that were on the low end of the spectrum. In fact, 43% said their policies had a $1 million to $5 million limit. When asked why they had not purchased a policy, 41% believe their own internal IT department and controls are adequate, while 25% indicated they do not believe they have a significant data exposure.*

The Wall Street Journal CIO Blog covered the topic of data security in a May 29, 2012 article titled, "As Flame Spreads, Most Companies Lack Cybersecurity Coverage."

Insurance defense law firms are presented with a ground-floor opportunity to work with insureds and self-insureds in regard to cyber security protection. As companies do acquire cybersecurity insurance coverage, law firms that can successfully have their name specified in the insurance policy as a preferred legal provider (sometimes known as an "accommodation") stand a better chance of being able to represent clients if and when litigation does arise. While being named in the policy is not equivalent to being approved as insurance panel counsel, it certainly puts the law firm in a stronger position to represent their own clients.

Additionally, law firms can develop deep industry-specific expertise within cybersecurity. Data dependency is present in many market sectors, including banking, health care (as evidenced by HIPPA), e-commerce, telecommunications, transportation, and retail.

Many law firms have already established data security capabilities, or are doing so now. Jenner & Block, for example, recently announced their new Privacy and Information Governance Practice under the direction of former United States Department of Homeland Security (DHS) Chief Privacy Officer Mary Ellen Callahan.

Cybersecurity Case Study: Heartland Payment Systems

Heartland Payment Systems, Inc., one of the nation's largest payments processors, publicly announced the discovery of a "Processing System Intrusion" on January 20, 2009. According to the company's 10K for the fiscal year ended 12/31/11, the Intrusion prompted regulatory investigations by:

- Federal Financial Institutions Examination Council
- Federal Trade Commission
- Louisiana Department of Justice
- Canadian Privacy Commission
- Other government agencies

Since its disclosure of the Intrusion on January 20, 2009 and through December 31, 2011, Heartland has expensed a total of $147.1 million, before reducing those charges by $31.2 million of total insurance recoveries. The majority of the total charges, or approximately $114.7 million, related to settlements of claims. Of particular interest to law firms,

Approximately $32.4 million of the total charges were for legal fees and costs incurred for investigations, defending various claims and actions, remedial actions and crisis management services.

Summary

Cybersecurity and cyber-insurance appear to represent a significant growth opportunity for insurance defense law firms. Opportunities arise both as insurance panel counsel for insurance companies and trusted legal advisors to insureds or self-insureds. Marketing Committee members within insurance defense law firms may find cybersecurity to be fertile territory for business development once the learning curve of a new practice group can be achieved.

Other Resources

Federal Communications Commission
Tech Topic 20: Cyber Security and Communications
http://transition.fcc.gov/pshs/techtopics/techtopics20.html

National Security Council Cybersecurity Overview
http://www.whitehouse.gov/cybersecurity

Congressional Research Service
"Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions," by Eric A. Fischer, June 29, 2012. See: http://www.fas.org/sgp/crs/natsec/R42114.pdf

FBI Cyber Crime Initiatives
http://www.fbi.gov/about-us/investigate/cyber/cyber

Securities and Exchange Commission (SEC) Guidance on Cybersecurity Risks and Disclosures
http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

"**White House Planning Executive Order on Cyber Security**," by Joseph Menn, Reuters, 9/25/12.
http://www.claimsjournal.com/news/national/2012/09/25/214151.htm

Legal Marketing Strategies

Courtesy of Legal Expert Connections, Inc.

About the Author: Insurance defense marketing consultant Margaret Grisdela is president of Legal Expert Connections, Inc. and the author of *Courting Your Clients: the Essential Guide to Legal Marketing*. She can be reached at mg@legalexpertconnections.com. More details at www.InsuranceDefenseMarketing.com.

Legal Expert Connections is a national legal marketing agency focused on business development for attorneys and experts. Our services include insurance defense marketing, outsourced legal marketing management, law firm brochures, and more.

Legal Expert Connections, Inc.
2385 NW Executive Center Drive, Suite 100
Boca Raton, FL 33431
1-866-417-7025
www.LegalExpertConnections.com
www.InsuranceDefenseMarketing.com
www.LawFirmBrochures.com

Remember, never stop marketing! The author invites your questions and comments.