Cc

Chris Christian, CIC, RPLU

Information for Insurance Professionals In the Know

Mini-White Paper on Information/Data Risk

Background:

An insured may have control over three kinds of information, the misuse or loss of which can cause harm.

- Private information (social security numbers, drivers licenses, bank account, credit card, address, familial connections, etc.)
- Medical information (illnesses, prescriptions, physician relationships, prognoses, genetic predisposition)
- Mission critical information (client-specific data used to deliver services, file documentation, billing information)

Loss or impairment of the first two types of data can result in third party liability. Loss or impairment of the third type can result in business interruption.

From whence does liability arise?

Inherent in an insured's relationship with its clientele is faith on the clientele's part that it will be no worse for dealing with the insured than if it had not done so. When a client puts its private, sensitive information in the insured's hands, it has a right to expect that information will not be intentionally, accidentally, or negligently used to harm the client.

This basic presumption has been bolstered by legislation in many states, and in some federal acts. Requirements for proper caretaking of private information are specifically codified for medical information, and are addressed in various legislative acts pertinent to certain industries, and in some cases, general business. These legislative acts require not only the proper securing of data, but also the notification of clients whose data has been compromised, among other actions.

Additionally, an insured may assume liability through commitments made in its contracts with clientele.

What kind of loss may occur?

A client whose data is compromised may become the victim of identity theft or other fraud. Fraud has long been an issue in an environment where the client may not be fully in charge of his or her faculties, or may be dependent upon others to take care of his or her estate or business and private affairs. This historical exposure has now been complicated by the rampant abuse of private information in establishing false identities, false accounts, false medical identities (to steal medical care), and false working credentials.

Any of these breaches of a client's identity could cause not only financial harm to the client, but also to his or her estate and/or beneficiaries, as well as untold amounts of stress, emotional distress, mental anguish, time and money spent repairing damage, getting records corrected, and so on.

Loss or impairment of mission-critical information also can compromise the insured's day-to-day operations and require costly data reconstruction or extra expense to operate emergency backup systems. As a side note, if the entity is not properly protected against loss of data, or does not have a plan to quickly replace lost data that is mission-critical, there could be liability to the directors and officers for failing to have such a plan, especially if the loss of the data negatively impacts the delivery of services or has other long-term detrimental effects.

Impairment, loss or misuse of data can occur through malicious actions of intruders, or can be perpetrated by employees. It can also occur accidentally, such as through transmission of data to an unintended recipient, or failure to shred sensitive documentation.

In addition to third party liability and business interruption exposures, the insured is at risk for a reputational loss. Due to requirements to disclose data breaches, it is no longer possible to keep such an event completely quiet. Add to the required disclosure the inevitable "word of mouth" publication of the event, and the insured can easily be harmed by common knowledge of its inability to safeguard sensitive information.

What coverages can be found?

Many policies today can provide coverage for third party liability for private and medical information. The scope of coverage can vary from web or network-based exposures to physical forms of data, and from solely outsider actions, to those perpetrated by an employee. Most policies will cover not only identify theft outcomes to data breaches, but also personal injury damages. Some will provide sublimits for notification costs, and for credit repair costs, as providing credit repair to breach clients mitigates the potential liability loss.

Some of these policies will also extend coverage to first party exposures. The causes of loss revolve around hacking, denial of service attacks, viruses, and other technology-driven actions. Many insureds rely upon their backup systems as protection from business interruption due to information loss. However, backup tapes may not be as current as expected, duplicate systems can be expensive, and technology-driven loss of data does not trigger an EDP policy or the business interruption provision of a property policy. Therefore, most insureds are bare on this exposure.