

# AMERICAN Agent & Broker

Your Source for Agency Success

PropertyCasualty360.com

## FEATURE STORY: PRIVACY LOSSES

### LEARN HOW TO INSURE CLIENTS AGAINST PRIVACY LOSSES WHEN DEALING WITH HACKERS, IDENTITY THIEVES AND LAWSUITS.

By **PAUL MISKOVICH** and **EDWARD SEIDL**

**T**he many risks are evident. Private information of all kinds—personal, financial, medical—resides on the computers of nearly every business. Hackers and identity thieves increasingly are compromising system vulnerabilities, seeking to break in and exploit the details.

Hacking has been generating high-profile news lately. Citigroup warned 360,000 credit card customers that some account data was compromised. AT&T apologized to 114,000 new iPad owners, including celebrities, after hackers leaked their email addresses to an online gossip site. Privacy breaches, both accidental and criminal, are increasing steadily, along with their costs.

Violation of privacy laws and regulations also has become one of the fastest-growing litigation areas, with lawsuits accusing companies of negligence in their computer system security, breach of warranty and failure to properly inform customers following unauthorized access or accidental loss of personal data.

The financial risks of privacy breach are growing for service businesses. Potential costs include liability to customers or employees whose details are exposed, regulatory and legal expenses to notify affected individuals, work to restore computer systems, business interruption, damage to reputation—even extortion demands.

Property-casualty agents and brokers should stay informed about this increasing risk and the coverage solutions that can help mitigate financial exposure. The frequent news of hacking attacks offers ample opportunities to discuss coverage needs, especially with clients in the miscellaneous professional liability category.

#### GROWING PRIVACY THREATS

Businesses that once were simple service providers have taken on added technology functions that today are integral to their operations. Not only do these businesses worry about errors or omissions in their primary services; they must be concerned about their computer systems holding protected personal information on thousands or millions of clients. Much of this information is regularly exchanged in the course of transacting business through websites and interacting with other service providers.

The result is a potential nightmare for medical billers, third-party administrators, marketing companies, collection agencies and other miscellaneous professional service organizations.

Common causes of data losses include criminal attacks by hackers, mistakes by employees or third-party outsourcers, and loss or theft of laptops and other mobile devices. Some recent examples from the Identity Theft Resource Center:

- 1 An IT vendor for a health insurer reports stolen computer drives holding data on 1.9 million customers: names, addresses, medical information, Social Security numbers and other financial information
- 2 A medical transcription firm inadvertently opens its server to access from the Internet, making more than 1,000 detailed patient records potentially available to third parties
- 3 A direct marketing vendor sends a mailing that accidentally prints the Social Security numbers of 8,000 people on the outside of the envelope
- 4 A collection firm is hacked, losing 1,800 consumers' confidential credit reports
- 5 An employee of a call center improperly downloads an electronic database of customer identities, Social Security numbers and payment card details

6 An email marketer for dozens of the largest U.S. companies is hit by hackers who gain access to millions of consumers' names and email addresses.

Some privacy breaches involve paper rather than electronic losses: A tax preparer's briefcase is stolen from a car, a thoughtless employee discards old files in a trash container, or confidential papers are left out on a desk. But technology has enlarged the scale of the privacy risk.

Protected personal information is generally defined as confidential data that could cause financial harm to a person if unauthorized users gain access. Examples are Social Security numbers, driver's license numbers or equivalent, bank account or credit card numbers, and certain medical or healthcare information.

Even unauthorized release of email addresses and passwords can make consumers vulnerable, because criminals pretending to be banks or trusted retailers send targeted phishing emails seeking data that would expose financial accounts to fraudulent transactions. Hackers also take advantage of the fact that many consumers use the same password for all of their accounts.

A loss can be extremely costly to a company. The average cost of 51 data breaches at U.S. businesses studied in 2010 was \$7.2 million, or \$214 per affected customer, according to the Ponemon Institute, a think tank on security issues.

#### COVERING PRIVACY RISKS

Many insurers offer coverage that can be endorsed to a standard miscellaneous professional liability policy, offering defense and indemnity coverage to insureds to manage potential liabilities from privacy breaches. First-party coverages that proactively cover expenses if a security breach occurs also are an option.

The basic privacy coverage is an enterprise-wide network security and privacy liability endorsement, which defends the insured against claims alleging negligence in maintaining or protecting personally identifiable information. In addition to customer information, the coverage includes claims by employees arising from unauthorized disclosure of data.

Generally, regulatory action defense coverage is coupled with that network security and privacy endorsement to provide a defense for actions brought against the insured by any regulatory or governmental organization as a result of a violation of privacy laws or regulations. The current standard in miscellaneous professional liability policies is not to cover claims brought by governmental agencies. Even when privacy coverage is purchased, it typically provides for defense costs but excludes payment for fines or penalties.

Crisis management coverage provides reimbursement of a company's expenses to respond to a privacy breach, including costs to notify affected individuals, provide credit monitoring services, engage forensic experts to determine the cause of the breach, and hire a public relations firm to help mitigate damage to a company's reputation. Unlike other coverages, crisis management coverage is not for liability to others but for direct costs incurred by the business. This coverage will assist companies in reassuring customers that the company recognizes the problem and wants to continue serving them.

Business interruption coverage, familiar to property insurers, is needed to cover the loss of revenue if a security breach causes a material disruption to a company's computer system and sales suffer as a result. This coverage generally is structured with a waiting period that gives the insured a fixed time, such as 12 hours, to get its computer system back up and running before the revenue losses are covered as business interruption.

Data restoration coverage may be required to offset the company's expenses to restore customer, vendor and employee files, which can be substantial depending on the severity of the data breach.

## More on the Web:

- ▶ [Cyberspace: The Next EPLI](#)
- ▶ [Insureds Without Cyber Policies Risk CGL Coverage Holes](#)
- ▶ [Catching the Cloud](#)

Read these related articles at [PropertyCasualty360.com](http://PropertyCasualty360.com)

A final coverage, computer system extortion coverage, may also be useful to protect businesses against hackers holding confidential data for "ransom." Often compared to kidnap and ransom coverage, this coverage provides funds that can be used by a company to investigate extortion threats and/or pay extortion losses, when a hacker gains access to company systems and demands payment to not disseminate the confidential information.

### SAFEGUARDING SECURITY THROUGH PRECAUTIONS

Preventive measures go hand in hand with insurance to protect businesses. Companies can take precautions to greatly reduce risk—and obtain better rates for insurance.

In general, underwriters providing coverage against privacy breaches will look first to see how much priority a company places on the protection of its databases. Insurers want to know if the business has hired qualified outside experts to review and enhance security procedures, and if those recommendations are being followed. Underwriters will need to learn who has access to the company's systems and if the information has tiered authority levels. The company should have dedicated people or groups assigned to protect the integrity of protected data.

Underwriters also look closely at information about encryption of data, password

procedures, backup procedures including off-site backup of data, disaster recovery plans, intrusion prevention systems, and the use of anti-virus tools.

### AGENTS AND BROKERS PLAY A VITAL ROLE

In a computerized and connected world, privacy concerns affect nearly every business—and the costs of a data breach due to hacking or accidental release can run into millions of dollars. Obviously, this is a risk that should be insured by any business handling confidential data.

So the next time you are reviewing coverage with miscellaneous professional liability clients, don't overlook these privacy exposures.

Insurers have made it fairly easy to buy the coverage clients need when safeguarding information has become a critical part of nearly everyone's business. **AA&B**



**Paul Miskovich** is senior vice president and cyber/tech program manager for AXIS PRO, a business unit of AXIS Insurance. Miskovich is a licensed P&C insurance broker and attorney in New York and New Jersey. He can be reached at 908-508-4339 or at [paul.miskovich@axiscapital.com](mailto:paul.miskovich@axiscapital.com).



**Edward Seidl** is vice president and miscellaneous professional liability program manager for AXIS PRO, a business unit of AXIS Insurance. Based in Kansas City, Seidl can be reached at 816-292-7292 or by email at [ed.seidl@axiscapital.com](mailto:ed.seidl@axiscapital.com).

**AXIS PRO**<sup>®</sup>  
PROFESSIONAL • MEDIA • TECHNOLOGY