CYBER LIABILITY COVERAGE FOR NON-PROFITS

News of cyber-crime and instances of massive data breaches are increasing each year. The headlines have been grabbed by major data breaches at discount retail chains, restaurant chains, financial institutions, video game developers, health care providers, government agencies and more. The Pew Research Center estimated this year that 18 percent of adults who engage in online activities have been the victims of stolen information, including Social Security numbers, addresses, or banking information – an increase from 11 percent in 2013.

And with each instance comes increased awareness of the need for cyber liability coverage, a painful but important lesson in the ways 21st century crime can infiltrate a business – and its customers' wallets. These infringements are happening with increasing regularity, breeding mistrust among consumers and wreaking havoc with companies that are left scrambling to pick up the pieces from these financial (and public relations) disasters. As a result, some estimates indicate that cyber liability insurance sales will double in 2014 from $1 billion just last year.

However, one group that has been relatively overlooked in conversations about data theft, firewall infringements, and complex malware programs associated with cyber liability is nonprofit groups – organizations that are particularly vulnerable because they often lack adequate manpower, are dependent on volunteers and frequently operate with limited capital. They may not have the resources to properly protect their infrastructure and, equally as alarming, detect when such a breach has occurred. Imagine how hard it would be for a nonprofit to raise funds following a breach of private information belonging to current donors. It may also be difficult to recruit new volunteers if the confidential information of current volunteers is compromised. The survival of the nonprofit organization would be at risk if a data breach weren't handled quickly and appropriately. The typical cyber liability insurance policies in the marketplace include things like public relations expenses, forensics, notification, credit monitoring services, and call centers. Without that professional help from an outside group, the day-to-day operation of a nonprofit could come to a screeching halt.

Cyber crimes are not just the result of nefarious criminals in foreign countries executing complex and well-organized schemes. The data breach culprit could be someone who works for the nonprofit organization – a rogue employee, a disgruntled volunteer or even someone who holds no affiliation to the affected group. The most common instances of cyber crime are the result of a lost or stolen laptop that contains encrypted information that details organization finances or sensitive donor information. Along with hacker events, human error or negligence are leading causes of data breaches.

Nonprofits have traditionally not been a targeted class for cyber liability insurance, but that's changing. Because they may be at a higher risk for breaches, nonprofit groups are the subjects of increased inquiries and endorsements as part of cyber liability protection. For example, the State of Michigan requires that it be included as an additional insured, for vicarious liability purposes, in the event that a nonprofit group with which it is affiliated is a victim of hacking or information theft. Many carriers have not been aggressive in their writings for cyber liability protection for nonprofits because the exposure can be just as large as a for-profit organization, but nonprofits may not have the funds to pay the appropriate premium.

Cyber crimes are only likely to increase, and no organization, regardless of its size, scope, or reach, is immune. As the demand for nonprofit cyber liability protection increases, it is important to know that there are a variety of very affordable solutions that exist to protect your client. From tweaking existing contracts, to adding additional insured clauses or co-defendant wording, your AmWINS Financial Services Practice is available to help you navigate this emerging and challenging coverage.

This article was authored by Kendra Schaendorf, an assistant vice president with AmWINS Brokerage of Michigan and member of the firm's financial services practice.