

Business Insurance

\$100

March 19, 2012

www.businessinsurance.com

SPECIAL ISSUE

CYBER RISKS

**UNDERSTAND
THE THREATS**

**MAXIMIZE
YOUR PROTECTION**

crain

Entire contents copyright © 2012 by Crain Communications Inc. All rights reserved.

NEWSPAPER

DATA POSTER INSIDE

**Featuring detailed information on
cyber insurance purchasing trends**

Business Insurance

Online features & highlights
www.businessinsurance.com



NEW BENEFITS ARC: With health plan costs far outpacing inflation, employers are looking for new ways to fund their health care benefit programs. www.BusinessInsurance.com/solutionarcs

LAST WEEK'S TOP FEATURES www.BusinessInsurance.com/BItop10	
1.	Brokers hopeful they have role in health insurance exchanges
2.	Insurance wholesaler AmWINS up for sale: Sources
3.	GALLERY: The Disaster in Japan—A Year of Recovery
4.	Solution Arc: Alternative Financing Strategies for Health Care Benefits
5.	Commercial insurance pricing rises 4th consecutive quarter
6.	Exchanges need to notify employers about worker subsidies
7.	Sandusky wants Second Mile insurer to cover defense costs
8.	Solution Arc: Emerging Market Strategies: Expanding Into Brazil
9.	N.Y. medical treatment guides add to workers comp costs
10.	In FOCUS video: Current trends in D&O liability insurance
GET ONLINE NEWS EACH DAY Subscribe to BI's daily newsletter	



DATA BREACHES: Learn how to limit damages if and when a data breach occurs with a live webinar on March 20. www.BusinessInsurance.com/webinars



CAREER CENTER: Sign up for BI's Career Center for a successful search. www.BusinessInsurance.com/careers



CARTOON GALLERY: View a collection of cartoons by Roger Schillerstrom. www.BusinessInsurance.com/cartoons



LEARN: Benefits of taking a hands-on approach to comp TPAs. www.BusinessInsurance.com/whitepapers

Business Insurance (ISSN 0007-6864) Vol. 46, No. 12, is published weekly, except for combined issues the first and second week of July, the fourth and fifth week of August and no issue the last week of December, by Crain Communications Inc., 150 N. Michigan Ave., Chicago, Ill. 60601-7524. Periodicals postage is paid at Chicago and at additional mailing offices. POSTMASTER: Email address change to customerservice@businessinsurance.com or mail to Business Insurance Circulation Department, 1155 Gratiot Ave. Detroit, Mich. 48207-2912. \$5 a copy and \$125 a year in the U.S. \$130 in Canada and Mexico (includes GST). All other countries, \$230 a year (includes expedited air delivery). Canadian Post International Publications Mail Product (Canadian Distribution) Sales Agreement No. 40012850, GST No. 136760444, Canadian return address: 4960-2 Walker Road, Windsor, ON N9A6J3. Printed in U.S.A. Copyright © 2012 by Crain Communications Inc.

Aon Risk Solutions

Continuity in the midst of change

It doesn't always happen like it should. The unexpected happens, but you have to keep pushing forward, regardless of circumstances and environment.

Aon's insights, solutions and expertise empower you to keep your organization sustainable now and in the future.

aon.com/empowerresults



Risk. Reinsurance. Human Resources. Empower Results™



CYBER RISKS

Strategies to manage the evolving threats to every business

Risk managers and insurers alike are rising to meet the unique and formidable challenges posed by cyber risks.

Areas of concern range from the exposures arising from stolen or lost mobile devices to the potentially much more devastating problems presented by cloud computing, where thousands, if not millions, of personally identifiable information records could be vulnerable to hackers.

Meanwhile, only about one-quarter of firms buy stand-alone cyber coverage, according to a *Business Insurance* survey, although many say they self-insure for cyber risks.

Among those who do not have stand-alone cyber insurance, there are other policies that can absorb some of the same exposures, including errors and omissions liability, comprehensive general liability and media liability. Each contains language that at least potentially picks up some cyber-related losses, although certain conditions must be met in each case for the policies to respond to a loss. But a single data breach could erode policy limits.

Furthermore, risk managers cannot necessarily rely on these traditional liability policies. Legal and insurance experts warn that insurers already have balked in at least some cases at providing coverage under noncyber policies and have sought declaratory judgments stating

they are not obligated to provide coverage. This trend could grow with the increasing availability of cyber coverage.

For those who seek specific cyber coverage, proper risk assessment is critical.

Organizations also need to present well-rounded risk management controls to insurers when seeking coverage. And those looking for cyber coverage should have little problem finding it—at least for many risks—because of abundant capacity and a competitive environment. Brokers are seeing available capacity of \$250 million to \$300 million, with rates based on risk exposure.

Meanwhile, as the business community gains a greater understanding of the extent to which they are exposed to cyber risks, some companies in high-risk industries are beginning to turn to captive financing for their cyber risk insurance programs.

Reinsurers and excess insurers are providing more than enough capacity for stand-alone cyber insurance products to meet the demand, although concerns over business interruption exposure and aggregated risk are growing. In addition, most cyber policies still do not provide sufficient coverage to restore a business' damaged reputation or devalued intellectual property, or to pay for security upgrades after an attack, among other coverage gaps.

SPECIAL ISSUE

CYBER RISKS

As data breach incidents and other attacks on companies' systems continue to grow, risk managers increasingly are involved in efforts to protect their organizations from the ever-changing cyber risk threat. Indeed, a collaborative approach to cyber security that brings together a variety of departments—from risk management, to information technology, to legal—is considered critical to such efforts.

In this special issue of *Business Insurance*, we provide insights into the strategies and practices that will help risk managers minimize their organizations' exposure to cyber liabilities and maximize their protection against financial loss from cyber risks. The issue includes a look at the evolution of cyber risks, views on how risk managers can best assess their own risks, as well as an examination of the role insurance plays in addressing cyber risks, whether through traditional policies or specialized cyber coverages.

In addition, our fold-out data poster features original *Business Insurance* research into the cyber risk awareness and insurance buying habits of hundreds of companies, as well as information on the frequency, severity and costs of data breach incidents.

INSIDE THIS ISSUE

DATA BI survey shows firms aware of cyber risks, but cyber coverage penetration is low. **PAGE 4**

THREATS From human error to cloud computing exposures, cyber threats keep evolving. **PAGE 4**

ASSESSMENT Including all stakeholders in assessing cyber threats is risk management necessity. **PAGE 6**

PERSPECTIVE Industrial cyber attacks generate wide-ranging concerns. **PAGE 9**

PERSPECTIVE Cyber risk coverages are available in existing policies. **PAGE 10**

COVERAGES Stand-alone cyber insurers offer higher limits at low rates. **PAGE 11**

REINSURANCE Reinsurers are starting to warm up to covering cyber exposures. **PAGE 13**

MARKETS The cyber liability insurance market is seeing rapid growth in capacity. **PAGE 25**

POLICIES A selection of liability policies provides coverage for data exposures. **PAGE 25**

COLLABORATION Risk managers and IT managers should communicate on cyber risks. **PAGE 26**

SECURE Risk managers don't need to be IT experts to offer valuable perspectives. **PAGE 28**

CAPTIVES Captives are seen as a viable alternative for insuring cyber risks. **PAGE 29**

INDEX

Ad Index **PAGE 27** / BI Classified **PAGE 26**

Business Resources **PAGE 26** / End Page **PAGE 30** /

News in Brief **PAGE 29** / Opinions **PAGE 8** /

Few firms buy coverage for cyber risks: Survey

By JUDY GREENWALD

Nearly three-quarters of companies don't buy stand-alone cyber insurance, though more than 40% of those companies report that they are self-insured for the risk, indicating awareness of the need for cyber risk mitigation, according to a survey by *Business Insurance*.

The survey found that only 25% of companies purchase stand-alone cyber risk insurance, while 71% do not, and 4% said they were not sure. Among those that do not purchase the coverage, though, 43% said it is because their company self-insures these exposures.

The survey, which was conducted by Signet Research Inc. for *Business Insurance* to evaluate organizations' cyber risk awareness and insurance buying habits, included responses from 344 company executives who either make or influence insurance purchasing decisions for their firms. A total of 72% of the respondents were in risk management positions.

Clearly, obtaining cyber insurance calls for a coordinated effort. Of those that do purchase the stand-alone coverage, 93% of the time the respondent consulted first with the IT department. That proportion increases to 100% for all companies with at least \$100 mil-

lion in annual revenues.

Other internal parties consulted included the legal department, cited by 61%; the chief financial officer, cited by 52%; the CEO, cited by 23%; and "other," which was cited by 11%. Just 1% of respondents do not consult with any other internal parties.

Asked when they first bought stand-alone cyber coverage, 27% buying the coverage cited 2010, including 40% of companies with less than \$5 million in revenues, 38% of those with \$100 million to \$1 billion in revenues, and 33% of those with at least \$10 billion in revenues. According to the San Diego-based Privacy Rights Clearinghouse, data breaches involving personal data reached a peak of 604 that year.

Among those who purchase the coverage, liability and legal expenses for damages to another party because of personal information data being released was far and away the most important coverage provided in a cyber risk policy. Such coverage was cited by 85% of respondents, including 100% of those in the less than \$5 million in annual revenue category, and 92% of those in the \$500 million to \$1 billion revenue category.

This was followed by coverage for the cost of crisis management,

notification and credit monitoring after a data breach, cited by 72% overall; coverage for regulatory fines and penalties, cited by 37%; coverage for the value of data loss, cited by 24%; and coverage for the loss of revenue due to data loss, which was cited by 23%.

The most popular coverage layer was \$5 million up to \$10 million, which was reported by 48% of the respondents who purchase cyber liability coverage. However, company revenues apparently played a role in the coverage purchased. For instance, 80% of the purchases in the \$1 billion to \$5 billion revenue range bought this layer, while 63% of companies in the \$5 billion to \$10 billion range bought at the higher \$10 million to \$25 million layer.

Larger companies have had more claims, according to the *BI* survey. A total of 38% of companies with \$10 billion or more in annual revenues had filed a claim within the past three years, compared with just 11% for all companies. No claims were reported by companies with less than \$100 million in revenues, which is perhaps an indication that smaller firms have not to date been likely targets for nefarious activity.

While 43% overall said they self-insure this exposure, that strategy

WHY COMPANIES DO NOT BUY CYBER COVERAGE

Reasons for not purchasing stand-alone cyber risk insurance



was most popular among firms in the \$5 billion to less than \$10 billion category, accounting for 68% of the total. The percentage drops to 46% for larger firms.

In addition to those who cited self-insurance as the reason for not buying cyber coverage, 18% said it was because they believe cyber risk exposures are covered under other liability policies; 17% said their IT department does not think the coverage is needed; and 16% said the coverage is too expensive.

Both purchasers and nonpurchasers were asked which cyber-related activities their organizations engage in.

Working with business partners and contractors that touch customer data, which ranked the highest, was cited by 47% of the respondents. This was followed by

the use of social media, including Facebook and Twitter, for marketing and communications, which was cited by 45%; credit card data collection and online payment processing, cited by 36%; providing online content or media, cited by 34%; and e-commerce business websites, 31%.

Among both purchasers and nonpurchasers, 55% of respondents cited operational information technology risks, including data loss, as the biggest cyber risk concern for their organizations. This was followed by theft of customer information, cited by 36%; interference with the company website, i.e. hacking, cited by 32%; outside interference with the IT system, cited by 27%; and the theft of intellectual property by electronic methods, 21%.

Data breaches evolve from nuisance to major business threat

By JUDY GREENWALD

Worrisome cyber risks range from small, stolen or lost mobile devices to attacks into the large cloud computing systems increasingly being used by many companies.

The common thread is business' vulnerability, and the risks those vulnerabilities pose to firms' profits and reputation.

"Ten years ago, random attackers used to be a big threat," said Tom Srail, Cleveland-based senior vp of FINEX North America at Willis North America. "They were just nuisance hackers," many of them "your younger-generation people doing it just for kicks," said Mr. Srail. But over the past five to eight years, there have been "much more targeted and much more businesslike attackers" who are looking for data, information and other things they can turn into money, such as credit card numbers, he said.

Causation "matters less and less," said Jeff Grange, senior vp and chief underwriting officer of global professional lines at Torus Insurance Holdings Ltd. in Jersey City, N.J. Whether the problem is because of a hacker or an insider who "goes bad" matters less than the customer not being able to access the technology platform. "Then you're in a bad place with

your customer," he said.

Meanwhile, threats represented by Internet activist groups such as Anonymous are a growing concern, said Richard J. Bortnick, a member of law firm Cozen O'Connor P.C. in

SOURCES OF RISK

Cyber risks come in all shapes and sizes. They include:

- Attacks on cloud computing systems
- Advanced persistent threats
- Political and social activism
- Phishing tactics
- Theft of mobile devices, memory sticks or thumb drives
- Disgruntled employees

Philadelphia. Activists have left Wall Street and "relocated to Internet Street," he said.

Political and social activism over the Internet "will continue to increase because it's easier, it's anonymous and you get a much higher return on human infrastructure investment that you do by simply campaigning out in a

park, or picketing," said Mr. Bortnick. Furthermore, "there's not a major cyber breach that the media doesn't latch onto and report, until there's nothing left to say about it, and then they continue" to report it anyway, he said.

Larry Collins, New York-based managing director and head of e-solutions at Zurich Financial Services Ltd., said, "All of these groups are running around for political gain, looking at your computer and chasing after who you are as a company, in terms of your reputation in the marketplace."

At the same time, lost mobile devices and simple human error remain big issues, say observers.

"People forget things, people lose things, people misplace things. People just don't think about security," said Mr. Bortnick. It may be as simple a matter as using password protection on a mobile device, or not responding to a "phishing" attack, where criminals masquerade as legitimate companies, he said.

Kevin Kalinich, Chicago-based global network and cyber risk practice leader at Aon Risk Solutions, an Aon Corp. unit, said the biggest change over the past 18 to 24 months is the risk represented by mobile communications and mobile transactions.

Last June, for instance, Daniel

Spitler—one of two men arrested in connection with writing code that was used to hack into AT&T Inc.'s computer servers, permitting them to access the email addresses of iPad3G users—pleaded guilty to various charges in U.S. District Court for the District of New Jersey, according to the U.S. attorney's office in Newark, N.J. About 120,000 email addresses and other personal information had been stolen over several days in June 2010, according to the U.S. attorney's office.

However, while mobile devices are still a concern, Mr. Srail said this may be a less frequent risk than it once was because of the focus on encryption and on disabling lost devices. "You don't see people carrying around flash drives" like they once did either, he said.

Cloud computing is another problem, say observers (see related story, page 6), while the loss of intellectual property is yet another issue, said Mr. Collins, who described intellectual property hacking as "very sophisticated."

He pointed to the so-called "night dragon" attacks, which involved coordinated covert and targeted cyber attacks conducted against global oil, energy and petrochemical companies.

According to a report last year

by Santa Clara, Calif.-based computer security company McAfee Inc., the attacks began in November 2009, and McAfee said it believes they originated in China.

McAfee said the attacks have involved a variety of methods, including social engineering, spear-phishing attacks that target email, and the use of remote administration tools "in targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations."

Some observers, however, say the essential picture has changed relatively little.

Robert Parisi, senior vp at Marsh Inc.'s FINPRO practice in New York, said, "We haven't seen a huge change in what's out there causing harm. The boogeyman that we see everyone's afraid of is (advanced persistent threats), the stuff that keeps the guys up at night, because...it's almost impossible to defend."

However, we "haven't see any truly catastrophic losses" resulting from APTs, Mr. Parisi said. Instead, "we still see a lot of exposure" from the same sources, including lost mobile devices, memory sticks or

See **THREATS** page 6

Insure the construction of Madison Square Garden? No sweat.

Sports and entertainment have been a significant part of this country's fabric since the very beginning. So when Zurich saw the plans for the Madison Square Garden complex in 1968, we knew the value and importance of the project for the city. We designed safety programs overseeing the demolition and the construction and also wrote the wrap-up insurance for the entire project. This helped lead to a more successful, productive America, in sports and entertainment and many other arenas of life. **Insuring success since 1912. Visit zurichna.com/100**



100 YEARS
INSURING AMERICA | ZURICH

Assessments key to mitigating cyber risks

By JUDY GREENWALD

A careful assessment of an organization’s cyber risks is critical to both protecting it from data breaches and effectively responding should a breach occur.

And while these assessments often are required by federal and state laws, they also may help firms obtain favorable coverage terms. These surveys should be conducted at least once a year, with more frequent updates as called for, cyber risk experts say.

“Cyber risk is increasingly becoming a board-level risk,” said Ben Beeson, London-based partner, global technology and privacy practice, at Lockton Cos. L.L.P., pointing to U.S. Securities and Exchange Commission guidance issued last year that requires publicly traded companies to report hacking incidents. This makes the job of conducting risk assessments easier, he said.

Experts strongly recommend that these risk assessments be conducted by a team representing a cross section of the company’s departments (see related story).

Mahmood Sher-Jan, vp of product management for Portland, Ore.-based ID Experts, a provider of data breach solutions, said factors the assessment should cover include the controls that are in place around electronically maintained information in a system; how the data is being accessed; where it resides; with whom it is shared, including sub-contractors; and how long it is held in the system.

Robert Parisi, senior vp at Marsh Inc.’s FINPRO practice in New York, recommends creating a risk map that reflects firms’ big risks, including those that are most frequent and severe, and those that may be catastrophic yet have an “almost nonexistent” likelihood of actually materializing. This process also should include an evaluation of risks’ financial and legal impact and regulatory and defense costs, he said.

Mr. Parisi said that in conducting the assessment, firms also should be sure to look at the “softer issues,” such as employee training and whether the company has taken steps as simple as using a

screen saver to remind workers to keep information confidential.

He said firms also must look not only at how they repel risk, but how prepared they are to deal with threats that penetrate their defenses, including its crisis- or breach-response preparedness.

Kevin Kalinich, Chicago-based global network and cyber risk practice leader at Aon Risk Solutions, a unit of Aon Corp., said once an organization quantifies its exposures, it needs to look at how it is mitigating exposure internally. A

TAKING STOCK

A careful assessment of an organization’s cyber risks is important. Here’s what to look for:

- Controls in place around electronically maintained information
- How the data is being accessed
- Where it resides
- Whom it is shared with, including contractors and sub-contractors
- How long it is held in the system
- “Soft issues” such as employee training
- How threats that penetrate defenses are dealt with
- How risk is allocated through contracts
- Coverage under various insurance policies

“huge issue” is allocation of liability by contract—“who’s responsible for what types of hold-harmless indemnity” agreements, he said.

Next, “take a look at existing insurance policies to determine if you have substantial coverage under property or general liability or some other media policy or crime—or even kidnap and ransom—policy,” he said.

Observers say these assessments should be conducted at least annually. Dave Naser, director of the governance, risk and compli-

Tap multiple resources when quantifying risks

By JUDY GREENWALD

Cyber risk assessment should be a team effort, experts agree. “You’re looking at a fairly complex piece of a company’s environment,” and that means a variety of people must participate in the assessment, said Larry Collins, New York-based managing director and head of e-solutions at Zurich Financial Services Ltd. “The first key is getting the right people involved,” said Tom Srail, Cleveland-based senior vp of FINEX North America at Willis North America. It is not something either risk managers or information technology security can do in a vacuum, he said. To be effective, it must be conducted from an “enterprise perspective,” he said. Depending on the company, participants in this process could include experts in risk management, information technology, security, human resources, procurement, treasury, finance, audit, marketing, sales, privacy, compliance and law, observers say. This may be a new approach for a company. Rupert Alabaster, head of cyber risk at BMS Group Ltd. in London, said, “We find that there isn’t always a great level of coordination between the traditional insurance officer and manager and the chief information officers. They don’t always coordinate in a way one would expect.” An attorney should be on

the team—and perhaps even lead it—to protect client-attorney privilege, said Richard Bortnick, a member of law firm Cozen O’Connor P.C. in Philadelphia. “If there’s an incident, and you get sued, the plaintiffs are going to want to discover what your plans were,” he said. “If you have an attorney discussing legal issues,” this will give you at least some protection from discovery if there is litigation, Mr. Bortnick said. Mr. Collins said Zurich recommends that the team be facilitated by an outsider “because you need somebody to coordinate this. You need a fresh set of eyes on the data, on what’s being looked at, and you need somebody who isn’t going to have the same perspective as those who are living in that environment. Sometimes the hardest thing to see in this world is the thing that’s right in front of you, and folks within that environment can’t quite get themselves out of their box to see” where risks can lie, he said. Furthermore, said Zach Scheublein, senior account executive at Frank Crystal & Co. in New York, “There needs to be a buy-in from senior leadership in the organization because really, it’s a top-down approach. If the directors and officers of an organization aren’t committed to protect, to mitigate their organization’s data breaches,” it will not happen.

ance practice at Smart Devine & Co. L.L.C. in Philadelphia, emphasized that “you always

want to be updating and keeping up to date on what’s out there, what’s happening, what kind of

new attack is out there.” Mr. Kalinich said firms need to lay the basic groundwork “for what the overall assessment is,” and then augment this on a continual basis to reflect developments, such as a new product or service, a merger or a divestiture.

He recommends that regardless of new developments, the risk assessment team should meet monthly “to share ideas and make sure plans are implemented on a corporate, enterprisewide basis.”

The frequency of assessments can help firms if there is an investigation following a breach, said ID Experts Chief Marketing Officer Doug Pollack. “If they’ve done a risk assessment within the prior 12 months, and if they took action to address the most egregious gaps identified in the risk assessment, the investigating party will often look at that as kind of a sign of good faith (the firm was) not acting in a cavalier fashion,” he said.

Tom Srail, Cleveland-based senior vp of FINEX North America at Willis North America, said these assessments can be done internally at no cost to the company; can be conducted by brokers, who can charge anywhere from nothing to a “fair amount”; or, if conducted by one of the Big Four accounting firms or IT vendors, cost hundreds of thousands of dollars for an in-depth audit.

“It really depends on the scope of the project,” said Mr. Srail.

Doing all this should help firms in dealing with insurers, observers say. Richard J. Bortnick, a member of law firm Cozen O’Connor P.C. in Philadelphia, said, “From a technical and pricing standpoint, the more secure an underwriter feels about a company’s security systems and protections, the more willing he or she may be with accepting the risk and perhaps affording some price abatement.”

Kirstin Simonson, St. Paul, Minn.-based underwriting director with Travelers Global Technology, a unit of Travelers Cos. Inc., said, “It’s really no different than any other incident response or risk management plan. What we’re trying to understand is, what are you doing to manage and mitigate risk on your end,” thus giving Travelers a “better picture on our end where we may be exposed on your behalf.”

Cloud exposures add new dimension to security threats

By JUDY GREENWALD

Cloud computing is a growing cyber risk that introduces a new element of vulnerability.

Larry Collins, New York-based managing director and head of e-solutions at Zurich Financial Services Ltd., said the problem with cloud computing is that communication in and out of the cloud creates an open “fourth wall.”

Kevin Kalinich, Chicago-based global network and cyber risk practice leader at Aon Risk Solutions, an Aon Corp. unit, said that while outsourcing to a third

party is efficient and cost-effective, “you’re losing control” with cloud computing. While the problem with mobile devices is one of frequency, most of those breach cases involve just a few customers at a time.

Breaches are a “much more severe issue” when it comes to the cloud because they are much larger, Mr. Kalinich said. He pointed to the incident involving online shoe and clothing retailer Zappos.com, a unit of Seattle-based Amazon.com Inc., whose breach earlier this year, he said, resulted in “hundreds of

thousands, if not millions,” of personally identifiable records being made accessible.

Cloud computing is bringing a new dynamic to the area of risk, said Paul Bantick, senior underwriter, large risks technology, media and business services, for Beazley P.L.C. in London. “Time will tell” how it plays out.

In addition, Mr. Bantick pointed to the problems caused by the Sony Corp. PlayStation breaches, which resulted in a 23-day closure of the PlayStation online network and an estimated \$171 million financial loss.

Threats: Cyber risks grow

CONTINUED FROM PAGE 4

thumb drives, he said.

Rupert Alabaster, head of cyber risk at BMS Group Ltd. in London agreed that little, if anything, has changed in certain respects. “The threats are not necessarily changing in terms of the basic ways or the reasons why people would want to get hold of electronic data or information that stores in the cloud,” he said.

However, Mr. Alabaster said, the ease with which wrongdoing can be accomplished has increased, while the amount of data involved has grown exponentially along with the costs incurred in connection with

cyber threats. This is because business is more complex, and more interlinked globally with other countries, which makes it easier for people to gain access to the data, he said.

Jay Sheehan, Hartford Conn.-based senior vp of Preferred Advantage L.L.C., the specialty brokerage division of Preferred Concepts L.L.C., said, “The reality about having information on the Web is that someone who understands the protocols of either the software or the hardware can get in. And once they’re in, they can disrupt your business, or they can take the personal information of your clients or your employees.”

Business Insurance
**Risk Manager
OF THE YEAR®
2012**

Business Insurance
**Risk Management
HONOR ROLL®
2012**

APRIL 17, 2012 | PHILADELPHIA, PA | LOEWS PHILADELPHIA HOTEL

6:30 am - 8:30 am

Networking Reception & Breakfast Award Recognition Program

Registration Open!

2012 Risk Manager of the Year®

John J. Marren
Director, Global Risk and Insurance Management CSL Ltd.

2012 Risk Management Honor Roll®

Grace Crickette
Chief Risk Officer, University of California

Julie L. DeSantis
VP, Risk Management , Sony Corp. of America

John Pearce
General Manager Policy and Risk, Fonterra Co-operative Group Ltd.

SPACE IS LIMITED RESERVE YOUR SEAT TODAY!

WWW.BUSINESSINSURANCE.COM/RMOY2012

In Partnership with:



MARSH

Opinions

EDITORIAL

Cyber threats grow, evolve

Cyber risks present a daunting and complex challenge for risk managers—one that is likely to grow.

Cyber threats present myriad risks, ranging from the loss or theft of increasingly pervasive mobile devices to attacks on the large cloud computing systems used by many companies, which could have a devastating impact on firms' bottom lines.

Fortunately, many risk managers recognize this. A *Business Insurance* survey indicates that while only about one-quarter of firms surveyed buy stand-alone cyber insurance coverage, 43% consider themselves self-insured for the coverage.

Somewhat troubling, though, is that 18% of firms surveyed said they believe they already have coverage under existing noncyber policies. In light of insurers' reluctance in some cases to provide this coverage, they would do well to confirm this with their brokers and insurers.

But even risk managers who have the coverage are far from reaching the point where they can relax. As observers have noted in the past, the "bad guys" continue to come up with ingenious new ways to make life miserable for risk managers and other staff, who are engaged in a continual struggle to protect their companies' computer systems on behalf of their customers, employees and firms.

Critical to any successful risk management program is risk managers' partnership with their information technology departments. Many already recognize this. The *BI* survey found that 93% of companies consult first with their IT departments before buying cyber coverage, including 100% of those with at least \$100 million in annual revenues. It remains unclear, however, how many of those who are self-insured—as well as those who do not have any coverage—consult with their IT departments.

Also worrisome are the significantly lower percentages of risk managers, even among those who buy stand-alone coverage, who say they consult with other internal parties, including their legal departments and chief financial officers.

Regardless of whether they have stand-alone coverage, are self-insured or consider themselves to have coverage under other policies, all risk managers who have not already done so should consider a coordinated approach, with a committee that meets frequently to address this rapidly changing area.

That is the best approach to dealing with this ongoing challenge.

LETTERS

Business Insurance welcomes letters to the editor.

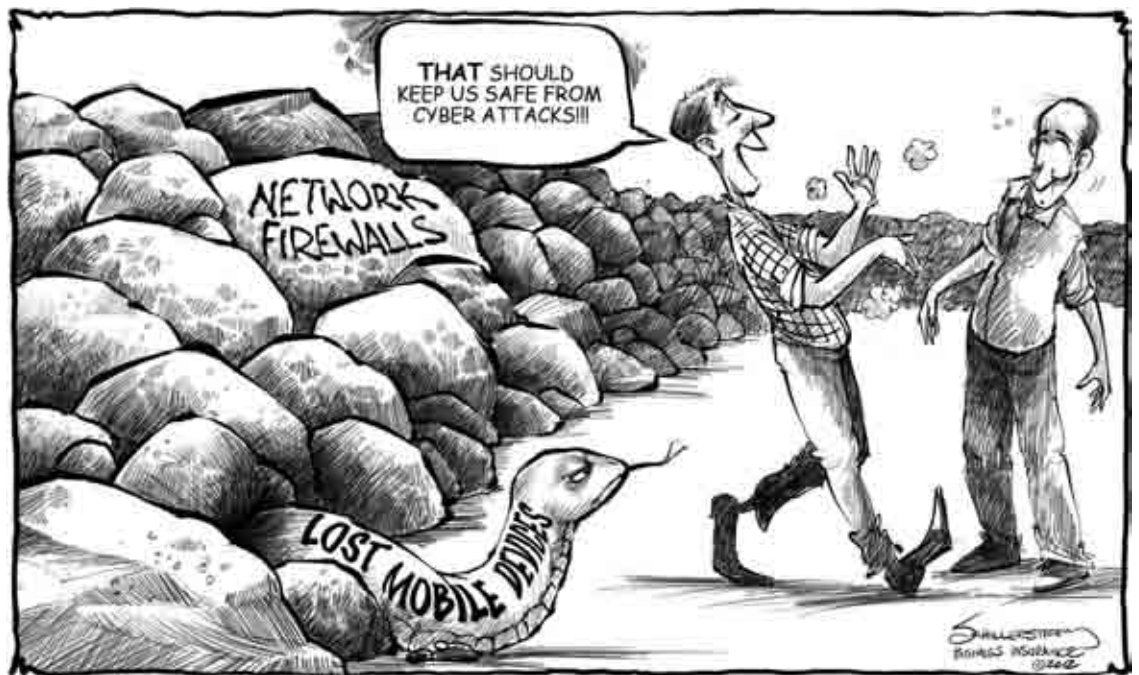
The section is intended to be a forum for readers' opinions and comments. We reserve the right to edit letters for clarity or space. We will not publish unsigned letters.

Please send your letters to:

Letters to the Editor, *Business Insurance*,
360 N. Michigan Ave., Chicago, Ill. 60601-3806

Fax: 312-280-3174; email: gsouter@businessinsurance.com

SCHILLERSTROM



COMMENTARY

Cyber crime now a national threat

On Dec. 7, 1941, and Sept. 11, 2001, the United States found itself under attack without warning.

Certainly, informed Americans in 1941 knew long before the attack on Pearl Harbor that there was a possibility that the country would find itself at war with Japan—sometime. And in 2001, we knew of al-Qaeda and knew there was a distinct possibility that the group would attack targets on American soil—sometime.

But in both cases, no one knew when "sometime" would be. When sometime arrived, the nation was caught unawares, and thousands died.

Now it appears that a different sometime is fast approaching, as was underscored in a recent speech by FBI Director Robert Mueller.

"Terrorism remains the FBI's top priority," Mr. Mueller said at a conference on cyber security in San Francisco this month.

"But in the not-too-distant future, we anticipate that the cyber threat will pose the No. 1 threat to our country," he said. "We need to take lessons we learned from fighting terrorism and apply them to cyber crime."

That's a good place to start, because this new threat—albeit sometimes apparently carried out by foreign governments—can't be dealt with in the matter in which traditional military threats were.

Readers of a certain age will recall when one of North America's most important 20th century defenses was the Distant Early Warning Line, which stretched across northern Canada. The

DEW Line was designed to detect Soviet bombers flying across the Arctic before they reached their targets in the United States and Canada.

Fortunately, no Soviet bomber ever crossed the DEW Line. Perhaps the defense perimeter's mere existence helped ensure that it was never penetrated. When the Soviet threat vanished, the DEW Line was dismantled.

But there's no way to build a DEW Line in cyber space. Unlike the old Soviet bombers, the attacks can come from multiple directions at once. While the attacks have to come from a physical place—somebody has to write the code that triggers the attacks—responding to them is far more difficult than targeting an airbase or submarine from which a Cold War-era assault would have originated.

Applying the lessons learned in fighting terrorism to dealing with the cyber threat is certainly a reasonable approach for now. But even as dealing with terrorism required a different approach than dealing with a conventional military enemy, effectively dealing with cyber crime will require new strategies as well.

Terrorism may still be the No. 1 threat to the country, but cyber crime's time is coming. Fortunately, this time around, as Mr. Mueller said, we know what the threat is, so we can take steps to prepare now. After all, chances are that sometime is going to come sooner than we expected.

Contact: mhofmann@businessinsurance.com



MARK A. HOFMANN
SENIOR EDITOR

Perspectives

Data breaches are evolving quickly from merely compromising a business' data or the personal information of its customers. Now cyber attacks are capable of producing physical effects, such as taking a utility grid offline, and affecting a wider community. Insuring against these industrial threats is complicated, says Vincent J. Vitkowsky, a partner at the Edwards Wildman Palmer L.L.P. law firm in New York, and organizations are challenged to assess their risks from a broad perspective.

Industrial cyber attacks generate wide range of coverage concerns

By Vincent J. Vitkowsky



Mr. Vitkowsky

Companies in critical infrastructure industries are prime targets for industrial threat cyber attacks.

Data breaches that compromise personal information and other data maintained by businesses have been widely publicized. But beyond these, another kind of threat has emerged.

Security company McAfee Inc. identified "industrial threats" first on its list of 2012 threat predictions. These are cyber attacks with physical effects, including the manipulation or destruction of industrial control systems and the equipment and machinery that depend on them. The attacks can put property and lives at direct risk. They present challenges to businesses, especially within the critical infrastructure sectors, and their insurers.

Industrial threat cyber attacks can occur through malware intrusions. The malware takes control of industrial control systems, which are the combination of hardware and software used to monitor and control equipment and machinery, often referred to as supervisory control and data acquisition systems, or SCADA. The purpose of the attack can be sabotage, extortion, competitive business advantage or simple mischief.

Game changers

The potential impact of these attacks was demonstrated in March 2007, when the U.S. Department of Homeland Security conducted a cyber attack exercise called Aurora. It hacked into a network controlling a diesel power generator and put the generator out of sync with the power grid. Video footage of the generator shows it shuddering, filling the room with steam and smoke, and halting.

The key, game-changing development was the appearance in 2010 of a virus known as "Stuxnet," which successfully disrupted the logic control system for the centrifuges that Iran uses to enrich uranium, reportedly making about 1,000 of them unusable. It is believed that the virus was transmitted by a USB stick plugged into an otherwise secure computer.

A DHS official testifying before the House Subcommittee on Oversight and Investigations on July 26, 2011, said that copies of the Stuxnet code, in various iterations, had become publicly available and could be modified to target other industrial control systems.

At the Black Hat computer security conference in August 2011, Dillon Beresford of NSS Labs revealed that he had created his own version of Stuxnet in less than three weeks of work, spending less than \$10,000 to replicate his target hardware environment.

Companies in critical infrastructure industries are prime targets for industrial threat cyber attacks. Companies in the energy sector, notably those that supply electrical power, are especially inviting targets for sabotage or extortion. Many of the systems that operate the U.S. electrical power grid are connected to the public Internet, which increases their vulnerability.

FBI Director Robert Mueller revealed that in July 2008, a company known as Pacific Energy Resources Ltd. reported that six computer servers had been rendered inoperable, disabling the leak detection systems on three offshore oil platforms. The attacks were conducted by a 28-year-old former consultant to the company who was disgruntled because he was not hired for a permanent position. He conducted the attack from his home computer using his various user accounts. It could have been worse. In this instance, the systems were restored before any leak occurred. According to the journal *Jane's Intelligence Review*, "with many offshore rigs increasingly using unmanned robot platforms, hacking into control systems could cause major damage to systems and disrupt or potentially halt production."

On Sept. 28, 2011, DHS gave reporters the first tour of its Central System Security Program facilities in Idaho Falls, Idaho. DHS official Greg Schaffer confirmed for the assembled reporters that the world's utilities and industries are becoming increasingly vulnerable. He said that disgruntled employees, hackers and perhaps foreign governments "are knock-

ing on the doors of these systems, and there have been intrusions."

In January 2012, researchers highlighted the exposures. First, one research group discovered and revealed serious vulnerabilities in widely used industrial control systems made by six leading manufacturers. These include weaknesses such as back doors, lack of authorization and encryption, and weak password systems. In addition, a graduate student at Cambridge University revealed that he was able to locate and map more than 10,000 industrial control systems that were accessible through the Internet. Only 17% of these required authorization to connect. This suggests that most of the operators are not even aware of the extent of their vulnerabilities.

Most industrial threat cyber attacks have been conducted by private individuals or criminal organizations. But in September 2011, a DHS bulletin advised that the collective known as Anonymous had expressed interest in targeting industrial control systems. DHS noted that Anonymous "could be able to develop capabilities to gain access and trespass on control system networks very quickly." There are very recent press reports that the National Security Agency believes Anonymous will have this capability within the next year or two, although others estimate it would take three to five years.

Industrial cyber attack threats also could be conducted by governments, including cyber attacks in support of traditional war or warlike hostilities. Terrorists are also seeking the capacity to launch cyber attacks with physical effects. Details of U.S. SCADA systems have been found on computers captured from al-Qaeda.

Insurance implications

In addition to physical effects such as property damage, industrial threat cyber attacks can cause business interruption or give rise to liabilities for contract breaches or torts. If the disruption affects the target's business associates, vendors or customers, they, too, may assert claims.

Some of these may generate

claims for insurance coverage that differ from those typically arising from data breaches revealing personally identifiable information. Resolution of these claims will depend on the nature of the attack, the damages, the claims, the type of policy and its terms and exclusions. Questions of causation could complicate the analysis. So would the involvement of insiders. And industrial threat cyber attacks will certainly present issues of attribution among individuals, criminals, hackers, terrorist organizations and governments.

Scenarios

Imagine an attack on power utilities in a Western country. U.S. intelligence agencies point to Iran, but Iran denies culpability. Al-Qaeda claims responsibility, but there is no independent evidence of its involvement. A group of criminals believed to be in the United States also claims responsibility and seeks to extort money by threatening future attacks. And short selling in foreign markets implies knowledge and involvement by foreign business or criminal actors. On these facts, determining the scope and effect of potentially applicable insurance coverages would raise many challenges.

Exposures to loss and theft of data impose significant cost and burdens on businesses, and can trigger claims under certain insurance policies. These continue to occur, and ongoing dedication of resources and attention is required to prevent them and mitigate the related exposures, such as notification of affected individuals and governmental agencies, costs of remediation and reputational harms.

But industrial threat exposures go far beyond the ordinary costs of breaches. They impose significant risks of physical harm and destruction, including potentially significant environmental damage, incapacitation of a nation's ability to respond to more conventional threats, and loss of life. Companies and their insurers, particularly those involved in critical infrastructure sectors, are challenged to assess their risks from industrial threat cyber attacks and take steps to mitigate their exposures.

Vincent J. Vitkowsky is a partner in the law firm of Edwards Wildman Palmer L.L.P. in New York. He can be reached at VVitkowsky@edwardswildman.com.

Perspectives

Recent cyber attacks and data breaches have been wide-ranging and expensive. Therefore, corporations and other entities should have a firm grasp on their insurance coverages for such incidents and what their policies will and will not cover. Scott N. Godes, of counsel at Dickstein Shapiro L.L.P. in Washington, tells what to look for when purchasing cyber insurance, and also discusses where traditional insurance policies, such as commercial general liability and employment practices liability, may apply.

Surprising sources of coverage

By Scott N. Godes

It is axiomatic that businesses today rely upon big data and computer networks to a degree not imaginable just a few years ago. This change in technology, however, also has led to risks that companies face today: data breaches, hacks, network interruptions and other cyber risks. The number of data breaches and cyber attacks that companies and other entities have faced has been so large and expensive that 2011 could be considered the year of the cyber attack.

The Corporation Finance Division of the U.S. Securities and Exchange Commission has recognized this change and recently issued guidance regarding the disclosure of cyber security risks, as well as what insurance reporting entities have for such cyber risks. The guidance on cyber risks lists a litany of cyber attacks, cyber risks, and other potential risks that businesses face in the context of data, network security and more. Significantly, the Corporation Finance Division states that appropriate disclosures may include a description of relevant insurance coverage.

Policyholders and insureds facing cyber risks and liabilities should analyze their entire slate of insurance policies to determine what coverage might apply to such risks. "Cyber insurance" policies should provide coverage for certain cyber risks, and there also may be overlapping coverage under other insurance policies for such risks.

The first place a company should look to determine whether it has, or may have, coverage for cyber risks is to any "cyber insurance" policies that the entity holds. A close look at these policies is warranted, as the coverage under such policies often varies significantly by policy. Note that just because a policy is sold as a "cyber insurance" policy, it doesn't mean the insurance company will automatically agree to cover or defend against potential liabilities for all cyber risks. Cyber insurance policies are relatively new and not as regulated as more traditional insurance policies; in fact, the market for cyber security policies has been called the Wild West of insurance. The policies often are sold with various coverage modules, provisions and insuring agreements, allowing for companies to pick and choose the coverage that they want to purchase

within the offered insurance policy. Because of the variety of coverages offered, a careful review of the policy form and coverages purchased before a claim arises is critical to understand whether the cyber insurance policy will provide coverage, and, if it will, how much coverage is available for the event.

When reviewing cyber insurance policies from the highest level, the entity should determine whether there is coverage for first-party risks and third-party risks. Entities also should closely consider whether their cyber insurance policies provide coverage for privacy breaches, even before there has been a "claim," to ensure that coverage exists for costs incurred immediately after the discovery of a data breach, including investigation and notification costs. Certain cyber insurance policies exclude coverage for costs relating to breaches of contract. Consider how such an exclusion would affect the entity's ability to handle a cyber risk that leads to breach-of-contract damages. Entities should review whether the cyber insurance policies specifically

provide coverage for violation of data breach statutes or similar statutes that may be passed in the future regarding the publication of or unauthorized access to personally identifiable information. They should focus on what damages are covered, and whether damages based on state-based consumer protection act statutes are covered. Entities also should consider whether there is coverage for any security audits that may be required by certain third parties, such as business partners.

Lastly, the entity should consider potential coverages for data loss or corruption, or the inability to access data or to conduct business because of the inaccessibility of the various cloud computing platforms on which the entity relies or provides to clients. The trigger for such coverage should not be limited to a "physical" cause of loss and should be broad enough to include cyber attacks, data breaches, hackings and other cyber events.

There may be overlapping coverage for certain cyber risks under a "standard form" commercial general liability insurance policy. When considering cyber risks, it is important to keep in mind the basic insuring agreements under standard-form CGL policies. Those policies often provide coverage for personal and

advertising injury, bodily injury and property damage. Each of these sections of the basic insuring agreement in a CGL policy may provide coverage for certain cyber risks.

Depending upon the allegations and the nature of the facts, there may be a duty to defend. It may be that the publication of information is personal and advertising injury, that the incident is property damage in the form of loss of use of or physical damage to computer hardware, or that there was bodily injury (under an expanded definition) because of alleged mental anguish.

Crime policies also may provide coverage for certain cyber risks. Crime policies often are sold with coverages provided through various insuring agreements, and not every insuring agreement is offered or purchased, depending upon the policy.

Many crime policies' basic and first insuring agreement provides coverage for loss of "money" or "other property" caused by the unlawful taking of electronic data or other confidential information by an individual falling within the policy's broad definition of "employee."

Depending upon the wording and the potential application of any exclusions, that coverage may be broad enough to cover the entity for the loss of its data as "other property." It also may be broad enough to cover the entity for any penalties incurred directly as a result of the theft, unless otherwise excluded. Other coverages, such as premises coverage, may apply to the extent that data or other information is stolen from the entity's "premises," as defined in the insurance policy. There is a solid argument in favor of coverage for data breaches under many policies' computer and funds transfer fraud coverage.

Certain crime policies also provide coverage for first-party costs incurred to restore or replace damaged or destroyed electronic data or computer programs stored within the insured's computer system. This coverage may extend to losses resulting from a virus or other electronic vandalism. Such coverage may be broad enough to include loss from a hacker damaging or destroying electronic data maintained on the entity's internal computer systems by introducing a computer virus.

Commercial first-party property policies often include coverage for first-party property damage and time-element expenses. The basic insuring agreement under such policies often provides coverage for loss of or damage to the entity's

insured property, covering all risks of direct physical loss of or damage to insured property at insured locations. Depending on the insuring agreement, there may be coverage for the damage or destruction of electronic data caused by certain physical events. Coverage also may be available for the destruction of data and for time-element expenses related to the inability to access computer networks. Certain first-party policies provide coverage for loss of "valuable papers and records," and that insuring agreement may provide coverage for loss of electronic data. Entities also should consider the potential scope of coverage for time element losses, such as earnings coverage, business interruption coverage, or contingent business interruption coverage resulting from the failure of a cloud or other third-party provider's services to the entity.

Entities should review employment practices liability insurance policies closely to determine whether there may be coverage for certain cyber risks, such as data breaches. For example, certain EPLI policies may provide the entity coverage for third-party claims by or on behalf of "employees" alleging "invasion of privacy" for the unauthorized disclosure of confidential "employee" information resulting from a data breach or cyber attack. Certain EPLI policies provide coverage for "wrongful employment acts," defined terms that may expressly include "employment-related torts" such as "invasion of privacy" for the unauthorized disclosure of personally identifiable information under the Health Insurance Portability and Accountability Act, credit information under the Fair Credit Reporting Act, criminal records and other confidential data.

Entities also should review their directors and officers liability insurance policies to determine the scope of "entity" or "Side C" coverage for purposes of responding to a data breach or cyber risk. Under certain policies, entity coverage no longer is limited to "securities claims," and may encompass a wide variety of "wrongful acts." The policies also may consider an investigation or demand letters to constitute a "claim," thereby triggering the duty to defend. A close review of policies with such coverage is warranted.

Scott N. Godes is the author of the award-winning Corporate Insurance Blog and co-chair of the American Bar Assn.'s Insurance Coverage Litigation Committee's Computer Technology Subcommittee. Mr. Godes is of counsel at Dickstein Shapiro L.L.P. in Washington, where he represents corporate insureds and frequently counsels clients regarding insurance for cyber risks. He can be reached at GodesS@DicksteinShapiro.com.



Mr. Godes

Cyber insurers offer buyers higher limits, cheap rates

Capacity increases as market matures, coverage expands

By MIKE TSIKOUidakis

The cyber liability insurance market has abundant capacity, with numerous insurers vying for business, keeping rates low and expanding available coverages.

As more insurers enter the cyber liability market, brokers are seeing available capacity of \$250 million to \$300 million and competitive rates.

Regulators in many states passed security breach notification laws in 2005, which spurred significant changes in the insurance coverage, according to Peter Foster, executive vp of Willis North America's executive risks group in Boston.

Now, compared with five years ago—when underwriters were worried about understanding cyber risks—capacity is significantly higher, said Emily Freeman, executive director of the technology and global privacy

group at Lockton Cos. L.L.P. based in London.

“Five years have passed and a lot more people are comfortable with the risk issues (and) are comfortable approaching the reinsurers,” she said.

On average, up to \$20 million in limits costs \$12,000 to \$14,000 per million, said Mr. Foster.

He said where limits are in the range of \$20 million to \$50 million, the premium is approximately 1% of the limit.

“We see accounts now that are below 1% and it's because they're putting \$200 million in limits,” he said. “The cost comes down dramatically as we move up because we've only seen a few multimillion-dollar losses.”

Nick Economidis, underwriter at Beazley P.L.C. in Philadelphia, said cyber policies at Beazley start as low as \$3,500. For large, sophisticated organizations, the rate per million is approximately \$15,000 to \$20,000, with “capacity up to \$20 million per risk,” he said.

“We're generally in the market for \$10 million.”

Mr. Economidis said cyber coverage has evolved from when it was first introduced in the late 1990s, and that evolution is a con-

tinuous process. “We certainly figured out how to underwrite it better and more efficiently,” he said.

Tim Stapleton, assistant vp and professional liability product manager for Zurich North America in New York, said the insurer offers up to \$25 million in limits. “That has actually changed over the course of the past three years. When we entered the market, we offered up to \$10 million, and we've since expanded our capabilities,” Mr. Stapleton said.

Zurich's cyber coverage has expanded from liability and privacy breach cost coverage to business interruption, digital asset replacement, cyber extortion, and Internet media, among others, he said.

For organizations that store a significant amount of data, their rate usually is significantly higher, said Kevin Violette, senior broker at OakBridge Insurance Services L.L.C. in Bloomfield, Conn.

For example, the rate for a manufacturer that stores little personal data on its network would be much lower than for a retail shop that works directly with the consumer on a daily basis, he said.

“Right now, rates are about as low as they're probably going to get, obviously driven by the capacity in the market, which has increased substantially over the past few years,” said Mr. Violette. “Markets are really clamoring for the business right now, and they're beating each other up to get premium on the books.”

Meredith Schnur, senior vp of Wells Fargo Insurance Service USA's professional risk group in New York, said that since the first cyber policy was introduced in the market in 1998, more than 35 pri-

mary policy forms for the risk have followed, and “we have a lot of primary capacity, which has caused a relative reduction in rates,” she said.

Available coverages include third-party network security, data privacy liability, Internet media liability, first-party business interruption, data asset loss and cyber extortion, Ms. Schnur said.

Other add-on coverages include crisis management expenses, which covers costs incurred as a

See **COVERAGES** next page

SEPTEMBER 5TH, 1:45 A.M.

A DEADLINE AND A BUSINESS LIFELINE

IN AN INSTANT,
DOUG HOLT
REMEMBERS
WHY HE TRUSTS
HIS AGENT

Doug wakes up wondering if that fire at his supplier's facility might also send his own future up in smoke. It's also the instant he remembers his property coverage, underwritten by CNA, and that if he needs to file a claim, they'll make it as painless as possible. Sleep tight, Doug.

To learn more about our broad portfolio of insurance products and services, and the industries we serve, visit www.cna.com.

Business Services • Construction • Financial Institutions • Healthcare • Manufacturing
Professional Services • Real Estate • Retail • Technology • Wholesale Distribution

CNA

We can show you more.®

Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. CNA is a registered trademark of CNA Financial Corporation. Copyright © 2012 CNA. All rights reserved.

Insurers examine cyber risk management strategies

By MIKE TSIKOUDAKIS

For the best cyber liability coverage, organizations need to present well-rounded risk management controls to insurers and carefully weigh an insurer's crisis management and claims management experience.

Most insurers have secured vendor relationships with crisis management firms to handle data breaches at a pre-negotiated cost, said Kevin Violette, senior broker at OakBridge Insurance Services L.L.C., Bloomfield, Conn.

"To the extent that (organizations) don't have those relationships in place, when a breach occurs they end up paying an emergency rate, which is significantly higher than what would be based upon what the carriers' rates would be," he said.

Some of the crisis management services include computer forensic firms, privacy counsel to determine the nature of the breach, notification to individuals, and potential credit monitoring, Mr. Violette said.

Organizations researching favorable

terms and pricing for cyber coverage also need to consider an insurer's claims management experience regarding cyber losses, experts say.

"Handling a cyber problem is different from managing a traditional liability problem. It has a crisis element to it the minute it happens," said Emily Freeman, London-based executive director of the technology and global privacy group at Lockton Cos. L.L.P.

To obtain favorable terms, conditions and pricing for their cyber exposures, organizations need to present well-

rounded risk management controls regarding how they handle data breaches, said New York-based Oliver Brew, vp of miscellaneous professional liability and technology, errors and omissions, for Liberty International Underwriters.

"The risk management is critical to the success and the appetite for an insurer," he said.

Tim Stapleton, vp and professional liability product manager for Zurich North America in New York, said that as claims from data breaches caused by third-party vendors increase, companies need to place an emphasis on their encryption and contracting procedures with third parties.

CAN YOU AFFORD NOT TO HAVE AN EXPERT AT THE HELM?

With so many security threats in today's digital world, can you really afford to have your Cyber, Security & Privacy exposures underwritten by anyone less than an expert?

S.H. Smith & Company employs the absolute best and brightest Cyber, Security & Privacy experts in the industry so that you do not have to. We have been placing Cyber, Security & Privacy liability since its inception; in fact, some of the most widely used Cyber, Security & Privacy policies were written by our experts. When it comes to underwriting trends, we set them rather than follow.



S.H. Smith & Company, Inc.

Specialty Insurance Broker



WANT TO HEAR FROM OUR EXPERTS?

Sign-up to receive our weekly newsletter by scanning this QR code with your smartphone.

WWW.SHSMITH.COM (800) 356-0168

Professional & Management Liability | Large Commercial Property, Casualty & Environmental | Programs | In-House Underwriting



Coverages: High limits, cheap rates

CONTINUED FROM PREVIOUS PAGE

result of a data breach, such as legal advice, notification expenses, credit monitoring and regulatory penalties, she said.

As cyber liability is an evolving risk, insurers have shifted much of the focus from Internet liability and network risk to data breach notification and third-party vendors, and have expanded coverages to respond to those exposures, experts say.

Also, insurers have secured relationships with crisis management firms to assist clients during a data breach. But for the best coverage terms, an organization has to demonstrate good risk management practices during the underwriting process (see related story).

The 2005 security breach notification laws pushed underwriters and brokers to design policies that would provide coverage for notification costs, credit monitoring expenses and forensic costs, Willis' Mr. Foster said.

"As the years progressed, different areas of risk really became more apparent," Mr. Foster said, noting that coverage recently has expanded to include protection for third-party vendors as more corporations outsourced their information to application service providers.

"It's not so much that the coverage has changed as that there's new coverage available, as much as coverages have expanded," Mr. Economidis said.

At Beazley, notification cost coverage has gone from a reimbursement-type structure with a dollar limit to a coverage based on the number of individuals that need to be notified, he said.

To support that structure, Beazley has taken the notification cost outside of the limit, "which was something we had to do when we went to a number of people vs. a dollar limit, because if you're not counting dollars you really can't subtract them from the aggregate," he said.

Reinsurers develop appetite for cyber liability risks

By **STUART COLLINS**

Reinsurers and excess insurers are providing more than enough capacity for stand-alone cyber insurance products to meet demand, but concerns over business interruption exposure and aggregated risk are growing.

Reinsurers are supporting the burgeoning cyber insurance market through direct writing, as well as providing treaty and facultative reinsurance, said Simon Milner, a London-based partner at JLT Specialty, a unit of Jardine Lloyd Thompson Group P.L.C.

The large continental European reinsurers—the German market in particular—have been especially active in offering cyber reinsurance, said Mr. Milner.

Munch Reinsurance Co. has a good appetite for cyber risks, preferably written on a quota share reinsurance basis, said Andreas Schlayer, Munich-based head of the reinsurer's IT Risk Topic Network.

Reinsurers deal with a wide range of cyber coverages that cut across many lines of business, said Michael Kuhn, Zurich-based senior property underwriter for Swiss Re Ltd., which underwrites cyber risks through direct, facultative and treaty reinsurance.

Reinsurers split cyber risks into different exposures and assess them and underwrite them separately, said Mr. Kuhn. The amount of capacity on offer and its price depends on the exposure, as well as the quality of policyholders' IT security, cedents' understanding of underwriting IT risks and risk accumulation, he said.

Reinsurers so far have focused more on reinsuring specialty cyber products, rather than broadening coverage in traditional property and liability reinsurance treaties, experts say.

Munich Re's preferred approach to cyber risk is to provide specialist treaty reinsurance for stand-alone cyber insurance.

"Specialist treaty reinsurance covers most of the areas insured under cyber insurance policies, like first- and third-party data breach costs, technology errors and omissions, damage from computer viruses, and products that cover cyber extortion," he said.

In addition to specialty coverages, Swiss Re also provides cyber coverage through traditional property and liability treaties, said Mr. Kuhn. "We do get requests from property, engineering and liability treaty clients that want to expand their insurance cover to provide certain cyber exposures," he said.

There are several reinsurers supporting primary cyber insurers with treaty reinsurance, said Ben Beeson, a London-based partner with Lockton Cos. L.L.P. However, reinsurers are not fully engaged with cyber risks, he said.

"Direct insurers are the real driving force in the market. But as the market evolves, I would expect reinsurers to become more involved and pick up the big catastrophe exposures in the

future," said Mr. Beeson.

A growing number of excess insurers also are helping build higher program limits.

As the frequency and severity of security breaches has increased, and as companies rely more on information technology, they have concluded that they need much higher coverage towers to protect their balance sheets and reputations, said Chris Andrews, Boston-based assistant vp of professional liability at Lexington Insurance Co.

Limits for primary security and privacy insurance remain relative-

ly stable at around \$10 million to \$20 million, said Mr. Andrews. However, excess insurers can bring coverage up to much higher levels—anywhere between \$30 million and \$200 million has been placed in the market, he said.

Financial institutions, health care and retailers require higher limits, while higher-education institutions also are requesting higher limits, he added.

Excess insurers are able to match growing demand for cover and for higher limits with additional capacity, said Mr. Andrews.

"Excess limits can virtually be as high as clients need to build their coverage tower," he said.

However, as the market grows, so do losses.

Reinsurers and insurers are becoming more wary of risk aggregation, said Lockton's Mr. Beeson. For example, reinsurers are concerned about the number of policyholders that back up data with the same cloud provider. "If a cloud provider is hit by a malicious attack, it will trigger multiple insurance policies," he said.

"Risk aggregation is only now stating to register on cyber insur-

ers' and reinsurers' radars," said Mr. Beeson.

Reinsurers are concerned with accumulation of risk, such as generic computer viruses, the trend toward outsourcing to cloud computing providers and contingent business interruption exposures for Internet service providers and telecommunications firms, said Mr. Kuhn.

There are two main sources of systemic risk, said Mr. Schlayer: first-party damage from a widespread computer virus, and

See **REINSURANCE** next page



Cyber Liability HOW AT RISK IS YOUR ORGANIZATION?

Standard hospital professional liability insurance does not cover cyber liability and the associated risks. With all the personal health information and personal credit information, healthcare facilities need cyber liability insurance to protect themselves from all types of internet and technology related problems.

BerkleyMed and Berkley Technology Underwriters are joining together and sharing their expertise to meet the unique needs of the healthcare self insured sector.

BerkleyMed and Berkley Technology Underwriters are member companies of W. R. Berkley Corporation, one of the most respected names in the property casualty insurance market.

Contact us to learn more about our offerings.



1-800-523-3815 | rwillis@berkleymed.com | www.berkleymed.com/cyber-liability

McAfee exec calls for government-backed coverage

By **STUART COLLINS**

A senior information technology industry figure has proposed that the U.S. government consider providing cyber reinsurance to encourage the development of a specialist insurance market, but market participants say they are more than meeting demands for limits.

In a statement to a U.S. House of Representatives committee on Feb. 8, Phyllis Schneck, vp and chief technology officer-global public sector for security technology company McAfee Inc., said insur-

ers are "reluctant to create a vigorous marketplace" for cyber security insurance.

"Government should give consideration to implementing reinsurance programs to help underwrite the development of cyber security insurance programs," Ms. Schneck told the House Energy and Commerce Committee's Subcommittee on Communications and Technology during a hearing on cyber security threats to communications networks and private-sector responses. "Over time, these reinsurance programs could be phased out as insurance mar-

kets gained experience with cyber security coverage," said Ms. Schneck.

However, brokers and reinsurers say there is ample capacity in the market for most cyber risks and they are more than able to meet current demand.

"Reinsurers have abundant capacity for cyber insurance that makes sense, but so far there has not been a great deal of demand," said Bryon Ehrhart, Chicago-based chief strategy officer for Aon Benfield and chairman of Aon Benfield Analytics, part of Aon Corp.

While there is plenty of reinsur-

ance capacity for cyber products such as security and privacy insurance, reinsurers are more cautious about business interruption exposures, he said.

Ms. Schneck also said the government should seek "positive incentives" to promote cyber security, rather than pursuing regulation. In particular, she backed the October 2011 recommendations made by the House Cybersecurity Task Force, led by Rep. Mac Thornberry, R-Texas. The recommendations included incentives such as information sharing, insurance reforms and tax credits, she said.

"Better enabling information sharing as outlined in Reps. Rogers' and Ruppersberger's bill is critical for addressing the cyber threat," said Ms. Schneck, referring to the Cyber Intelligence Sharing and Protection Act of 2011 was introduced Nov. 30, 2011, by Reps. Mike Rogers, R-Mich., and C.A. Ruppersberger, D-Md. "There are also other positive incentives that can help address some of the fundamental challenges (Internet service providers), telecoms and other members of the communications ecosystem have—challenges in hiring the right type of cyber security experts, regulatory disincentives, economic disincentives and the immaturity of the insurance market, which has limited the growth of the kind of insurance programs needed for companies to insure against catastrophic losses," she said.

Ms. Schneck also called on the government to impose limitations on liability for damages as well as for noneconomic losses.

In May 2011, the White House announced its Cybersecurity Legislative Proposal, which would enact a single federal legislative scheme outlining businesses' obligations in notifying consumers when there is a breach of their privacy, as well as increase the criminal penalties for cyber criminals.

ACORD **INSURANCE**
LOMA **SYSTEMS**
FORUM

May 15–17, 2012

Rosen Shingle Creek, Orlando, Florida

Register now at acordlomaforum.org

**Get Connected
with Thought
Leaders.**

TECHNOLOGY

INNOVATION

CONNECTIONS

BUSINESS

Reinsurance: Big appetite

CONTINUED FROM PREVIOUS PAGE

business interruption losses from a major Internet outage.

"Business interruption losses from a major Internet outage are very difficult to model and could possibly impact all policies on a portfolio," he said. "We consider it noninsurable and therefore exclude it from reinsurance cover," Mr. Schlayer said.

However, computer virus exposures are insurable, as they can be modeled with a probabilistic model, he added.

It is likely that reinsurers and insurers soon will require more due diligence on outsourcing and the security of providers, as a condition of cover, said Mr. Beeson. "A big data breach of a cloud provider would likely be a game-changing event for insurers," he said.

Cloud computing is comparable to supply chain risks for property business, said Mr. Schlayer. "It is possible that a number of policyholders could be affected by one event at a single cloud provider," he said.

As yet cloud computing is not a problem, but reinsurers are watching to see how the sector develops, said Mr. Schlayer.

"It will be interesting to see the impact of rising losses on capacity and the number of players in years to come," said Mr. Andrews.

Business Insurance[®]

Cyber risks 2012

Business Insurance[®]
Insights
to Solutions

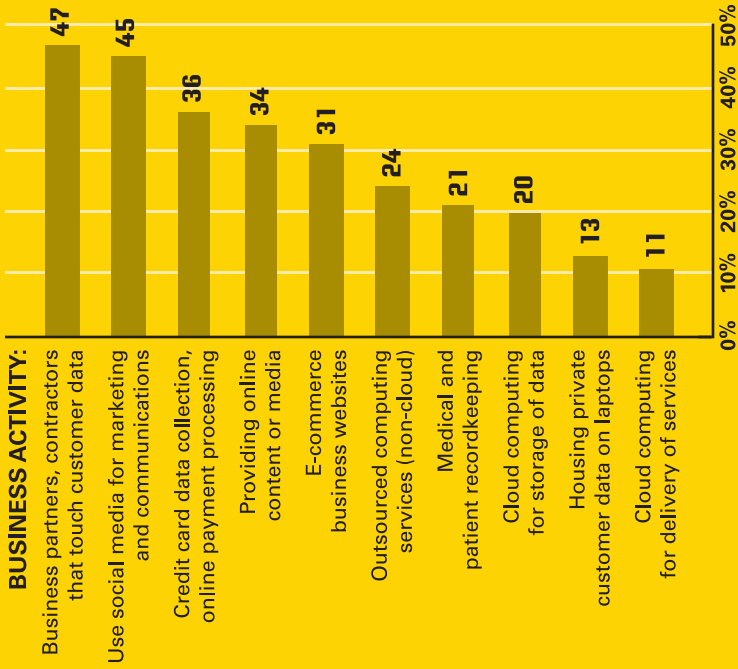
Sponsored by:

CHARTIS[®] 
Your world, insured
www.chartisinsurance.com

Cyber risk exposures and costs have risen significantly in the past five years.

CYBER RISK EXPOSURES

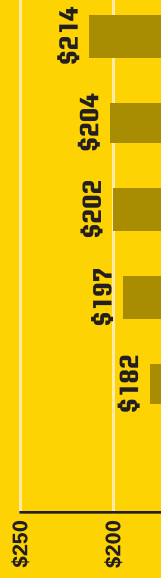
Percentage of companies engaged in activities associated with cyber risks



Source: BI Survey

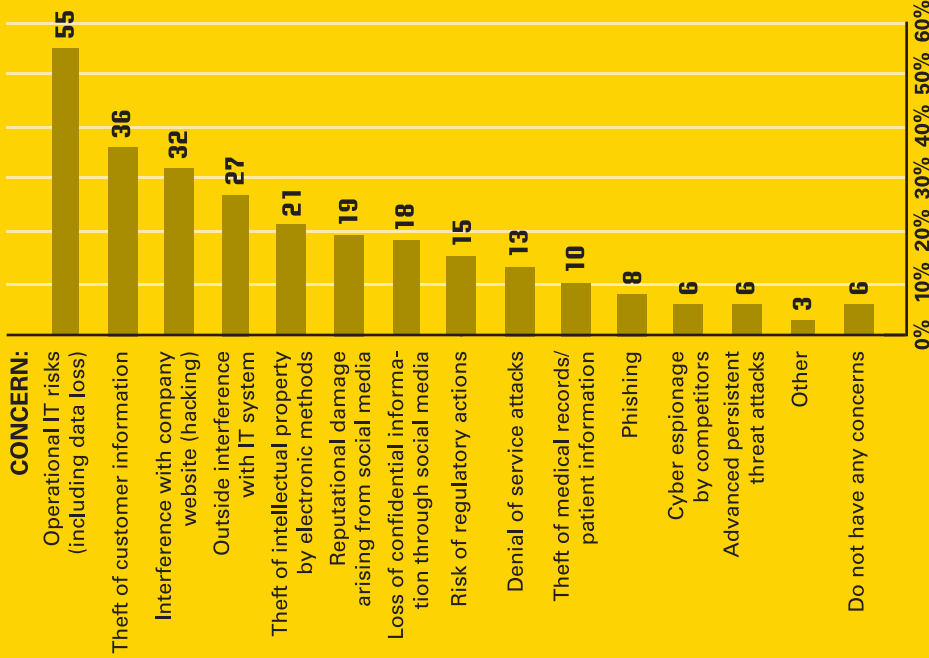
RIISING COSTS PER RECORD

Average cost per compromised record



CYBER RISK CONCERNS

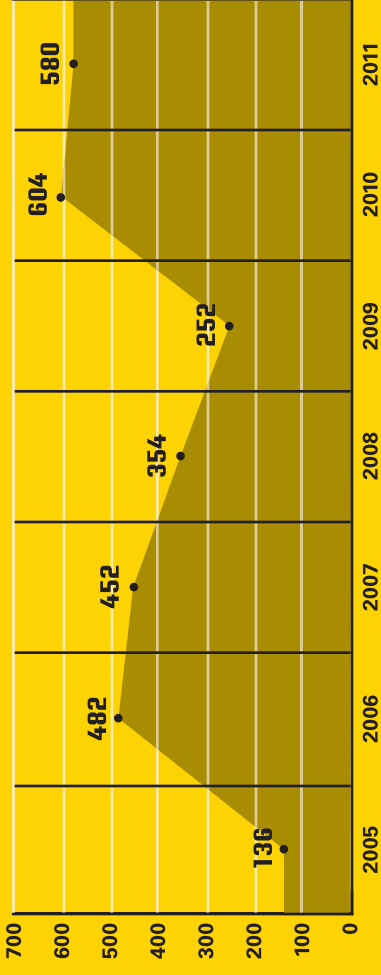
Based on percentage of respondents citing top 3 concerns



Source: BI Survey

DATA BREACH FREQUENCY

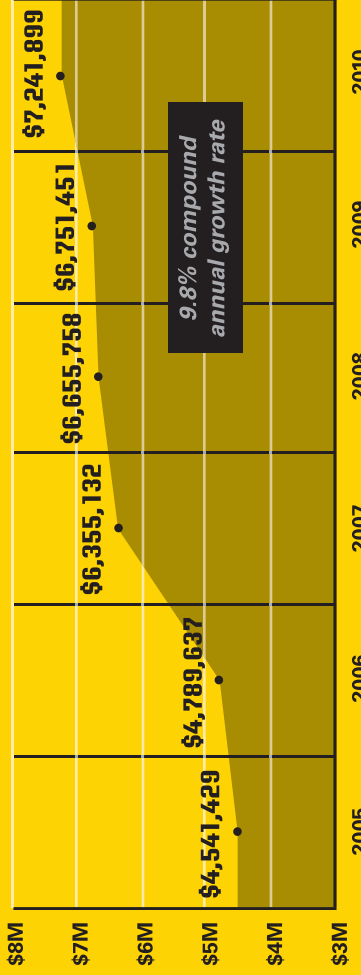
Reported number of data breaches involving personal data



Source: Privacy Rights Clearinghouse

DATA BREACH SEVERITY

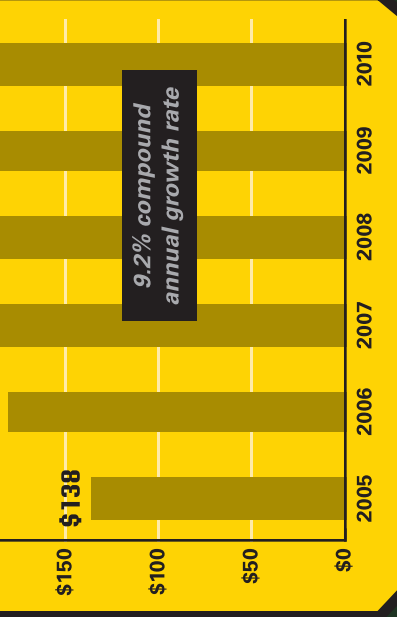
Average organizational cost of a data breach involving personal data



Source: Ponemon Institute L.L.C., U.S. Cost of a Data Breach, sponsored by Symantec Corp.

COSTS VARY BY METHOD OF ATTACK

Average annualized cybercrime cost weighted by attack frequency



Source: Ponemon Institute L.L.C., U.S. Cost of a Data Breach, sponsored by Symantec Corp.

Few companies insure themselves against cyber risks

BUYING CYBER RISK POLICIES

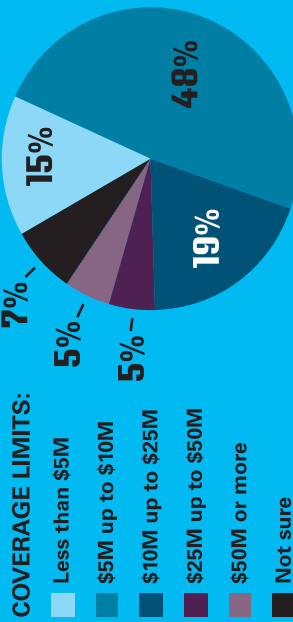
Do you buy stand-alone cyber risk insurance?



Source: BI Survey

CYBER RISK COVERAGE LIMITS

Total coverage limits of stand-alone cyber risk insurance purchased



Source: BI Survey

crain

Produced by the *Business Insurance* Research Department and published in the March 19, 2012, issue of *Business Insurance*, available exclusively to print subscribers. Limited copies of the issue are available for single copy sale via Crain Communications Customer Service, customerservice@businessinsurance.com, or 877-812-1587. This document and information contained therein is the copyrighted property of Crain Communications Inc. and *Business Insurance* (© Copyright 2012) and is for your personal, non-commercial use only. You may not reproduce, display on a website, distribute, sell or republish this document, or the information within, without the prior written consent of *Business Insurance*. Poster design by David Blum, www.InfoMonkeys.com

SPONSORED BY:



CHARTIS
Your world, insured
www.chartisinsurance.com

TYPE OF ATTACK:	2010	2011
Denial of service	*	\$187,506
Web-based attack	\$143,209	\$141,647
Malicious code	\$124,083	\$126,787
Malicious insiders	\$100,300	\$105,353
Phishing and social engineering	\$35,514	\$30,397
Stolen devices	\$25,663	\$24,968
Botnets	\$1,627	\$1,727
Malware	\$1,090	\$1,579
Viruses, worms, trojans	\$2,064	\$1,517

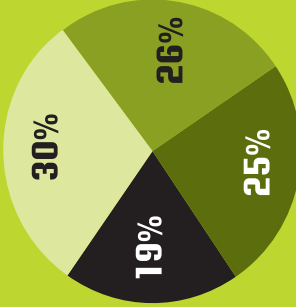
* Not included in 2010 survey

Source: Ponemon Institute L.L.C., Second Annual Cost of Cyber Crime Study

Internal corporate efforts to prevent cyber risk exposures

DATA PROTECTION STRATEGIES

How companies characterize their approach to cyber risk management

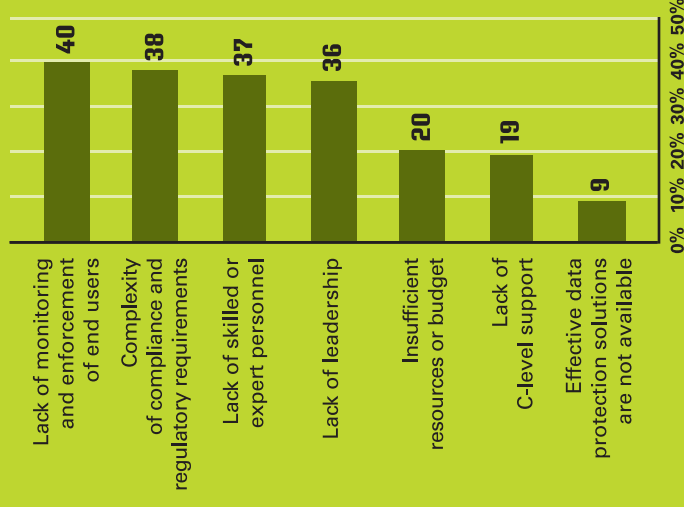


- We have an informal strategy
- We have a formal strategy, but it is not implemented across the enterprise
- We do not have a strategy
- We have a formal strategy that is deployed across the entire enterprise

Source: Ponemon Institute L.L.C., Best Practices in Data Protection

BARRIERS TO EFFECTIVE DATA PROTECTION

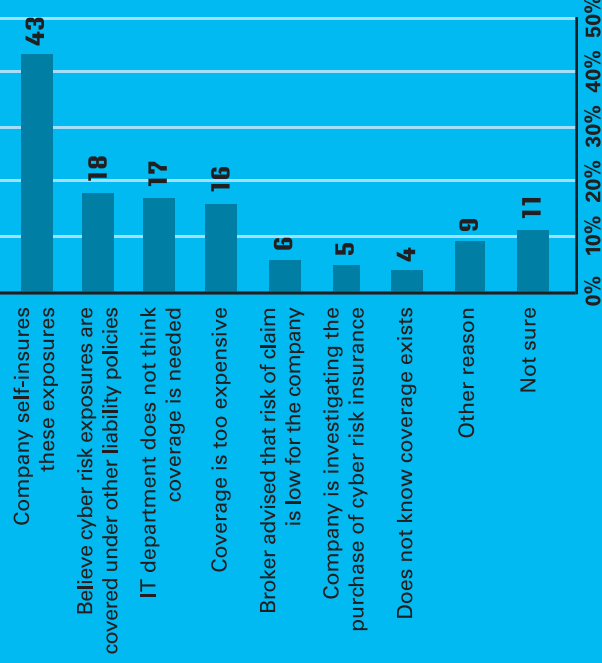
Risk and IT professionals cite most significant barriers in achieving effective data protection



Source: Ponemon Institute L.L.C., Best Practices in Data Protection

WHY NOT BUYING STAND-ALONE CYBER RISK INSURANCE

Reasons for not purchasing stand-alone cyber risk insurance



Source: BI Survey



FOLLOW OPPORTUNITY

wherever it leads.

**Chartis will be
there with you.**

Our global workforce serves clients in over
160 countries and jurisdictions, providing
local expertise with unmatched international
perspective. Let us do the same for you.

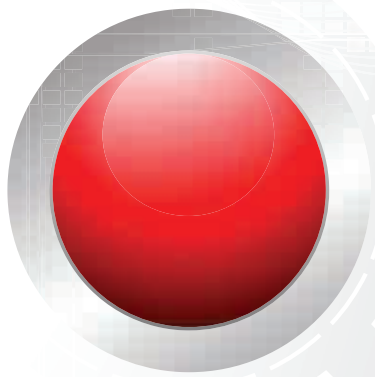
Learn more at www.chartisinsurance.com

CHARTIS 
Your world, insured

All products are written by insurance company subsidiaries or affiliates of Chartis Inc. Coverage may not be available in all jurisdictions and is subject to actual policy language. For additional information, please visit our website at www.chartisinsurance.com.

Special Advertising Section to

Business Insurance®



CYBER LIABILITY INSURERS & SERVICES

Cyber liability is one the most rapidly growing areas in the insurance and risk management sector. While Internet-based commerce is expanding the reach of organizations, allowing greater interaction between customers and vendors, and providing numerous operational efficiencies, there are significant security concerns that organizations must address.

Any organization that uses the Internet has to be aware of the threat of hacking and put security measures in place to reduce the likelihood of their systems being hacked. But it's not just hackers that can jeopardize a company's operations; several of the most widely publicized computer security breaches have been traced to lost or misplaced hardware, such as a flash drive or laptop.

And when data is lost, there are often severe consequences both in terms of reputational damage and direct financial losses.

Given the complexity of the issue, cyber security can no longer be viewed as simply an information technology issue. Several departments within an organization, including risk management, have to play a role in any sophisticated security plan.

In addition, outside vendors, such as security consultants to help reduce the risks and insurers to help address the financial costs, often are brought into support internal efforts.

The following pages contain information on various companies offering services that support organizations in their efforts to control their cyber exposures.

For more information on advertising in all our Business Insurance Custom Guides, contact 312-649-5224.

ID Experts

www.idexpertscorp.com

Data Breach Trends that Threaten Your Business

Data breaches are costing businesses billions of dollars a year. Industries with large volumes of high-value data—bank accounts and medical records to name a few—are particularly vulnerable to data breaches. Thieves value “big data” for its profit potential—often reselling it to other thieves or using it in multi-million-dollar fraud schemes.

Several trends are contributing to the increased growth in the number and complexity of data breaches:

1- Hacking. Hacking is nothing new. But what is troubling are the increasingly sophisticated techniques hackers are using like “social engineering” to break into networks. Hacking attacks have hit a five-year all-time high as a cause of data breaches, according to the Identity Theft Resource Center’s 2011 Breach Report.¹

2- Growing dependence on third-party providers. Economic realities are causing companies to outsource many of their functions, such as billing, to a business partner or provider. Unfortunately, the more parties with access to privacy data, especially when outsourced externally, the more likely a data breach will occur.

3- Taking data to the cloud. To offset computing expenses, many organizations are moving applications and data processing to third-party cloud providers. Storing data outside a company’s own security network, however, creates an additional risk factor outside your direct control.

4- Using mobile devices for business. Many organizations are incorporating mobile devices, like tablets, into their every-



day practices. To save money and to simplify life for employees, companies are allowing the use of personal devices to store or process sensitive corporate data. The portable and less secure nature of mobile devices makes them and their data, all too easy to steal or lose.

Economic realities and technological advances have forever changed the way companies amass, use, and store their biggest asset—data. The increased dissemination of data to more people in less-secure environments puts that asset at risk for exposure.

ID Experts understands the data breach risks that businesses face. We know firsthand how data breaches occur, how best to assess breach risks, and how to prepare a response that delivers the most positive outcomes.

ID Experts is the leader in comprehensive data breach solutions that deliver the most positive outcomes before, during and after a data breach.

Let ID Experts Help Reduce Your Risks of a Data Breach

**Complete Data
Breach Care
by ID Experts
provides positive
outcomes.**



The chances that your organization will experience a data breach have never been greater. New technologies and the dissemination of more data into less-secure environments put your company’s sensitive data at risk for exposure. And with the legal, reputational, and financial harm a data breach can cause, it takes an expert to manage the risks and mitigate the damage.

For years, ID Experts has helped companies understand their data breach risks, protect their data, and manage their response to a privacy incident. ID Experts works in collaboration with top insurance carriers, brokers and breach coaches (lawyers) to ensure a seamless breach prevention and response process for clients. Some of our solutions include:

1- Professional risk assessment. The cost of a risk assessment is less than 1% of the average cost of a data breach. ID Experts’ risk assessments by CIPP-certified professionals provide insight into the risks associated with the confidential information your company uses, makes recommendations on policies and procedures, and outlines best practices on managing privacy data to reduce your business’s exposure to a data breach.

2- Breach preparedness. Despite the best precautions, data breaches do occur. But having a strategic plan in place can reduce the impact of a data breach on your business and your customers. ID Experts will help you develop a ready-to-execute Incident Response Plan that guides you through all phases of a data breach response—minimizing risk to your business and your customers.

3- Breach response. When a data breach hits, you need fast, strategic action. Rely on ID Experts to manage all aspects of a data breach response: forensic investigation; notification to affected customers, regulators, and the media; and identity monitoring and recovery. Use ID Experts’ unique software tool (RADAR) to assess incident risks and state and federal laws and regulations.

By reducing the risk of a data breach, ID Experts’ breach preparedness and response solutions may help lower your premiums on cyber insurance coverage. But whether or not you choose cyber insurance, you can depend on ID Experts to deliver the best value for your data breach investment.



WHAT WE DO

ID Experts is the leading provider of comprehensive data breach prevention and response solutions.

EXPERIENCE

Founded in 2003, ID Experts has managed hundreds of data breach incidents for leading healthcare organizations, corporations, financial institutions, universities, and government agencies across the United States.

INDUSTRIES WE SERVE

- Healthcare
- Government
- Education
- Enterprise
- Financial
- Retail/Consumer

PROFESSIONALS WE TARGET

- Compliance
- Privacy
- Risk Management
- Information Technology
- Security
- Legal
- Finance

BREACH PREVENTION:

- Privacy and Security Risk Assessments
- Policy and Procedure Compliance
- Incident Response Plans
- RADAR – Online Incident Assessment Tool

BREACH RESPONSE:

- Forensics Investigations
- Breach Notification and Call Center
- Crisis Communications
- Identity Monitoring & Restoration

CYBER INSURANCE

ID Experts is a preferred vendor of data breach services for many major insurance carriers.

INDUSTRY AFFILIATIONS

- ANSI/IDSP (Identity Standards Panel)
- Internet Security Alliance
- International Association of Privacy Professionals (IAPP)
- HCCA (Health Care Compliance Association)

ENDORSEMENTS

ID Experts’ Data Breach Preparedness and Response services are endorsed by the American Hospital Association.

CONTACT

Jeremy Henley
Insurance Solutions Executive
760.304.4761
jeremy.henley@idexpertscorp.com

1. http://www.idtheftcenter.org/artman2/publish/headlines/Breaches_2011.shtml



Your antidote for **data breach strain** is here - **Complete Data Breach Care by ID Experts**

Customer churn. Reputational harm. Legal fees. Lawsuits. Data breaches affect every aspect of your business. With so much on the line, you need the help of experts to help mitigate your risk for a data breach — and lessen the impact when a data breach happens.

ID Experts Complete Data Breach Care can help you and your organization achieve positive outcomes

before, during and after a data breach. Our unrivaled combination of experience, resources, and proprietary tools for business — our ID Expertise — delivers solutions that best protect your company and the customers that you serve.

Don't go it alone — call ID Experts. We're your partner in data breach prevention and recovery.

Experience a less painful recovery from data breach.

Visit **www.idexpertscorp.com** today.



ACE USA

www.acegroup.com/us

ACE Privacy and Network Security Coverage

Today every organization uses technology to deliver its products and services, and any company can be affected by a breach of sensitive customer or employee information. In our privacy conscious world, the loss of a single laptop can turn into a public relations disaster—with the potential to damage the organization's brand and balance sheet.

Policies Address Industry-Specific Needs

Each organization is unique, and technology risks can vary greatly from company to company. In response, ACE has designed a full line of privacy, network, media and technology error and omissions products to address the distinct risk transfer needs of different industries. ACE DigiTech® is designed for technology companies and provides integrated errors and omissions, privacy, network security and media coverage, while ACE Privacy Protection® provides privacy, network security and media coverage for companies in all industries.

Value-Added Loss Mitigation Program

ACE's privacy and network security products go beyond risk transfer coverage and include access to ACE's Privacy and Network Security Loss Mitigation Program. This broad-based, flexible risk management system provides a state-of-the-art loss mitigation portal, support from an ACE Data Breach coach and specialists, network security assessments and other claim benefits and services. We recognize that it may not be possible for organizations to completely eliminate the possibility of a data breach or network security failure. However, the ACE Privacy and Network Security Loss Mitigation Program can help organizations reduce the likelihood of these incidents,



Michael Tanenbaum
Senior Vice President
ACE Professional Risk



Toby Merrill
Vice President
ACE Professional Risk

mitigate the loss from an event and proactively develop a strong defense for any ensuing regulatory or legal actions.

Underwriting and Claims Handling Expertise

Experience counts when structuring policy language and settling complex claims. ACE underwriters understand the nuances in the specialty areas they serve and work to provide appropriate, cost effective approaches that consider all of a company's activities. Following an insured event, ACE claims managers work with clients to manage the litigation process to a satisfactory conclusion.

With a proven track record of providing capacity, financial security, expertise and service, ACE Professional Risk creates valuable insurance programs so companies can focus on what matters most—running a successful business.

ACE Professional Risk, a division of ACE USA, is staffed by a specialized team of innovative underwriters and provides management liability, professional liability and surety products throughout the U.S.

Does Your Data Breach Policy Offer Choice?

Choosing an insurance policy to address your organization's privacy, data and network security exposures can be difficult. There are dozens of insurance carriers offering "privacy", "network" or "cyber" policies and endorsements to address both first and third party exposures. But are all these options created equal? Quite simply, no. Just as you need to read the ingredient labels on the food you purchase, it is important to understand the terms and conditions of the policy to truly understand the coverage provided.

One key area of focus is the data breach expense fund. This insuring agreement covers expenses incurred in responding to a data breach event. At a minimum, these policies should cover the expense of retaining a computer forensics specialist, a law firm to determine compliance with privacy regulations, firms to notify and provide credit monitoring services to affected individuals and a public relations firm to restore the company's reputation.

Drilling deeper into the coverage "ingredients", it's also important to understand the conditions to coverage. For

instance, does the carrier require prior written consent before incurring costs to remediate an event? If so, similar to a primary care physician in a health management organization (HMO), the carrier will serve as a gatekeeper to covered services. Failure to obtain prior written approval may result in a denial of coverage. Also similar to an HMO, some policies require the use of a dedicated vendor — leaving you with no choice on the provider handling the data breach response. When making a purchasing decision, this lack of choice and control may seem acceptable. However, in the face of a data breach, it could mean the difference between a well managed response with favorable interaction with your customers and significant legal expenses with lingering reputational damage.

Just as you want to maintain control in selecting the best physician for you and your family, you should also want the same choice in selecting vendors that will handle your organization's response to a data breach. It's important to "read the label" and know what you're buying. This knowledge could help preserve your organization's reputation — and balance sheet.



insuring progress®

What We Do

ACE Privacy Protection: Coverage for privacy liability from lost computer equipment, network security breaches, human errors – including mistakes by third party service providers.

ACE DigiTech: Professional liability coverage for your technology products and services and state-of-the-art network security and privacy liability protection for sensitive data hosted on your systems.

Who We Target

ACE Privacy Protection:

- Businesses managing sensitive customer or employee information, third party corporate information, computer network or website
- Targeted classes include retail, financial institutions, healthcare

ACE DigiTech:

- General technology service providers
- Hardware, software, systems architecture consultants/integrators
- Application service providers
- Data processors
- Software developers

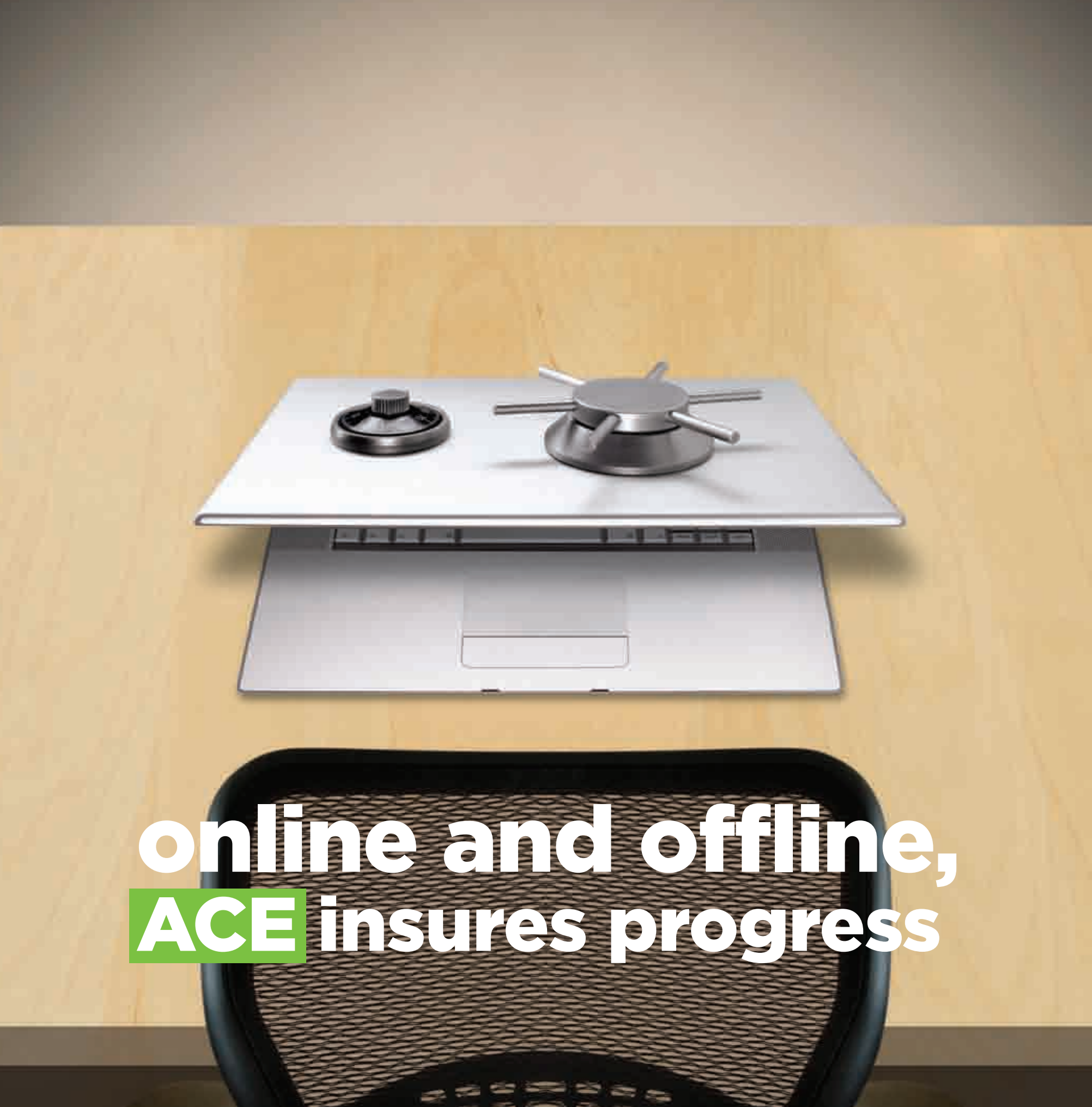
Policy Highlights

- Covers wrongful acts of insured and its service providers
- Privacy coverage includes:
 - personal information in any format
 - breaches not restricted to network event
 - customer and employee information
- Free access to eRisk Hub® loss prevention website and resources to manage privacy and network risk
- Data Breach Team access with pre-negotiated, discounted rates
 - independent specialists in legal, computer forensic, notification, call center, public relations, fraud consultation, credit monitoring and identity restoration
 - multiple vendors in most service categories
- Data breach expenses include voluntary notification and expense of complying with consumer notification provisions of applicable jurisdiction that most favors coverage
- No retention, coinsurance, prior written approval or post-discovery time restrictions for Data Breach Fund (voluntary notification subject to prior written approval)

Contact

ProfessionalRiskEOPProducts@acegroup.com

For additional information and resources, including podcasts on how to prepare and respond to data breaches, please visit: <http://www.acegroup.com/us-en/businesses/privacy-network-security.aspx>.



online and offline, **ACE** insures progress

Property & Casualty | Accident & Health | Life

To address complex privacy issues, it takes the right people, a strong balance sheet, global capabilities, and a flexible approach. These are the strengths of ACE that allow us to offer a suite of products and services designed to address a broad range of technology, network security, privacy and data breach risks. We take on the responsibility of your risks so that you can take on the responsibility of making things happen. We call this *insuring progress*. Visit us at acegroup.com/us



insuring progress®

SELECTIVE®

www.selective.com

In the rapidly evolving age of cloud computing, email, and smart phones, conducting business electronically is the norm. But if your company experiences a cyber loss, will you be prepared to deal with it?

According to a 2011 survey conducted by Ponemon Institute, organizations both small and large have experienced multiple electronic security breaches, with more than half (59%) of the respondents citing two or more breaches had occurred in the last 18 months.¹ Even more concerning, as of October 2011 small businesses (companies with less than 500 employees) accounted for an astounding 40% of all targeted cyber attacks, with an average cost equating to \$188,242 per occurrence.² With staggering statistics like this it's no wonder that 60% of small businesses close just after 6 months of a cyber attack due to the un-planned and un-protected expenses that arise.² The rate and frequency of cyber attacks continue to increase; and unfortunately the businesses that are being targeted, are the ones who typically have limited resources in place to efficiently protect themselves.²

It's for these reasons that businesses need to think about securing Cyber Liability protection, like CyCurity® from Selective. Not many companies can afford to invest hundreds of thousands of dollars building a state of the art secure computer network – but most organizations can invest in cyber coverage with premiums starting as low as \$175.

Selective's CyCurity® offers three coverages (electronic media liability, electronic information security liability, and security breach expenses) designed specifically to help pro-



tect an organization from cyber losses. This protection helps reimburse you for expenses, such as notification and case management required by state and federal law following the compromise of your customers' personal information. In addition, it provides defense and costs of damages for 3rd party cyber incidents resulting from using the internet and other electronic means to communicate and transact business. A few loss examples include intellectual property infringement, a posting on your web site that defames a person or business, or failing to protect personal information of customers. While these examples are only a few of the many benefits afforded with CyCurity® from Selective, they help illustrate the value this type of coverage can provide to an organization. With the cost of cyber crimes in excess of \$114 billion annually², it's more important than ever to put in place proactive measures to help protect your future today.

¹ <http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf> ² <http://www.homelandsecuritynewswire.com/80-us-small-businesses-have-no-cyber-security-policies-place?page=0,0>

 **SELECTIVE®**
Response is everything.

The insurance you receive is only as good as the company behind it. Selective has been providing great products and great service for agents and consumers since 1926. In addition, Selective has achieved an "A+" (Superior) financial strength rating from A.M. Best for the past five decades.

Offering a broad range of commercial, personal, alternative market and flood insurance programs, Selective provides a comprehensive suite of coverages to meet customers' unique needs.

At Selective, Response is everything®....We understand the value in the ease-of-doing business and that timing is crucial and communication is key. That's why Selective has robust technology and fully empowered employees who are able to make decisions on the spot. Our agents and customers can trust us to be there when they need us because we know...Response is everything.®

For more information, please contact Adam Irish, Selective Technology Business Segment Manager at (800) 777-9656 ext. 1584 or adam.irish@selective.com.



**When it comes to insurance,
Selective understands
the value in the
ease-of-doing business.**

That's why our dedicated team of experts are committed to providing great products and great service in response to your ever-changing needs.

You can trust us to be here when you need us because we know...Response is everything.®

 **SELECTIVE®**
Response is everything.
www.selective.com

Cyber liability market taking off with insurers

By MIKE TSIKOUDAKIS

The cyber liability insurance market has seen rapid growth in capacity, with new entrants creating a buyers' market by increasing competition for premium dollars.

There are approximately 30 primary insurers offering cyber liability coverages, with available capacity at \$250 million to \$300 million, industry experts say.

Just five years ago, capacity was at about \$100 million, with five or six insurers in the space, said Kevin Violette, senior broker at OakBridge Insurance Services L.L.C., in Bloomfield, Conn.

Today, cyber liability is a major growth area for insurers, said Peter Foster, executive vp of Willis North America's executive risks group in Boston. "Every insurer I talk to said that this is their No. 1 growth product within the organization," he said.

"The professional liability pie hasn't grown any bigger over the past three or four years with the problems with the economy," said Brad Gow, vp of professional lines insurance at Endurance Specialty Underwriters, a unit of Endurance Specialty Holdings Ltd. in Stamford, Conn. "The one consistent area of growth in the professional liability space is cyber."

While cyber liability coverages emerged in the late 1990s, they addressed computer security issues (see related story). But now, insurance buyers frequently seek coverage because of data breach-related privacy concerns, which have grown dramatically amid an increase in cyber crime and the proliferation of notification laws and regulations in the United States and overseas, cyber insurance experts say.

The take-up rate on stand-alone cyber coverage is about 30%, said Larry Racioppo, Stamford, Conn.-based executive liability practice leader at Towers Watson & Co. "So when you figure that 70% of firms do not buy network security and privacy, I think the opportunity is there to really try to get some of that 70% that don't buy and try to

develop some market share for your product," he said.

As broad soft-market conditions during the past five years have depressed other lines of business, carriers are entering the cyber liability space to increase their market presence and overall book of business, Mr. Violette said.

"Whenever carriers can round out their risk profile and get themselves in good with a client, it just solidifies their relationship in being able to offer this coverage, which almost is a necessity at this point," he said.

Some of the newer players in the cyber liability market are traditional property/casualty under-

MARKET FORCES

Insurers increasingly are competing for cyber liability business:

- About 30 insurers offer coverage
- \$250 million to \$300 million in capacity available
- Scope of coverage expanding

writers, said Willis' Mr. Foster. "It's sort of pushed those traditional markets to enter a market that they might not feel they have enough actuarial data around their underwriting, but feel like they have to get into or they're going to lose business in the process," he said.

Travelers in June 2011 launched a cyber policy that includes third-party liability and first-party coverages such as network and information security liability, regulatory defense expenses, crisis management event expenses and security breach remediation, among others, according to a statement.

Endurance Specialty Underwriters began offering cyber liability coverages in February, Endurance's Mr. Gow said.

"It's something that if we wished to grow, we felt we needed to get into," he said, noting that Endurance can offer \$20 million in capacity and operates on a primary and excess basis.

Hacker insurance evolves into 21st century

By MIKE TSIKOUDAKIS

In the beginning, there was hacker insurance.

At an event in 1997, Emily Freeman, then working for broker Sedgwick Group P.L.C., met individuals from IBM who provided computer security best practices for organizations' network-based computer services and wanted to somehow link up with the insurance industry.

"At the time, there were professional liability policies for technology companies, but there really wasn't a policy that would work for someone who wasn't a Web developer or a technology company," Ms. Freeman said. "So we entered into a project to create one."

The policy, Net Secure, was written as a cooperative effort with IBM and went on to define terms such as denial-of-service attacks and malicious code.

"This wording was accepted, and capacity was backed by a syndicate in Lloyd's and two U.S. insurers," which were American International Group Inc. and a unit of Zurich Financial Services Corp., said Ms. Freeman, who now is executive

director of the technology and global privacy group at Lockton Cos. L.L.P. in London.

Net Secure was completed in 1998 and was in the market in 1999, providing civil liability coverage, crisis management costs and regulatory coverage, Ms. Freeman said.

While there was early interest from retailers and financial institutions, there weren't many buyers, she said.

Brad Gow, vp at Endurance Specialty Holdings Ltd. in Stamford, Conn., created one of the first first-party cyber forms that covered hacking, viruses and business interruption during his time at CIGNA International.

The insurer in 1998 released CIGNA Data Guard, which was known as "hacker insurance" and was predominantly purchased by technology companies that understood the threat, Mr. Gow said.

In developing the coverage, Mr. Gow and his team worked with IBM to assess the spectrum of known cyber risks, dividing the threats between first-party and liability threats. At the time, liability threats "were almost purely theoretical, because there

was a lot of confusion around whether or not (general liability) forms covered threats arising out of third-parties being harmed by your system being hacked," Mr. Gow said.

"Insurance carriers had so much trouble getting their arms around it, the natural inclination was to look for reinsurance support," Mr. Gow said. "And the reinsurers, at that point, knew even less than we did and were characteristically concerned with systemic threats...that could aggregate through an individual carrier's portfolio and their own portfolio if they were working with multiple carriers."

"In the beginning, just that computer security piece was scary," said Nick Economidis, Philadelphia-based underwriter at Beazley Group P.L.C.

Mr. Economidis said computer security expert assessments would cost \$10,000 to \$20,000, and was built into the premium.

"So it was very expensive coverage for a long time and it was very limited coverage," he said. "Over time we certainly figured out how to underwrite it better and more efficiently."

The frequency of liability arising out of data threats is lower than the actual losses of the data itself, which has forced insurer innovation to economically tackle those costs and expenses, Mr. Gow said.

"A company that is relatively new to the market like Endurance has to work extra hard to break in and come up with some novel approaches toward handling these exposures," Mr. Gow said.

New entrants in the cyber liability market also are fueling greater competition, the benefits of which are trickling down to the

insurance buyers in the form of lower rates, combined coverages and streamlined application forms, experts say.

"There's a lot of demand among the broking community for a product that isn't just the same as all the others, but really simplifies and makes accessible the type of coverage that clients are increasingly demanding," according to Oliver Brew, vp of miscellaneous professional liability and technology errors and omissions for Liberty International Underwriters.

The specialty insurance unit of

Liberty Mutual Group Inc. in February rolled out three cyber policies that focus on common threats to companies, including data privacy breaches and technology E&O.

"We're fulfilling a need in the market by combining some of the E&O coverages with the privacy coverages," he said.

Insurance buyers can now combine all of their cyber exposures under one form, where traditionally insurers used separate forms for first-party and third-party liability exposures, Mr. Violette of OakBridge said.

Range of liability policies provide some coverage for data risks

By RUSS BANHAM

In this era of costly data breaches and subsequent reputational damage, many organizations rely on cyber risk insurance, which provides a range of first-party and third-party coverages. Yet, there are other insurance policies that also absorb some of the same exposures that cyber risk insurance addresses.

Among these are errors and omissions liability, comprehensive general liability, and media liability. Each of these policies contains language potentially

picking up some cyber-related losses, although the devil is in the details. Certain conditions must be met in each case for the policies to respond to a loss.

Another downside to these policies absorbing cyber perils is the financial limits of the insurance they provide, as a single data breach may erode financial limits of protection needed to absorb the losses the policies customarily cover.

Despite the modicum of cyber protection the policies may address, the message is clear—don't rely exclusively on them to

absorb an exposure as potentially devastating as cyber risk. As Ken Goldstein, vp at Chubb Group of Insurance Cos. in Warren, N.J., puts it, "The most comprehensive way to address cyber risks like unauthorized access or virus transmission is through cyber liability insurance."

Nevertheless, because each of the aforementioned policies may possibly absorb elements of cyber risk, the goal is to assess all the policies from a holistic standpoint, with an eye toward integrating them to afford the broadest protection.

E&O and other professional liability policies overlap with cyber policies in terms of covering negligence-related losses.

"If I'm rendering a service to someone and cause them to be vulnerable to being hacked, I can be sued for negligence," said Robert Parisi, senior vp and cyber practice leader at New York-based broker Marsh Inc. "In this regard, there would be third-party protection much like that afforded in a cyber policy."

Mr. Parisi cited software providers, security companies and payment processors as

examples of insureds that may find some protection. "Say I'm a payment processor and I enable retailers to take credit cards, and then I lose the personally identifiable information that these retailers have sent me about their customers," he said. "State law requires the retailer to notify affected individuals and possibly provide credit monitoring. Since I was negligent, the retailer can sue me for the expenses it incurs, which would be covered under my E&O policy."

See **POLICIES** next page

BI Classifieds

To place your ad, contact Monique Murray 212.210.0129 • E-mail: mmurray@BusinessInsurance.com

Business Insurance, Classified Department, 711 Third Ave., New York, NY 10017-4036
Call for details on print and internet advertising

LEGAL NOTICE

IN THE MATTER OF THE CONSERVATION OF THE TRUST FUNDS OF UNITED CAPITOL INSURANCE COMPANY
Supreme Court of the State of New York
County of New York
Index No.: 401784/02
NOTICE

Pursuant to an order of the Supreme Court of the State of New York, County of New York ("Court"), entered June 14, 2002 ("Conservation Order"), the then-Superintendent of Insurance of the State of New York and his successors in office were appointed as conservator ("Conservator") of a certain trust fund ("Trust Fund") of United Capitol Insurance Company ("United Capitol") and, as such, has been directed to conserve funds in the Trust Fund pursuant to Article 74 of the New York Insurance Law ("Insurance Law"). The Superintendent of Financial Services of the State of New York has now succeeded the Superintendent of Insurance as Conservator of United Capitol. The Conservator has, pursuant to Insurance Law Article 74, appointed Jonathan L. Bing, Special Deputy Superintendent ("Special Deputy"), as his agent to carry out the responsibilities of the Conservator, through the New York Liquidation Bureau ("Bureau"), 110 William Street, New York, New York 10038. The Conservator, by the Special Deputy, has submitted to the Court a verified petition ("Verified Petition") seeking an order: (a) approving the conservation agreement ("Conservation Agreement") executed on October 14, 2011, a copy of which is annexed to the Verified Petition as Exhibit 1, by and between Andrew R. Stolfi, Acting Director of Insurance of the State of Illinois, as liquidator ("Liquidator") of United Capitol and the Conservator; (b) authorizing the Conservator to distribute the Trust Fund to the Liquidator in accordance with the terms of the Conservation Agreement; (c) releasing and discharging, upon distribution of the assets in accordance with the terms of the Conservation Agreement and the filing of a final report, the Conservator, his predecessors and successors in office, their agents, attorneys and employees, from any and all liability arising from their acts or omissions in connection with this proceeding; (d) authorizing the Conservator to take further actions which he, in his discretion, deems advisable for the protection of creditors and of the assets in his possession and for the termination of this proceeding; and (e) providing for such other and further relief as this Court.

A hearing is scheduled on the Verified Petition on the 5th day of April, 2012, at 2:30 p.m., before the Honorable Joan A. Madden, JSC, New York Supreme Court at the Courthouse, IAS Part 11, Room 351, 60 Centre Street, New York, New York 10007. If you wish to object to the Verified Petition, you must serve a written statement setting forth your objections and all supporting documentation upon the Conservator and Clerk of the Court, at least fifteen business days prior to the hearing. Service on the Conservator shall be made by first class mail at the following address:

Superintendent of Financial Services of the State of New York as Conservator of United Capitol Insurance Company
110 William Street
New York, New York 10038
Attention: John Pearson Kelly
General Counsel

By filing the Verified Petition, the Conservator is seeking the approval of the Conservation Agreement from the Court. The Verified Petition and supporting papers are available for inspection at the above address. In the event of any discrepancy between this notice and the documents submitted to Court, the documents control.

Requests for further information should be directed to the Bureau's Legal Division at (212) 341-6755.

Benjamin M. Lawsky
Superintendent of Financial Services of the State of New York as Conservator of United Capitol Insurance Company

Mark your Calendar...

Industry Financials, Year-End Results: Revenue/Profiles of Leading Companies

Publishing: March 26
Classified Ad Close: March 20

RIMS Conference Review

Publishing: April 2
Classified Ad Close: March 27
Bonus Distribution: RIMS

Contact Monique Murray at 212-210-0129 For Details

TAKE FULL ADVANTAGE OF YOUR RESOURCES!

In Print...



and Online



Contact Monique Murray @ 212-210-0129 for details

Business Resources

CLAIMS SERVICES

DIALYSIS COST Solutions

— CALL —

UNICUS Claim Controls, Inc.

1-855-864-2871



You're hired.

Business Insurance CAREER CENTER
The ultimate career resource in the insurance industry.

<http://careers.BusinessInsurance.com>

Policies: Wide range of coverage

CONTINUED FROM PREVIOUS PAGE

The E&O insurance essentially would stand in for the first-party coverages typically provided in cyber risk policies. There is a weakness to this scenario, however. "It has to be tied to negligence," Mr. Parisi said. "If the loss is linked to an intentional act by an employee, it will not be covered. Thus, you have gaps in coverage, which is why you would want to have cyber insurance."

Media liability insurance also may absorb aspects of cyber risk. Designed primarily for publishers, broadcasters and content providers, the insurance transfers the risks of libel, slander, defamation, invasion of privacy, and copyright and trademark infringement. Coverage for cyber losses may be found in a media policy for content on a website containing private information that is breached by a third party.

"Say a hospital creates content on its website featuring actual X-rays of patients for teaching purposes," said Tom Srail, a senior vp in the Cleveland office of FINEX North America, the executive risks practice at broker Willis Group Holdings P.L.C. "If the hospital neglected to redact patient information on the X-rays, and this data is breached by an outside party, the media coverage may apply if the patient sues the hospital."

Media liability insurance is a variation of E&O coverage—hence it suffers the same Achilles' heel with regard to absorbing cyber losses. "Again you're dealing with negligence triggers," Mr. Parisi said.

Mr. Goldstein said many newer forms of media liability insurance

Stand-alone coverage offers best data breach protection

Aside from the coverage considerations, another drawback in leveraging errors and omissions liability, comprehensive general liability, and media liability policies for cyber risk is their adverse impact on insurance limits.

"The GL is designed to broadly protect a company's assets if it is sued for causing property damage or personal injury," said Dan Riordan, president, specialty products, in the New York office of insurer Zurich North America. "The limits of financial protection generally are based on risks other than cyber liability. If the policy is then used to absorb a large cyber loss, it may be inadequate to address the many other risks for which it is largely intended."

The other observers shared this view. "We have several newspaper clients who all have decent media liability insurance protection, but we still advise them to purchase stand-alone cyber insurance, which they do," said Tom Srail, a senior vp in the Cleveland office of FINEX North America. "They understand that if there is a big data breach in one year, they run the risk of either eroding the limits or blowing through them."

Robert Parisi, senior vp and cyber practice leader at New York-based broker Marsh Inc., summed up the situation concisely. "My position is that if you're looking for true coverage against a data breach, you need to get data breach coverage."

—By Russ Banham

BACKUP PLAN

These other coverages can absorb some of the same exposures that cyber risk insurance address:

- Errors and omissions liability
- Comprehensive general liability
- Media liability

ance now specifically exclude cyber liability.

Whereas the aforementioned policies may absorb first-party breach notification, credit monitoring, credit restoration, and other expenses, GL policies may pick up third-party cyber liabilities. "The GL is not designed to address first-party types of issues, and frankly many GL car-

riers would take the position that third-party liability wasn't contemplated with respect to cyber," Mr. Goldstein said. "Still, there may be some coverage, the triggers being 'damage to tangible property' and 'personal injury.' The former raises questions over whether or not data is tangible or intangible. Hence, the move by most carriers to do their homework and specifically exclude 'unauthorized access' in the policy."

Mr. Parisi agreed. "We've seen situations in the past where less-than-precise language in a GL policy can be interpreted as providing coverage going forward, even though this was not the underwriters' intent," he said. "Newer GL policies include language that clearly disallows coverage for damage to data."

Risk managers, IT should collaborate

By RUSS BANHAM

One would imagine that risk managers have a tough time conferring with their information technology colleagues to define, assess and manage cyber risks.

But that's not so, according to a handful of risk managers who confide that they routinely and collegially collaborate with their IT counterparts. Given the extraordinary financial exposures that IT creates for enterprises—a data breach can terminally ruin a company's reputation—this is a very good thing.

"I don't recognize from my experience that IT is at all egomaniacal," said Carol Fox, director of the strategic and enterprise risk practice at the New York-based Risk & Insurance Management Society Inc. "In my prior job as risk manager at Convergys (Corp.),

and today as RIMS' risk manager, I've never found IT to be obstructive. Rather, they have been partners in helping me identify, manage and transfer risks."

Ms. Fox, who is the author of RIMS' new report, "ERM Best Practices in Cyber Risk," is far from alone in this view.

"I have no horror stories to report in working with IT," said Carmelo Casella, vp of corporate insurance at New York-based Bank of New York Mellon Corp. "Every year, as I renew our cyber liability policy, I sit down with our underwriter and our data security leader in person, and we follow this up with three to four conference calls a year. He explains our data security improvements to the underwriter, which I could never articulate as specifically, and they both get along splendidly. All in all, it's a productive experience."

This collaboration between risk management and IT depends on a mutual understanding of the organization's technology networks, systems and software applications, and the myriad risks they foster. This can be a collegial experience according to Grace Crickette, risk manager for the University of California (see story, page 27).

The vital need for risk management and IT to work together smoothly and efficiently also was cited by Wayne Salen, director of risk management at Labor Finders International Inc., a West Palm Beach, Fla.-based industrial temporary staffing firm with 100,000 employees. "IT recognizes the gravity of the security risks they, in effect, create, and are more than happy to have someone like me, who focuses on risk and insurance,

See **COLLABORATE** next page

Collaborate: Working with IT

CONTINUED FROM PREVIOUS PAGE

plug the holes," Mr. Salen said. "They're more than receptive to my input."

In Labor Finders' case, proximity has allowed the directors of IT and risk management to collaborate often. "We're peers located in the same building on the same floor, and both report directly to the CEO," Mr. Salen said. "While there is a degree of truth that many IT people aren't particularly communicative or personal, this has not been my experience."

Like Ms. Crickette, Mr. Salen endeavored to understand the business of IT, researching a wide range of security standards put forth by the American National Standards Institute, the International Organization for Standardization and others. In developing the internal IT risk standard at Labor Finders, he said the ISO 31000 Guide 73 proved an invaluable source document. "I'm not an IT expert by any means, but I can talk the talk," he added.

So can Ms. Fox. "It's really all about cross-dialogue—my need to understand IT risks and how IT is managing them, and their need to understand what we're doing insofar as procuring coverages to transfer risks," she said.

Just prior to leaving Convergys, she noted that the risk management team and the IT group partnered to do an enterprise risk assessment of IT. "When the new CIO came in and we provided him the findings, he was so impressed that he asked us to train 300 IT managers on risk management," Ms. Fox said. "Risk management at the time was a staff of four, but we were able to partner with IT in creating a 20-minute online training course."

Ms. Fox said she found that frank questions opened the door to dialogue and real collaboration. "It's not like IT hasn't thought about risks like data breaches—they're just happy to know that we in risk management also think about these things and are there to help."

Risk managers should get acquainted with data security

By RUSS BANHAM

Like other institutions of higher education, the University of California is subject to a variety of unique exposures related to electronic information security and privacy.

With 10 campuses and five medical centers, the university is faced with managing a multitude of systems and endless records of students, faculty, staff and patients. If an outside party hacks into or otherwise steals or corrupts these records for criminal purposes, the university is

financially responsible for notifying victims, monitoring their credit and restoring it, not to mention potential fines, penalties, litigation and reputational reverberations.

Grace Crickette, Oakland, Calif.-based chief risk officer at the University of California, takes these threats seriously.

"The first thing a risk manager must do when collaborating with another discipline like (information technology) is to learn their taxonomy," she said. "A number of years ago, I started subscribing to periodicals on IT to better understand the security

aspects. And I stay involved with the (American Society of Safety Engineers) and the (Institute of Security Executives Inc.). Both organizations welcome risk managers."

Ms. Crickette said she is "utterly fascinated" by the world of IT. She maintains that IT professionals also share a healthy respect for enterprise risk management.

"Our CIO, director of security and I enjoy partnering together," she said. "We're always looking for opportunities to leverage our insurance and self-insurance programs to support IT's goals."

Business Insurance®

SHOW DAILY @ RIMS 2012

Philadelphia April 15 - 18

Get your message in the hands of RIMS attendees

Business Insurance and RIMS are making it easier than ever to reach targeted buyers of risk and insurance products during the 2012 RIMS conference and exhibition in Philadelphia. Business Insurance is the publisher of the official Show Daily of the RIMS conference on Monday, Tuesday and Wednesday of conference week.

With wide distribution at the conference and online you can be sure that your message will reach your targeted audience.

- A PDF of each full Show Daily edition will be available online at BusinessInsurance.com and at RIMS.org
- A link to the Show Daily PDF is included in Business Insurance's daily news emails and conference emails from RIMS

Take advantage of this exclusive opportunity to reach these targeted buyers of risk and insurance products and the full risk management community. Advertise in the official 2012 RIMS Show Daily, published by Business Insurance. Advertising Closing **March 22, 2012.**



For more information, including details about all our media packages, Scan the QR code at left or call 312-649-5224 or email advertising@BusinessInsurance.com

MAKE SURE YOUR
COMPANY/PRODUCT
GET'S NOTICED
SIGN UP TODAY!



ADVERTISER

INDEX

Issue of March 19

ADVERTISER	PAGE #
Ace USA	22/23
ACORD/LOMA	14
Aetna	32
Aon Corporation	2
BerkleyMed	13
Business Insurance	7, 19, 27, 29, 31
Chartis	18
CNA Insurance	11
ID Experts	20/21
Selective Insurance Company of America	24
S.H. Smith & Company, Inc.	12
UNICUS Claim Controls Inc.	26
Zurich North America	5



Business Insurance® www.BusinessInsurance.com
INSIGHTS TODAY FOR THE RISKS OF TOMORROW

Risk managers don't need to be IT experts

By **RODD ZOLKOS**

Most risk managers might not be information technology experts, but they can effectively manage cyber risks by applying their expertise in such areas as contract risks, assessing the value of exposures and communicating the potential impact of exposures across their organizations.

"I'm not an IT expert," said Lee Garvin, director of risk management at JetBlue Airways Corp. in Forest Hills, N.Y. "But what I do see are the contracts, and that's the place that we can do our best to protect our companies, in my opinion."

As companies outsource more and more IT and data processing tasks, a vendor might offer just the technology solution your company is looking for, Mr. Garvin said. But it's important to consider what they are providing in terms of data security and indemnification for losses resulting from any service interruptions or data breaches.

"Some of the products that are out there are absolutely fantastic, but what are they backed up with?" he asked. "How much is the indemnity that's in the contract really worth to you?"

As privacy rules continue to emerge at the state and federal levels, cyber risk management is becoming an increasingly important topic for risk managers and their superiors, said Jim Whetstone, senior vp and U.S. technology and privacy manager for Hiscox Specialty in Chicago. "Hacking events have a much more material effect on the company than they did in the past," he said.

"In the past you could argue that maybe there was a reputation-

al risk," Mr. Whetstone said. "Now risk managers can say there's a direct cost of these events."

Using last year's California Supreme Court ruling in *Pineda vs. Williams Sonoma Stores Inc.* that held that ZIP codes can be considered personally identifiable information in certain cases as an example, "It's really quite a changing time in terms of what's out there in terms of risks and what companies' potential risks and liabilities might be," said Scott N. Godes, of counsel in the insurance coverage practice at Dickstein Shapiro L.L.P. in Washington.

"We now have 46 states with data breach notification statutes. There's pending legislation in Congress," Mr. Godes said. In addition, the U.S. Securities and Exchange Commission has produced cyber security disclosure guidance requiring publicly traded companies to disclose their cyber risks to investors and makes those companies' boards responsible for assessing their exposures and taking appropriate steps to address them, he said.

"Because of the ongoing changes, it's certainly something companies need to be paying attention to," he said.

Mr. Garvin said it's important that risk managers advise others in their organizations about possible exposures as they outsource IT services, informing leaders of such areas as supply chain and procurement and those in the information technology department about the potential exposures and the need to seek indemnification from vendors.

"In the end they might not want to do it, but at least you've let them know what's going on," he said.

As the company seeks those outside partners, "I come up with contractual wording that I've worked out with my brokers and we tell people this is what we want in our RFP," Mr. Garvin said.

"From a risk manager's perspective, the insurance is just one avenue," Mr. Whetstone said. "They need to be talking not only to the IT department but to legal about how to address some of these issues in contracts."

Other people the risk manager should involve in the discussion about cyber exposures vary by organization, he said. "I've been in meetings where a company has brought a dozen or more individuals from various departments, and they've all had something to share," Mr. Whetstone said.

Meanwhile, a knowledgeable risk manager can help other areas of the company address potential cyber exposures.

"The more the risk manager knows about this, the more they may be able to help," he said. For example, the IT department might say it can't afford to encrypt every laptop. But, by citing the potential costs of dealing with a data breach if a laptop is stolen, the risk manager can help

Using a three-step process to tackle cyber liability risks

By **RODD ZOLKOS**

According to one cyber risk insurance expert, there are three basic areas risk managers should consider first as they look to address their organizations' cyber liability exposures.

Jennifer G. Smith, vp in the global technology and privacy practice with Lockton Cos. L.L.C. in Washington, said the first thing she would suggest risk managers do in seeking to manage their information technology-related exposures is identify their organization's relevant internal documents.

"Take a look at the one or two most applicable information security standards to their organization," she said.

In most cases two of those will prove to be ISO 27001 and ISO 27002. Part of a family of information technology security standards published by the International Organization for Standardization, ISO 27001 focuses on risk assessment, while ISO 27002 focuses on best practices recommendations for information security management.

Within their organizations, risk managers also should be able to find some kind of information security policies and practices manual. "Theoretical or otherwise, that's required by a host of different laws," Ms. Smith said.

At a large company, the manual might be a single document updated every few years, she said, while at a mid-size or smaller company it

might take the form of "a series of emails and a flow chart."

"I'm not suggesting every risk manager should read that in its entirety and be able to quote it verbatim," Ms. Smith said. But a risk manager should at least be familiar enough with its contents to be able to refer to it in terms of privacy policy, data breach incident response, and vendor or outsourcing protocols.

"That's the starting point, to understand those three documents," Ms. Smith said.

The second step is for the risk manager to identify the relevant internal stakeholders, she said. "It's really important for risk managers to know who in their organization is responsible for what in terms of IT," she said. "It's usually legal, it's usually IT or information security, it's usually somebody in finance, somebody in risk management and, in bigger organizations, someone in compliance or audit."

The third step is to identify external resources, according to Ms. Smith. "Know what you've already got in the way of outside counsel if you have it," she said. A risk manager also should identify existing outside support the organization might have in such areas as forensic computer investigation and breach notification providers.

"If you've done one, two and three, the fourth is a breeze," Ms. Smith said. "That's insurance."

make the case for the funds needed for encryption tools.

"I feel confident that we have people looking at this stuff," said JetBlue's Mr. Garvin. But, he conceded, with cyber risks, "I don't think you can ever say you're great, because somebody will find a way in. A lot of this stuff—it can happen to anybody."

In 2011, for example, JetBlue notified employees that their personal information had been compromised by malware, though no evidence was found that the hackers ever actually got access to files with personal information.

Taking the right approach to managing cyber risks can help a company obtain favorable coverage terms, experts say. While acknowledging the losses his company has experienced, Mr. Garvin said, "because of the approach that we take, I think that might make the underwriter more apt to write us, and I do think we have

favorable terms."

"There are factors that play into it that make us more comfortable with the risk than otherwise," said Mr. Whetstone. "Do they have somebody in the organization who owns these issues? Do they have a risk manager who understands these problems?"

If a risk manager has addressed what he or she sees as the three primary legs of managing cyber exposures (see related story), the task of obtaining adequate cyber risk coverage is made considerably easier, said Jennifer G. Smith, vp in the global technology and privacy practice with Lockton Cos. L.L.C., Washington.

"If you complete the three-ring circus, you're actually going to have better premiums...and better terms," she said.

Ms. Smith said the best cyber risk policies she's seen have been heavily manuscripted "with really up-to-date terms and conditions."

Business Insurance

**Publisher/General Manager,
Strategic Business Media:**
Mark Stach (Chicago)

**Associate Publisher/
Online General Manager:**
Paul D. Winston (Chicago)

Editor: Gavin Souter (Chicago)

Editor-at-Large: Jerry Geisel (Washington)

Managing Editor: Matt Scroggins (Chicago)

Assistant Managing Editors:
Charmain Benton (Chicago);
John D. Thomas (Chicago)

Art Editor: William Murphy (Chicago)

Senior Editors: Roberto Cenicerros (Boise);
Judy Greenwald (San Jose);
Mark A. Hofmann (Washington);
Sarah Veysey (London);
Joanne Wojcik (Denver);
Rodd Zolkos (Chicago)

Associate Editors: Matt Dunning (New York);
Sheena Harrison (Chicago); Bill Kenealy (Chicago);
Mike Tsikoudakis (Chicago)

Copy Desk Chief: Katherine Downing (Chicago)

Copy Editor: Ann Reus (Chicago)

Video Producer/Copy Editor:
Mallory Gillikin (Chicago)

Editorial Assistant: Anna Gaynor (Chicago)

Research Director: Kevin P. Edison (Chicago)

Editorial Cartoonist: Roger Schillerstrom (Chicago)

Advertising Sales Director:
Susan Stilwill (Chicago)

Regional Sales Managers:

Ron Kolgraf (Boston); Robert B. Murray
(New York); Mary Pemberton (Denver)

Southeast & Classified Advertising Manager:
Monique Murray (New York)

Sales Representative: Holly Harris (Texas)

Production Manager: J. Thomas Janka (Chicago)

Assistant to the Publisher:
Justine Karl (Chicago)

Audience Marketing Director:
Michelle O'Malley (Chicago)

Director of Demand Generation Services:
Steve Susina (Chicago)

Marketing Manager
Kathy L. Barnes (Chicago)

Digital Product Manager:
Christina Kneitz (Chicago)

EDITORIAL: Boise: 208-286-1425;
Chicago: 312-649-5200;
Denver: 303-278-7444; London: 44-207-457-1400;
New York: 212-210-0100; San Jose: 408-774-1500;
Washington: 202-662-7200

ADVERTISING: Boston: 617-292-4856;
Chicago: 312-649-5224; Denver: 303-898-4043;
New York: 212-210-0136

SUBSCRIPTIONS & SINGLE COPY SALES:
1-877-812-1587 (U.S. & Canada)
1-313-446-0450 (All other locations)

Business Insurance is published by
Crain Communications Inc.

Chairman: Keith E. Crain

President: Rance Crain

Secretary: Merrilee Crain

Treasurer: Mary Kay Crain

Executive Vice President/Operations:
William A. Morrow

Senior Vice President: Gloria Scoby

Vice President/Group Publisher:
Christopher Crain

**Group Vice President/Technology,
Circulation, Manufacturing:**
Robert C. Adams

Vice President/Production & Manufacturing:
Dave Kamis

Chief Information Officer: Paul Dalpiaz

G.D. Crain Jr. Founder (1885-1973)

Mrs. G.D. Crain Jr. Chairman (1911-1996)

S.R. Bernstein

Chairman-executive committee (1907-1993)

COVERING EXPOSURES

Risk managers' unique knowledge of their organization and its contracts gives them special insights into cyber risk exposures. Their expertise allows them to:

- Identify their organization's relevant internal documents, e.g. information security standards such as ISO 27001 and ISO 27002 and an information security policies and practices manual.

- Identify the relevant internal stakeholders, such as the legal, IT and finance departments.

- Identify external resources, e.g. outside counsel, forensic computer investigation and breach notification providers.

- Advise others in the organization about possible exposures as they outsource IT services.

- Come up with contractual wording to be able to show third-party vendors when making requests for proposals.

Captives seen as vehicles for cyber risks

By MATT DUNNING

As the business community's understanding of data breaches, network shutdowns and other cyber threats becomes more nuanced, some companies in high-risk industries are beginning to turn to captive financing for their cyber risk insurance programs.

In Vermont—by far the largest captive domicile in the U.S.—as many as 10 large companies have added cyber risk coverage to their existing single-parent or group captives, or have launched a new captive company specifically to address cyber exposures, according to the state's Department of Banking, Insurance, Securities and Health Care Administration.

David Provost, deputy commissioner of the department's captive insurance division, said that while those firms—which he described as “very large, nationally recognized brands”—had their own unique reasons for switching to captive insurance coverage for their cyber exposures, a common theme was the need for greater transparency of their up-front costs.

“At that size, it can be hard for some companies to put a real value on this kind of cover in the traditional market,” Mr. Provost said. “They can certainly get someone to quote them a premium, but they have a hard time figuring out whether the price is worth the transfer of the risk.”

Mr. Provost said most companies have elected to add a cyber liability program to an existing captive, as opposed to launching an entirely new entity. Insured limits on the captive cyber policies registered in Vermont vary widely, Mr. Provost said, ranging from \$1 million to \$100 million, with as much as \$25 million in excess retentions or reinsurance.

Experts say most of the interest in captive cyber risk financing has been exploratory in nature and has developed only among the handful of industries most likely to retain high volumes of personal consumer data, including financial institutions, managed health care, software and Internet services, and national retailers.

“It's pretty common among emerging risks,” said Steve Bauman, a New York-based senior vp and head of global corporate captive services at Zurich North America. “Folks are always a little bit hesitant to get their captives

Regulators scrutinize coverage expansion

By MATT DUNNING

Where the licensing process is concerned, captive programs designed to insure cyber risks are likely to receive the same level of scrutiny from regulators as any other captive program.

The difference separating a captive proposal for cyber risk—as an addition to an existing captive or as a separate insuring subsidiary—and one for a more traditional brand of insurance is likely to be the breadth of information available to a prospective parent company, according to David Provost, deputy commissioner in the captive insurance division of the Vermont Department of Banking, Insurance, Securities and Health Care Administration.

“Whenever you decide you're interested in a captive, the first thing you need to do is

an internal feasibility study,” Mr. Provost said.

Typically, Mr. Provost said, domiciles such as Vermont evaluate captive proposals based largely on an applicant's loss history, actuarial analyses, projected premiums and expected losses. However, he said, regulators frequently augment their approach to accommodate proposals for unconventional captive products, a category that certainly includes cyber liability insurance.

Even with little supportive data, Mr. Provost said domiciles still can evaluate and approve a captive application based on a company's “financial commitment” to the product.

“When you look at the limits you want to write for your company, you need to consider whether the captive has the surplus to handle those limits,

and do you as the parent have the financial strength to support that retention in the long term,” Mr. Provost said.

Domicile regulators also are likely to pay close attention to an applicant's data and network breach prevention and response strategies when considering licensing a captive cyber risk program, Mr. Provost said. Previous captive agreements are not necessarily treated as a binding precedent, though it may be advisable for companies to turn to consultants or peer networks for advice on established best practices.

“We always say that if you've seen one captive, you've only seen one captive,” Mr. Provost said. “Each company is going to be unique in terms of their exposures and their approach to risk management, so it's going to vary tremendously.”

CAPTIVE PROS & CONS

Experts say many large companies are exploring the prospect of using a captive insurance program to underwrite data breaches, network continuity and other cyber risks, but only a handful actually have made the switch to a captive-backed policy. Some of the potential advantages and deterrents of captive cyber insurance are:

Pros

- Greater transparency of insurance costs
- Opportunity for tax savings on expected claim payments
- Better access to high-limit coverage for at-risk industries
- Forces greater focus on internal data breach prevention and response protocols

Cons

- Retention funding requires large up-front and long-term financial commitment
- Data breaches are low-frequency, high-severity risks that are difficult to model
- Fast-moving cyber regulatory environment adds additional complexity

involved in something that's brand new or emerging, especially if it could have high volatility.”

Several factors likely are holding back more widespread implementation of cyber risk captives, experts said. For one, most mid-size and large companies would have little difficulty purchasing cyber risk coverage in the traditional insurance markets, depending on their flexibility on pricing.

“The commercial marketplace seems to be largely able to respond

to clients' needs in a way that most clients are comfortable paying for,” said Sean Rider, a New York-based managing director for Willis Group Holdings P.L.C.'s global captive practice.

Perhaps more of an impediment to greater utilization of captives to address cyber liability is the fluid nature of cyber risks. Aside from the seemingly endless permutations of data and network security threats, companies also must contend with regulators pursuing

greater protections for consumers in the event of a breach.

Also, captive insurance tends to be more effective when applied to high-frequency, low-severity risks. A given company may only experience one data breach in a period of several years, but the total cost of mitigating that event could be devastating.

“As a result, using a captive as a risk financing mechanism for a cyber insurance program, depending on the size and complexity of the captive, might unduly expose that program to a catastrophic loss,” Mr. Rider said.

Nevertheless, experts said they expect to see a gradual upswing in the number of companies utilizing captive programs to finance their cyber insurance coverage, especially as more risk managers and C-level executives develop a fuller understanding of the true cost of data and network security.

“I'm seeing a lot of companies move toward a more centralized management of their overall privacy and data security exposures,” said Catherine Mulligan, a New York-based senior vp and national underwriting manager for specialty E&O at Zurich North America.

inBrief

Aon shareholders OK move to London

Aon Corp. shareholders have approved the relocation of the broker's headquarters to London from Chicago. A spokesman for Aon said that more than 82% of the outstanding shares were voted at the meeting and that, of those, more than 98% were voted in favor. Aon President and CEO Greg Case has said the move will help Aon grow its business in emerging markets. Aon also said it expects to reap tax benefits from the move.

AIG's tax treatment comes under fire

Four former members of the Congressional Oversight Panel for the Troubled Asset Relief Program are calling for an end to tax breaks favoring American International Group Inc. Former Chair Elizabeth Warren and former panel members Damon Silvers, Mark McWatters and Kenneth Troske, issued a joint statement asking that the tax exemptions granted to AIG at the height of the 2008 financial crisis be revoked. Specifically, the exemptions override longstanding tax laws limiting the extent to which a company can offset future taxes with past losses.

Sandusky, Second Mile in defense dispute

Former Pennsylvania State University assistant football coach and founder of nonprofit youth charity Second Mile Inc. Gerald A. Sandusky disputed claims that the charity's insurance company was not obligated to provide defense coverage costs in connection with child sexual abuse allegations facing Mr. Sandusky. Federal Insurance Co. in December filed a declaratory judgment against Mr. Sandusky that it has no obligation to pay his defense costs or to indemnify him for civil and criminal lawsuits alleging sexual abuse of children, according to court documents.



DON'T....
let your access to **BusinessInsurance.com** end!



REGISTER TODAY AND GET 10 ARTICLES A WEEK
OR SUBSCRIBE TODAY FOR UNLIMITED ACCESS!

www.businessinsurance.com/section/subs

Business Insurance®



Apple customer has serious beef

In many of Cupertino, Calif.-based Apple Corp.'s television advertisements about its new iPhone 4S, individuals are shown using the smartphone's new voice-activated assistant feature Siri to make appointments, find restaurants and even learn the guitar chords to classic rock songs.

But if iPhone 4S users ask Siri what she thinks about a lawsuit accusing Apple of false advertising, she probably won't understand the question, much less direct them to the complaint, according to disgruntled customer Frank M. Fazio, who filed his complaint March 6 in U.S. District Court in San Jose, Calif.

"Through an extensive and comprehensive nationwide marketing campaign, Defendant has conveyed the misleading and deceptive message that the iPhone 4S's Siri feature, a so-called voice-activated assistant, performs useful functions and otherwise works as advertised," according to the suit, which seeks class action status. However, "the iPhone 4S's Siri feature does not perform as advertised, rendering the iPhone 4S merely a more expensive iPhone 4."

For example, when Mr. Fazio "asked Siri for directions to a certain place or to locate a store, Siri either did not understand what Plaintiff was asking, or, after a very long wait time, responded with the wrong answer," the suit states.

The suit also claims Apple knew that Siri would not perform as advertised based on a footnote on the company's website stating that "Siri is currently in beta and we'll continue to improve it over time."

"Siri is, at best, a work in progress," according to the suit, which seeks unspecified damages and restitution.

Apple did not immediately return phone calls seeking comment.



CONTRIBUTING: Matt Dunning, Judy Greenwald, Mike Tsikoudakis, Joanne Wojcik

End Page



Facebook fellowship helps The Hobbit pub

It may not be necessary to bring in the orcs after all.

Fans of The Hobbit, a pub in Southampton, England, had been up in arms over an initial report that the tavern was a target of the company that owns the film, stage and merchandising rights to J.R.R. Tolkien's "Lord of the Rings" trilogy and "The Hobbit," according to British newspaper the Daily Echo.

The pub's owner, Stella Roberts, had said she was ordered by Berkeley, Calif.-based Saul Zaentz Co. to remove all references to Mr. Tolkien's creations or face litigation.

The pub, which has been in business more than 20 years, has interior and exterior artwork, a website and fonts, as well as "Lord of the Rings"-themed cocktails that evoke the Tolkien classics.

Ms. Roberts told the newspaper she does not have the funds to stand up to the company. "It's not just a case of changing the name—it's all the merchandise, artwork,

absolutely everything. We never planned to steal anybody else's ideas—we're all such huge fans of Tolkien that it's more like homage."

But it may all have been a misunderstanding. In a follow-up article, the newspaper said it had been told by Mr. Zaentz that he does not necessarily want to remove all references to Mr. Tolkien's work and "certainly doesn't want to run anyone out of business."

He said he wants to resolve the dispute "amicably" and suggested the pub could be asked to pay a nominal license fee of \$100 a year.

Mr. Zaentz contacted the newspaper after a Facebook campaign to save the pub attracted worldwide attention, with backing from actors Stephen Fry and Sir Ian McKellen, who both appear in the upcoming film, "The Hobbit."

One can imagine that, somewhere, Gandalf is looking on approvingly.



His and hers? Not when selling car insurance

Charging female drivers the same premium rate as male drivers in Europe is an "outrage" and "inappropriate," a London-based insurance company said Thursday.

Legal & General Group P.L.C. was the latest insurer to respond to a 2011 European Union court decision where insurers are to stop setting prices based on gender.

The decision could push up auto insurance costs for women, who pay less than men because they are statistically less likely to be involved in accidents, according to reports.

Industry experts say the rule, effective December 2012, could raise costs for women drivers, cut male pensions and prompt more legal challenges to insurance pricing practices, according to reports.

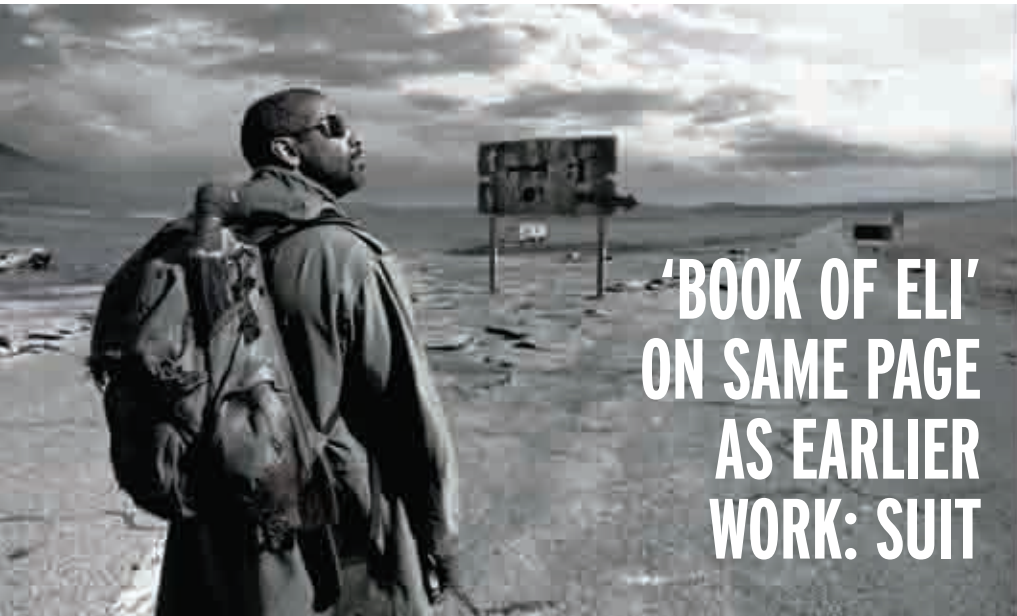
The court's decision immediately drew criticism from the insurance industry, which said different pricing for men and women was legitimate given their different risk profiles, according to news reports.

The introduction of unisex rates was "an outrage," John Pollock, executive director of risk at L&G, said in a report.

"It will make us entirely powerless to differentiate between risk for male and female customers. It's completely inappropriate," he said.

Analysts in a separate news report said the decision would have little long-term impact on insurers' earnings, as they have enough flexibility over pricing to ensure any changes would cancel each other out.

But the gender ruling could pave the way for a potentially more damaging legal challenge to insurers' reliance on their customers' age in setting prices and payouts, they said.



'BOOK OF ELI' ON SAME PAGE AS EARLIER WORK: SUIT

A Georgia-based writer has accused the directors and screenwriter of the 2010 dystopian hit "The Book of Eli" of stealing the idea for the movie from an unpublished work she submitted to a Writer's Digest contest six years before the film's release.

Author Bridgette Burgin claims that Writer's Digest judges gave her work, entitled "The Final Call," to screenwriter Gary Whitta, who used it as the basis for directors Allen and Albert Hughes' movie "The Book of Eli," according to her complaint filed in the U.S. Court for the Central District of California.

In her complaint, Ms. Burgin cites

more than 50 similarities between her work and the movie. She is seeking punitive and compensatory damages for harm to her "professional reputation and diminution of her intellectual property," and for "adversely affecting her ability to obtain gainful employment in this field," according to the court documents. Ms. Burgin's complaint also claims that she is entitled to impound and destroy all offending materials, should a judgment be rendered in her favor, but does not specify whether she would pursue such action.

Workplace Safety and the Aging Workforce

Theme issue: April 9 - Ad closing: March 28

The aging of America's workforce is forcing companies to re-evaluate their health and safety programs.

Business Insurance takes a closer look at the programs employers can initiate to:

- Retain valuable skills
- Lower injury losses
- Increase productivity

From workstation assessments to health and wellness programs, this theme issue covers the gamut of information that readers need to navigate the challenges and rewards of an aging workforce.

**Make sure your company's solution
is part of this great issue!**

Special advertising opportunities:

Exclusive Data Poster/Data Spread sponsorship

Call 312-649-5224 to reserve your space today!



*Or scan the QR code to find
solutions to all your marketing needs.*



Quality health plans & benefits
Healthier living
Financial well-being
Intelligent solutions



Smarter is a health plan that thinks outside the office.



Over a quarter million downloads, the Aetna Mobile app.¹

- Find in-network doctors and pharmacies just about anywhere.
- Look up prescription costs *before* buying.
- Use with your doctor and ask questions before you leave the office.

See the proof at smarteris.aetna.com/mobile

¹App Store, Android Market and App World as of February 2012.

© 2012 Aetna Inc. Plans offered by Aetna Life Insurance Company and its affiliates. Health benefits and health insurance plans contain exclusions and limitations. Providers are independent contractors and are not agents of Aetna. Provider participation may change without notice.
2012004

