INTO THE BREACH

Underwriters expand data security and privacy protection with telecommunications as one key market. Some big communications companies say they still prefer to retain risk. ● **BY GREGORY DL MORRIS**

In mid-March, the professional liability division at American International Group Inc. began offering security and privacy insurance for liabilities related to mishandling of confidential data. National Union Fire Insurance Co. of Pittsburgh rolled out nationally the coverage it had been offering on a case-by-case basis since last year to existing clients.

AIG/National Union, along with CNA, St. Paul Travelers, Chubb and Zurich, are established players in the market, while there are several new entries, including One Beacon out of Boston. Underwriters and brokers report that telecom operators are the primary buyers for this type of coverage, followed closely by financial services and medical firms.

Broadly speaking, capacity is reported to be adequate and premiums are holding steady or even dropping in some lines. However, brokers and insureds indicate that limits remain low. The market seems to be evolving more slowly than might be expected because of several factors, not the least of which is an institutional reticence by the big telecom firms to transfer risk.

One risk management executive for a major telecom says dismissively, "Data security is just not something that we insure. Traditionally, we do have higher retentions (than companies our size in other industries), but this (privacy risk) is not something that we have ever tried to quantify, nor have we had our brokers come to us with anything."

There is also a distinct reticence by telecoms of all sizes even to discuss the topic. AT&T, Verizon, Sprint, Vonage and other firms large and small declined to comment on the record about their data and privacy risk management, saying to be cited would make them a target. However, several risk managers were willing to provide input without attribution.

"We just had a minor incident," says one senior risk manager. "We lost two laptops with employee data on them. It's not like we had a security breach, not like we had to reconstruct the data, but it was very costly to extend protections to the people whose data was compromised. One of my colleagues here asked me if we were covered for those costs, and I had to say, 'No, just for the loss of the laptops.'"

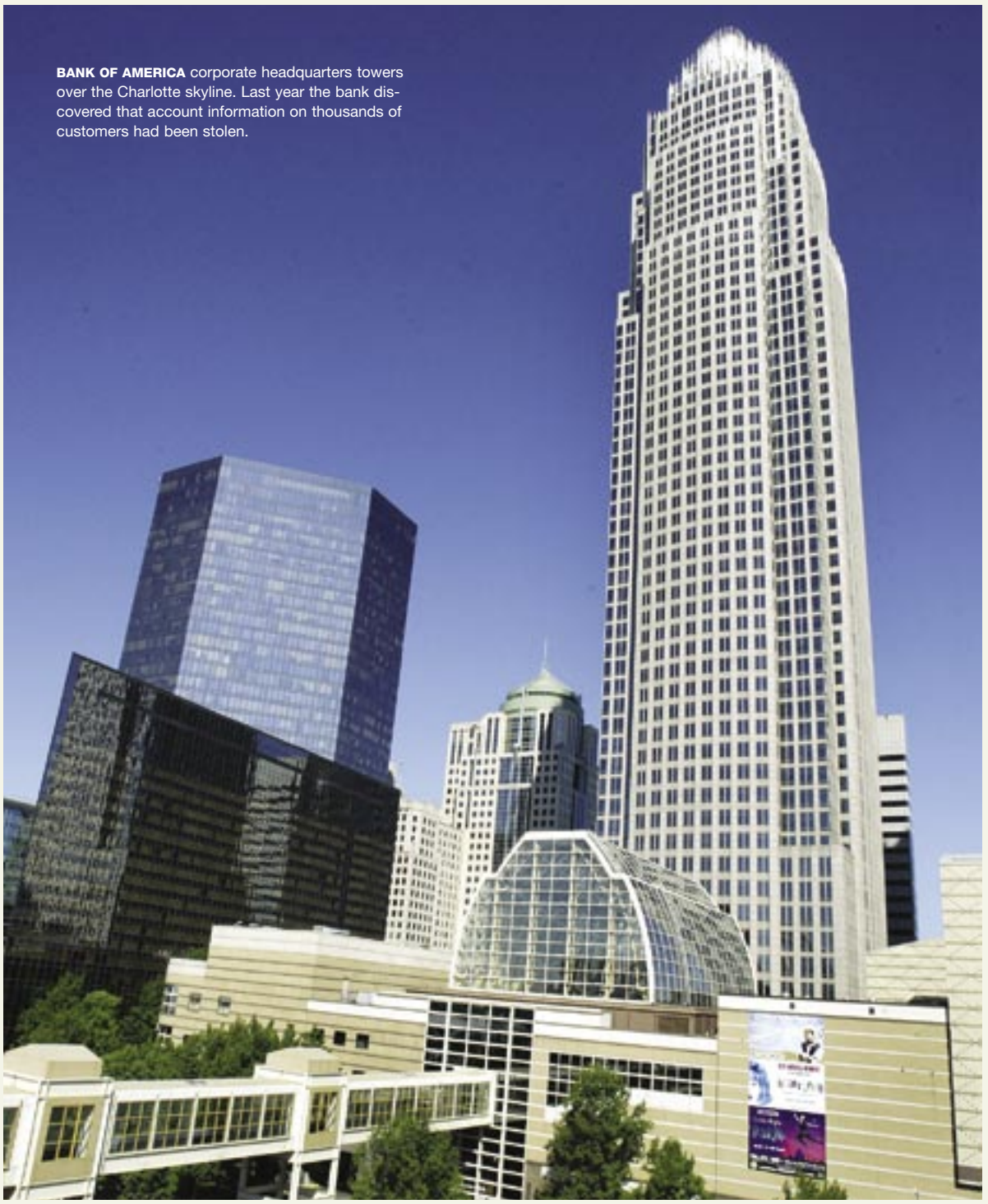
AIG/National Union cites data from the Identity Theft Resource Center indicating that more than 134 computer security breaches affecting potentially more than 57 million individuals were reported in 2005. The insurer also refers to a study by the Ponemon Institute indicating that last year, U.S. companies incurred an average cost of $14 million per breach incident, with costs ranging as high as $50 million.

"Beyond the financial consequences, new laws that require admission of data breaches are increasing public concern and potential liabilities," says Michael Smith, president of the professional liability division of National Union. He says the new coverage addresses the liabilities that arise when private or confidential information is put at risk by many means, including a failure of security or wrongful release or disclosure of information by the insured, the insured's employee or another third party.

"Five years ago, we began offering network liability coverage that covers legal defense costs, as well as specific risks arising out of a failure of security, hacking, viruses, and accidental information released as a result of hardware or software failures," says Nicholas Economidis, vice president and product manager for technology at National Union.

He adds that just last December, the company began writing an enhanced privacy coverage, "including wrongful release of data or a failure to protect data. It also covers vicarious liability of a vendor's failure to protect personal information. Telecoms are the primary businesses to which we are offering the privacy coverage, but it is open to all sizes and types of companies. So far we have one telecom insured, and several large financial institutions."

John Wurzler, vice president of technology for CNA, applauds the increase of capacity in the market but notes dryly, "This is not new to us.



AP PHOTO, CHUCK BURTON

BANK OF AMERICA corporate headquarters towers over the Charlotte skyline. Last year the bank discovered that account information on thousands of customers had been stolen.

About 16 percent of our book of business for our NetProtect coverage is from telecoms, about 1 percentage point larger than financial services or health care."

Michael Silvestri, product manager for NetProtect, adds, "In the fourth quarter of 2003, we were the first to offer privacy liability protection under NetProtect, and I am glad that the industry is moving in this direction. We see the protection of custodial data as a special responsibility for telecoms. When we first started developing this coverage, we saw a sharp increase in the amount of private information that was being collected—call information, transmissions, billing—and also a gap in existing coverage."

As this is a fast-moving market, Wurzler says CNA has broadened the initial network or cyberrisk coverage to include offline data, "the things in your filing cabinet and on your fax machine. We were the first to do that without limiting the trigger to a breach of security, so we would cover things like employee mistakes."

A wider range of security and privacy risks is very much on the minds of telecom risk managers, says Valynda Murphy, managing director of Marsh's technology and telecom practice. "There are so many ways a customer's information could be revealed. It could be by accident, sending data to the wrong party, or a disgruntled employee deliberately posting information. The biggest risk we see again and again is privacy. What is needed is control from within, and then transfer of some risk for better protection."

CLOSING THE GAPS

The other legacy issue that consolidated and recombined telecom companies face is conflicting practices and systems. "Any time there has been a merger or acquisition, you know there are areas that are not protected," says Murphy. "Even if a company claims to be fully protected, multiple systems mean noncompatibility."

In contrast, "some smaller companies do a good job of protecting themselves," she adds. "Often they only have one or two systems, and they can get their arms around their exposures. If they have a limited number of locations, or a smaller network, it is easier to protect. And if you can show an underwriter you are protected, you can get coverage. Prices have come down, there are more offerings in data security and privacy than there were three or four years ago, there are new underwriters entering, and there is more capacity."

One Beacon got into the business via several acquisitions, and is content to let the big telecoms retain their risks. "Our interest is in the smaller side of the market, but we are a multiline underwriter with P/C, liability, E&O, workers' comp and so forth," says Matthew Mueller, national manager of the technology segment for One Beacon. "Right now we are looking at some new solutions specifically for data security and privacy protection because those are most evident as the key issues that are not being addressed (by other carriers) or are not being properly addressed."

There are two key challenges he sees in this market, which are really reciprocal: brokers and underwriters who do not understand the market, and risk managers at the small telecoms who may not be able to identify and manage their data and privacy risks. "My observation in general is that risk managers are not always equipped to quantify and arrange to transfer their privacy exposures," says Mueller. "At the smaller companies they tend to be jacks-of-all-trades. That is a wonderful opportunity for a broker or underwriter to step in and be helpful."

On the other side of the coin, Mueller acknowledges that the whole field of telecom security is barely two decades old, and that some areas, like electronic 911 tracking and voice over Internet protocols, or VoIP, are just emerging. "There is no track record for the underwriters," he says. "There is no actuarial data. It is a very challenging process for insurers, and the technology is constantly changing. For example, a company may be working in ATM—asynchronous transfer mode—and a broker will come in and say, 'So you make cash machines.' "

Once a conversant broker or underwriter is found, Mueller urges telecom risk managers, especially those whose companies are working in emerging technologies, to "describe in detail your risk management protocols, not just for what you do now, but what you plan to do. There are lots of cases out there where an insured finds it has gotten itself into a new business or technology that is not covered, that its underwriter never even anticipated. On the other hand, there may be some risks that are just not practically transferable."

The irony there is that because some telecom security risks may have to be retained, other transferable risks may not be insured. Alfred Tobin, managing director for Aon's national property practice, says there are many cases where telecom companies do not think about buying coverage that is available—transmission and distribution coverage, for example. "Then along comes an event, a hurricane that just rips you, and you realize that coverage was available."

If the legacy carriers want to retain most of their exposures, Tobin figures they know what they are doing. Despite the name, "the Baby Bells are mature customers in mature markets." But for issues like privacy, he acknowledges that "to retain that risk you have to have a database of losses. We have a group of attorneys who do nothing but study that—privacy, copyright, software developments. And there are certain established underwriters who understand that."

"THE MAJOR EXPOSURE IS MORE LIKELY TO BE A DRAMATIC DISCLOSURE OF A SMALL BIT OF INFORMATION ABOUT LOTS OF PEOPLE RATHER THAN LOTS OF INFORMATION ABOUT ONE PERSON. BREADTH IS THE CONCERN, RATHER THAN DEPTH."

—Tom Ricketts

Mike Thoma, second vice president for technology underwriting for St. Paul Travelers, also plays down some of the novelty aspect of the telecom security market. "For protection of their own data on their own networks, telecoms are similar to any large company. We have products for first-party technology E&O, and also an Internet liability product." In underwriting Thoma says his firm "looks at the controls a client has in place: the management controls, the recognition of exposure, the levels of encryption."

He says that his firm is not developing any major new offerings, "there are not any significant needs for that, just for enhancements." Thoma also stresses that "physical hazards remain just as big a threat as privacy or piracy. There is a lot of concern around security or risk in transmission, but that is actually a minor risk. It is inefficient for the perpetrators of these acts to try to steal data in transmission. They want large quantities of data. The bigger risk is the physical risk of a laptop or CD-ROM being stolen."

Tom Ricketts, senior vice president, tech and telecom practice leader at Marsh, agrees that telecom technology and risks are changing almost daily, so the detailed actuarial data have yet to be compiled. But he adds, "The insurance industry actually has quite a bit of experience in privacy. That includes personal injury, financial losses and management controls. Underwriters understand these risks from many years in the mass-media market."

What is new is the breadth of the risks. "A hacker getting into someone's handheld and downloading a lot of personal information, as happened in one high-profile case recently, is big news," Ricketts explains. "But the major exposure is more likely to be a dramatic disclosure of a small bit of information about lots of people rather than lots of information about one person. Breadth is the concern, rather than depth."

The data and privacy market today is like the employment-practice liability market of 10 years ago, says Steve Levene, executive vice president for brokerage firm Lockton, based in Dallas. "No one was buying. Then all of a sudden there were big claims, the frequency started to ratchet up, the attorneys found that there was money in it and now everyone buys the coverage. Look at what people are doing these days."

The key in the present market is to evaluate both clients and underwriters, says Bill Miles, vice president of financial services for Lockton. "We look at the client's customer base, the services it provides, the content it provides, and especially its vendor and customer contracts for indemnification and liability. This is a tough class to underwrite, because the telecoms move so quickly. Unfortunately, the products available off the shelf do not completely address the particular needs. Underwriters are getting warm to the market, and getting coverage has gotten easier."

Lockton is currently working with three underwriters—AIG, Ace and London house Beazley & Hiscox—to develop two specialized forms of coverage, shorter periods for recovery time and damage to brand value if there is a loss. "With new laws that require disclosure, are people going to stay away from a company that has a breach?" Levene asks.

Mandatory disclosure may just be the tipping point for data and privacy coverage, says Peter Foster, senior vice president of E&O cyberrisks for Willis. "Identity theft is a big driver. Now there are 23 states that require companies to notify consumers if there has been a breach. It used to be that IT could keep it quiet. Now it's going to be public. We have already seen some multiparty lawsuits as well as class actions. The plaintiff's bar is taking a long look at this."

Willis has its own assessment for clients, covering confidentiality, data integrity, network availability and the disruption continuity plan. "Our practice is with large to midsized companies," says Foster, "and we emphasize building cyberrisk into their overall program. We look at their existing coverage, see what we can cover with endorsements and then fill in the gaps."

GREGORY DL MORRIS *lives in New York City. He can be reached at riskletters@lrp.com.*