Can the Right Insurance Help Mitigate Cyber Risk?

By Diane McNally

In today's hyper-connected world, the chance of losing valuable protected data to careless keystrokes or clever hackers is greater than ever. Even using the best and most secure industry software, it is impossible to eliminate the risk of a breach, especially since many breaches result from negligence or due to employee errors.

As cyber laws and regulations become more restrictive, expect even greater costs and responsibilities.

Photo Illustration © 2019 iStockPhotos.com

Are Benefit Plans Fully Covered by Vendors' Insurance?

While vendor contracts should stipulate their obligation in a beach, trustees or committee members may be liable for their plan's data no matter where it resides and how protected. Even if vendors have cyber liability insurance with adequate policy limits and a well-maintained data incident plan, scenarios exist where a benefit plan's own coverage is needed, such as:

- The vendor improperly responds or neglects to respond to a breach.
- A large-scale breach is beyond insurance limits or forces a vendor into bankruptcy.
- Plan trustees inadvertently release sensitive data.

With these and other possible scenarios occurring, purchasing the right coverage is one cost-effective way for trustees to manage risks.

What is Cyber Liability Insurance?

Cyber liability insurance covers unauthorized (malicious or accidental) access to and/or disclosure of personal information. The policy provides experts to respond to a breach and pay associated direct notification costs. The policy also provides defense, settlement, and judgment coverage should a third party sue for financial damages. These services are not covered by other insurance, and their costs may become the responsibility of the public sector plan or the trustees.

Comprehensive cyber policies typically offer:

- **Breach Notification Teams**
  - In the event of a breach, the policy provides forensic, legal, and public relations experts.
- First-Party Breach Notification and Remediation Costs
  - Most Cyber liability policies will pay for notifications to those affected – no matter their residence location in compliance with applicable state, federal or even foreign country's laws – and provide discounted services for call centers, credit monitoring, and identity theft remediation. This avoids engaging expert services mid-crisis at inflated non-negotiable rates.
- Third-Party Liability Coverage and Fines
  - Even when first-party notifications are handled properly, litigation and fines may follow from impacted participants and governmental agencies. This liability coverage addresses allegations of negligently mishandling data as well as improperly notifying participants – the primary reason a separate cyber liability policy is sought.
- **Expert Technical Support**
  - Most insurers offer access to websites dedicated to reducing cyber liability exposures containing articles, statutory law reviews, forms and templates, sample information security policies, loss scenarios, and other relevant information.

CONTINUED ON PAGE 10

INSURANCE CONTINUED FROM PAGE 6

In today's increasingly vulnerable environment, public sector plan sponsors need to view breaches not as "if" events but rather as "when" events and to consider all measures – including an appropriate cyber policy – to protect the data they hold and maintain. Legal counsel should be consulted to fully understand liability the trustees and plan may face were a breach to occur. As laws change, these conversations should happen on an annual basis. ◆

Diane McNally *is a Senior Vice President and Principal in Segal Select Insurance's New York office.*

The Voice for Public Pensions

PERSist is published by the National Conference on Public Employee Retirement Systems.
Website: www.NCPERS.org • E-mail: amanda@ncpers.org