

# Insure Your Company Against Data Breaches

In the cases that have been reviewed, the average fine is \$100,000.

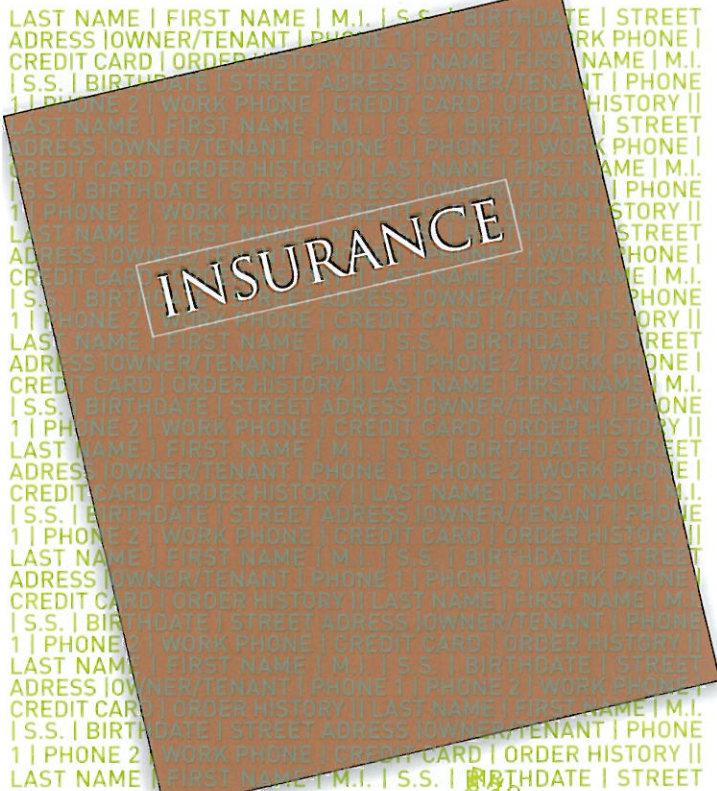
In today's electronic world, identity and credit theft have become very common occurrences. Sometimes, it is a single case of thievery. Other times, it is part of a much broader act where a business network and the data it contains are compromised. Personally, I was a victim of one of these credit-card theft situations. An employee of a Washington, D.C.-based restaurant swiped my credit card but not just for the payment of the meal. He used it to set-up a Pay-Pal account from which he wired funds, drawn out of my account, to an overseas location. Thankfully in my case, the breach was caught immediately, and there was very little residual damage or cost incurred (just the difference in the exchange rate).

I was lucky, but for each positive story, there are too many that don't have a happy ending. So, is it any wonder that the Federal Communications Commission (FCC) stepped up last year and issued new rules to protect consumers? In an attempt to minimize the possibility of data breaches, the customer proprietary network information (CPNI) rules impose specific rules on telecommunications providers.

Late last year, NTCA pushed to educate telecommunications companies on the revised CPNI rules. Personally, I wondered if their messages hit home. The following examples tell me that a few companies have not addressed the issue. The commission's Web site lists at least 20 cases where CPNI violations have been found in the last 16 months, and several of the companies are NTCA members. In the cases that have been reviewed, the average fine is \$100,000. Another report on the site notes that as of the end of 2007, the FCC had issued 22 proposed forfeitures associated with the protection of personal information during the year, for a total of \$1.6 million. Clearly, FCC fines are a potential liability for a telecommunications provider.

Can insurance policies cover fines? The logical area to look

for coverage would be the General Liability policy since this would be an allegation by a third party that your business was legally liable for failing to comply with a law, rule or regulation. The General Liability policy basically covers bodily injury, property damage, personal injury and advertising injury, and it extends medical payments to those with physical injuries despite the absence of liability. A violation of a rule, law or regulation does not on its own trigger coverage under the insuring agreement of any of these coverage sections. ▶▶▶





With  
Cooperative roots,  
*we understand*  
what it takes  
to serve  
*rural customers*



### Internet Solutions

Virtual ISP

Value Added Services

ISP Consulting

### Call Center Services

Internet Help Desk

Video Support

Voice Trouble Calls

**Golden West Technologies**

Headquartered in Rapid City, SD

1.800.343.1869

www.gwtis.com

Where else could you possibly look? The second policy to review might be the Executive Liability coverage, also known as Directors and Officers Liability policy. Assuming that the claim is that a director, officer or manager acted improperly and a regulator is making a third-party allegation against them for the failure to carry out their duties, this policy would be a possible insurance solution. However, in most coverage forms, the definition of "loss" would eliminate Executive Liability policies as potentially responding to the claim because penalties imposed by law generally are excluded. A third insurance reimbursement option would be a Network Security and Data Liability policy. This is a specialty liability policy not currently included in any carrier's standard General Liability or Executive Liability policies. This coverage would pay for regulatory expenses and fines when a breach has occurred. This means failure to submit a form properly or on time is simply a cost of doing business. Your insurance provider can, at best, provide you with notification that the form is due by a certain date, assuming they know of the issue at hand.

What are the liabilities and costs associated with CPNI breaches, fines and circumstances when your network is compromised and data is stolen? Are there insurance products and organizations that can assist you with risk analysis, risk-management and insurance solutions?

The liabilities or fines can be easily calculated for both fines and the cost of a breach, but keep in mind that the cost of a breach is on the increase and what it costs today could double in a year. The FCC records place the cost of a fine at \$100,000 and state that it cannot be covered by insurance. Before exploring insurance and risk management solutions for a data breach, the cost of breach should be recognized. In 2008, as of January 29, the Identity Theft Resource Center reported 47 incidents with 391,753 records exposed. In 2007, the same source tallied 448 data breaches and 127 million records uncovered. Of

those companies studied that suffered a network invasion, 63% reported operational cost and 40% reported financial loss. The average loss, as reported by the E-Crime Watch Survey, was \$507,000.

There are two other ways to look at cost and help you personalize what the cost might be to a business of your size. The Identity Theft Resource Center also shows that the operational cost per record breached is on average \$197 per record. Keep in mind, this does not even include injury claims. The second calculated cost is lost business due to harm in reputation, which costs an average \$128 per record. These types of losses or incidents have the potential to bankrupt an unprotected company.

When there is a breach of an individual record or into your network to multiple customers' private data, what is the potential liability for this and what are insurance and risk-management options that can protect and you and reimburse third-party claimants on your behalf if your network is compromised? The General and Executive Liability policies will not respond to this type of claim for the same reasons provided previously, with one additional twist. The General Liability policy could potentially provide protection under the property damage and the personal injury sections.

However, property damage is generally defined as damage to tangible property, and data is not tangible. Therefore, there would be no coverage. Personal injury as defined in a liability policy includes: false arrest, malicious prosecution, wrongful eviction or entry into a property, libel or slander, and copyright, trade dress or slogan infringement. None of these will provide defense against a data breach. There are specialty policies for both property and liability. As was the case with coverage for the cost of fines, these are not currently part of insurers' General or Executive Liability coverage that can provide a wealth of protection for a telecommunications provider.

There is coverage for data you own and that which is housed on your network that you are responsible for, and there is also protection for your legal

liability. Coverage is available that protects your own data and that of others that you might house on your computer system if it is damaged by electronic disturbance or human vandalism. The best coverage will not only provide coverage for the cost to reproduce the data and replicate your system but also will cover the loss of income or accounts receivables that occurred due to the damage. The best of the best coverage also will provide reimbursement if the damage has created a denial of service—meaning you were locked out of your own system. These policies typically will cover the cost of gathering information for regulatory agencies that have interest in the breach. This would cover the cost of gathering anything the FCC or any other party needed to determine the extent of the violation and of your liability. It is also possible to buy coverage for the harm to your reputation, which is the cost of a public relations firm to do damage control in the media. Damage control also might take the form of providing customers who had data compromised with free credit monitoring for a year. Credit monitoring is a common requirement of regulators as part of a fine or settlement in these kinds of cases.

The liability section of the specialty policies will pay for damages incurred by claimants and their expense to protect their private information. Coverage normally is provided for the cost of regulatory fines, assuming they are a result of a breach of data and not a fine for failure to comply with a filing date. Certain liabilities are not covered, including fraud, fiduciary claims, racketeering charges, violations of employee retirement plan and benefit laws, directors and officers claims, and protection provided in a General Liability policy. All these policies are very broad and will protect you as long as the limit of coverage you purchased is adequate.

CPNI and the fact that the FCC has data protection on its agenda as an important item may be enough of a driving force for your company to take action. Only five states do not have active or pending laws with regard to what a

business must do in the event of a breach. The states without laws as of January 2008 are: Oregon, South Dakota, New Mexico, Missouri and Mississippi. If you still don't see the risk and decide to retain the exposure to a data breach, make sure you can recognize all exposures, analyze them, and plan to elimi-

nate the risk and then implement your plan. You should be able to rely on your insurance and risk manager to help you with non-insurance transfer of exposure. ■

*Peter J. Elliott, CPCU, is CEO and president of Telcom Insurance Group. He can be reached at PJE@TelcomInsGrp.com.*

**PARTNERING**  
*for a Stronger Rural America*

Offering a broad range of financial solutions, COBANK partners with communications companies across America to help them meet their business objectives of today and strengthen their ability to address the needs of tomorrow.

**Ritter**  
COMMUNICATIONS  
E. Ritter Communications  
Marked Tree, AR  
Acquisition

**ALPINE**  
communications  
Alpine Communications, L.C.  
Elkader, IA  
Refinance &  
Capital Expenditures

**zayo**<sup>™</sup>  
BANDWIDTH  
Zayo Bandwidth, Inc.  
Louisville, CO  
Acquisition

**BEVCOMM**  
Rural Communications  
Holding Corp.  
Blue Earth, MN  
Acquisition

**Avenue**  
Avenue Broadband  
Tyler, TX  
Acquisition

**OXFORD NETWORKS**  
Oxford Networks  
Lewiston, ME  
Refinance &  
Capital Expenditures

**Solarus**  
Solarus  
Wisconsin Rapids, WI  
Refinance &  
General Corporate Purposes

For more information, please call  
1 (800) 542-8072 or visit  
[www.cobank.com](http://www.cobank.com).

**COBANK**