

Insurance for Cyber Risks



By Melanie Lockwood Herman

Executive Director

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity, Insurance and Risk Financing

Today's nonprofit leaders are aware that dependence on data, software, systems and tech vendors brings untold benefits as well as potential downside risks. From the impact of data loss to claims alleging the failure to safeguard personal information, a nonprofit's reputation and resources are 'on the line' in the online age. Effective risk assessment and risk management can help an organization's leaders feel confident that appropriate steps have been taken to minimize the likelihood of a downside risk. Strong risk protocols and preparation can instill confidence that the nonprofit will do the right thing should a data loss, breach of privacy claim, or vendor error occur.

Once risk assessment and risk management are in place, it's time to consider risk financing: how will we pay for the cost of losses and harm we're unable to avoid?

During the March 2013 webinar on "Cloud Computing Risks," hosted by the Nonprofit Risk Management Center, Matt Prevost, AVP of Cyber and Professional Liability at Philadelphia Insurance Companies provided expert commentary on the insurable exposures related to cloud computing and storage. Matt's comments covered factors that underwriters consider in underwriting cyber coverage, as well as common mistakes that nonprofit insureds make when they migrate to the cloud. Matt graciously agreed to answer some follow-up questions, to help RME readers understand the nuances of cyber exposures and coverage.

MELANIE. *Matt, you mentioned in the webinar that nonprofit insurance buyers often make potentially dangerous assumptions when they rent server space from a cloud company. In your experience, what are the most common assumptions, and why are they dangerous?*

MATT. In some cases, nonprofits that elect to outsource data storage assume that the security somewhere else is better than what they currently have. That may be the case, but often times is not. The other wrong assumption is that the contractual relationship between the nonprofit and the technology provider adequately protects the nonprofit. These contracts often shift responsibility to the nonprofit rather than the technology provider. Additionally, within these contracts, the technology provider has minimal risk for regulatory or legal compliance, because the nonprofit retains full responsibility for the data it owns and stores. One exception is personal health information. Technology providers are now finding themselves subject to the expectations of HIPAA as business associates.

"Most stand-alone cyber products are scalable. What that means is that they offer a menu of

insuring agreements from which the nonprofit insured can choose.”

MELANIE. *During the webinar you explained that nonprofits can purchase coverage for costs they incur in the wake of a data loss/privacy breach (“first party losses”) as well as losses suffered by others for which the nonprofit may be liable (“third party losses”). Is it possible to buy a policy that addresses both coverages or are separate policies required?*

MATT. Most stand-alone cyber products are scalable. What that means is that they offer a menu of insuring agreements from which the nonprofit insured can choose. And a growing number of companies offer cyber endorsements to other coverage lines. These endorsements are typically sub-limited with relatively low limits and tend to be in line with either third party exposures or first party exposures.

MELANIE. *I’m aware that Philadelphia has a very large book of nonprofit business. Can you estimate what percentage of your nonprofit customers buy cyber liability coverage?*

MATT. Without giving actual figures on Philadelphia’s book, I would estimate that less than 15% of all nonprofit organizations purchase coverage. Most nonprofits are just now becoming familiar with their exposure to cyber risk. With that new awareness comes interest in the insurance products available to finance those exposures.

MELANIE. *Do you see an uptick in interest following widely publicized privacy breaches, such as the recent cases involving Sony and TJ Maxx?*

MATT. We do. At the same time, there are smaller breaches publicized almost daily in local newspapers that tend to get more attention. Small and middle market nonprofit insurance buyers can relate to those smaller breaches much better. We have seen a significant interest following recent HIPAA enforcement as well. Many types of nonprofits are covered entities under HIPAA (e.g., clinics, mental health organizations, social service organizations). As covered entities they can envision the financial burden (e.g., damages, fines and penalties) that would result from claims alleging violation of HIPAA.

MELANIE. *When nonprofit leaders ask us what coverage limit they need, we generally explain that there is no formula for determining the right limit for a particular policy. Affordability is obviously an issue, but it’s hard to predict what a liability claim will cost. Since cyber-based data loss and privacy breach claims are still relatively new, I imagine there isn’t a lot of data on what these claims cost generally. How should a nonprofit go about determining the appropriate coverage limit for a cyber liability policy? What deductibles are typically available for this coverage?*

MATT. Many carriers, including Philadelphia Insurance Companies, have risk management resources built in to their policy premiums. Philadelphia’s eRisk Hub, powered by NetDiligence, provides potential policyholders and current policyholders with access to data breach cost calculators, notification costs calculators, as well as updates to the regulatory and legal climate.

MELANIE. *Are there any key features of coverage that affect pricing?*

MATT. Key underwriting components include: total annual revenues, the type of PII (personally identifiable information) or PHI (private health information) the nonprofit collects, the number of records, and most importantly, the level of cyber risk controls an insured has in place or is willing to implement.

MELANIE. *You mentioned during the webinar that there are more than 40 markets (insurers) that provide various forms of cyber coverage. Are there dramatic differences in policy forms, or is coverage offered on Insurance Services Office (ISO, www.iso.com) or other common forms?*

MATT. There are dramatic differences in policy forms and it is important to work with an agent or broker who understands those differences. Like with any insurance product, it is most important that the policy responds to your needs. For example, if your nonprofit doesn’t have the funds to retain PR help in the wake of a data breach, a cyber policy that would cover these costs for an affordable premium is a great alternative.

MELANIE. *Last question. What approach do you recommend for getting a handle on cyber property and liability exposures? Are there a few key steps that our nonprofit readers should take?*

MATT. Awareness and preparedness. Not only awareness of how important it is to securely store data (especially the most sensitive forms of data-PHI, PII and confidential information) but also being aware that losses occur every day in both small and large organizations. Having minimum controls (typically outlined in cyber insurance applications) can prevent most privacy or data breach events, but being prepared and knowing how to react following a breach is imperative. If you're a nonprofit professional and are looking to learn more about this growing risk, reach out to your agent, broker or carrier for help.

MELANIE. Thanks for sharing your valuable insights on a truly timely and complex topic.

Melanie Lockwood Herman is Executive Director of the Nonprofit Risk Management Center. She welcomes your feedback on this article and questions about the Center's resources at Melanie@nonprofitrisk.org or (202) 785-3891. Matt Prevost is Assistant Vice President, Cyber & Professional Liability at Philadelphia Insurance Companies. Matt welcomes your questions about any of the topics in this article at Matthew.Prevost@phly.com or (610) 538-2203.