Does Your Employee Benefit Plan Need Cyber Liability Insurance?

By Brian L. Smith and Mark A. Dobrow, Segal Select Insurance Services

Technological advances, especially those involving electronic data storage, inevitably introduce new risks that public sector HR personnel need to be aware of and understand. Examples of data-storage media that can make benefit plan participants' personal information more vulnerable than ever before include discs, flash drives and, most recently, the "cloud." Future advances will likely introduce new vulnerabilities, making a foolproof system perpetually elusive.

Stories about improper disclosure of individuals' private information, also referred to as data "breaches," are common. Moreover, recent changes to the federal law protecting health information increase the likelihood that more data breaches will come to light. (See the sidebar, "Background.")

Typically, insurance purchased by employee benefit plans does not adequately cover improper disclosure of participant private information, even if those policies do not specifically exclude data-breach events. Fortunately, however, there is a product available in the marketplace designed specifically to help protect against these exposures: cyber liability insurance (also known as "data-protection insurance").

Although it is easy to view cyber liability as an IT or a benefits issue, public sector HR personnel need to be aware of what is happening and what can be done to protect their stakeholders, such as employees and resident citizens—as well as the state or local government—from the inadvertent disclosure of personal information. This article presents an overview of cyber liability insurance. It describes various ways in which data security can be breached, addresses the legal consequences and clarifies how cyber liability coverage applies when data has been breached.

Types of Data Breaches

There are three general types of data breach:

- ***Breaches Due to Computer System Failures*** Examples of this type of breach include computer malfunctions that accidentally distribute personal information in some fashion, such as via a mass email, in a Web posting or on printed material.
- ***Breaches Due to Employee Mistakes or Negligence*** Examples of this type of breach include information sent in misdirected emails, posted inadvertently on a public-facing network, lost on devices such as laptops, smartphones, and discs/thumb drives, or even contained in mishandled paper records.
- ***Breaches Due to Malicious Acts by Employees or Third Parties ("Hacking")*** Such breaches can occur and go undetected because of security weaknesses that permit entry by viruses or network vulnerabilities that allow "trojans" or "phishing." Hacking of this type compromises the network and allows the theft of participant data in the period during which the breach is undetected.

All of this personal information can be used to perpetrate identity-theft schemes or other crimes, including cyber extortion, where public disclosure of the information or sale to other cyber criminals is threatened.

Potential Consequences of a Breach

The vast majority of states now have privacy laws that apply to entities that use or store sensitive health and non-health personally identifiable information, as defined in the applicable statute. There are also federal rules protecting such information. As noted in the sidebar "Background," the Health Insurance Portability and Accountability Act (HIPAA), the federal law that governs the privacy and security of individuals' protected health information (PHI), was amended by the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act to include a breach notification requirement. These state and federal laws, and their related regulations, have established various requirements to notify and protect affected individuals when the security of private information, whether held electronically or on paper, is breached. Many of these laws have standards of enforcement and compliance that approximate or exceed various provisions contained within HIPAA's HITECH rules, including, but not limited to, new or increased fines and penalties, stringent self-audit requirements and new authority for state attorneys general to pursue civil actions on behalf of state residents who are adversely affected by these violations. To avoid fines and penalties due to a breach event, various legal requirements must be met.

"Although it is easy to view cyber liability as an IT or a benefits issue, public sector HR personnel need to be aware… "

In addition to the fines and penalties that could be associated with a breach, a plan could face significant remediation-related expenses. On average, direct costs per breached record amount to approximately $70-$75, according to the Ponemon Institute, a

CONTINUED ON PAGE 14

CONTINUED FROM PAGE 13

research center on information security. The direct costs can include mailings to inform participants of the breach, free credit monitoring for each affected participant, identity-protection services, investigative costs involved in identifying what information was taken and how it occurred, as well as audit and consulting services, legal services related to compliance and public relations/communications services.

Protection That Can Be Provided by Cyber Liability Insurance

Cyber liability insurance, which was introduced in approximately 1999, has gained importance in recent years because it can help mitigate the liabilities associated with a data breach. Those liabilities might include administrative, technological and legal costs. Cyber liability insurance policies are intended to cover an entity's first-party breach costs (as described in the next paragraph) as well as to provide protection from third-party liabilities (described later in this section) that might result from a breach event.

The first-party breach costs that these insurance contracts are generally intended to cover include credit monitoring, forensic investigations and legally required notification expenses. The policy can also respond to cyber extortion threats, if that particular coverage provision is purchased. Subject to the limits of liability purchased, the coverage approach typically taken by these policies is to provide the insured plan with experienced professionals to expeditiously handle the fallout from a breach event. These professionals are a real "value added" feature of cyber liability insurance.

Attorneys who specialize in privacy compliance are typically assigned to assist the breached entity. Forensic experts might be engaged to stop an ongoing breach, fix the damaged network, restore data and attempt to prevent future similar breaches from occurring. Public relations firms are often provided to help in communications and call centers can help manage the deluge of calls that may follow notice mailings.

The team of experts that is assigned to handle the breach event will be supplemented by funds, the policy's limits of liability, provided by the carrier to cover not only the cost of the experienced professionals, but also the ancillary costs of providing legally required notification expenses, credit monitoring and the other first-party costs noted above. The policies are unique in that they will often be triggered, meaning the carrier will respond by providing the team of experts, while a data breach is still occurring rather than simply reimbursing incurred costs after the event takes place.

The other advantage to these policies is that they provide protection from third-party liabilities that may result from a breach event. Third-party liabilities are liabilities arising from individuals who allege that they have been harmed by the breach (*e.g.*, through actual identity theft leading to financial loss or injury to reputation due to sensitive health information being disclosed) and who might seek financial redress.

Some policies include limited regulatory proceeding coverage (coverage for lawsuits or investigations by federal, state or municipal regulators relating to privacy laws) and extend the policy to cover certain fines and penalties that may also be assessed, if they are allowable by law. Like many insurance policies, these policies provide unique coverages, are subject to negotiation and continue to evolve.

When a plan considers purchasing cyber liability insurance, it must carefully scrutinize the scope of coverage provisions because policies can be very different. For example, while most policies have similar definitions of what constitutes a breach event, their obligations to respond with specific coverage such as financial, legal or technical assistance can vary greatly. Some will cover notification to affected parties only if there is a *legal obligation* to do so or if the *insurance carrier* decides there is a risk of harm that would be mitigated by disclosure. Some will cover notification on a voluntary basis where it is up to the insured to decide to notify participants even if there is not a legal obligation to do so.

In addition to a careful review of the coverage available, plan sponsors considering cyber liability insurance should be prepared to answer the list of questions from potential providers noted in the sidebar "Questions to Address Before Seeking a Quote for Cyber Liability Insurance." Their answers to these questions will largely determine the coverage terms.

Conclusion

Given the continuing need for plans to adopt ever-greater levels of technology for administrative efficiency, the risk of inadvertent disclosure of personal information is real and might be escalating. Regardless of the investment made in protecting and securing networks, the networks continue to prove vulnerable to human error and malicious or criminal attacks. The latter are a particular cause for concern because of their prevalence and the fact that they are the most expensive to handle.

Cyber liability insurance is a valuable risk-mitigation tool that helps to cover first-party costs and third-party liabilities from some of the consequences of a breach of personal information. With the rising incidence of cyber breaches, increased regulatory enforcement and the costs associated with both, HR may wish to learn more about this insurance and consider whether adding this protection to their insurance portfolio makes sense.

Brian L. Smith is the Chief Operating Officer of Segal Select Insurance Services, Inc., the insurance brokerage subsidiary of The Segal Group, Inc. He has 40 years of experience in insurance brokerage. Smith can be reached either by phone at (212) 251-5333, or by email at ***bsmith@segalsi.com****.*

Mark A. Dobrow is a vice president and consultant with Segal Select Insurance Services, Inc., the insurance brokerage subsidiary of The Segal Group, Inc. He can be reached either by phone at (312) 984-8660, or by email at ***mdobrow@segalco.com****.* —*N*