Demystifying Cyber Liability Insurance

By Whitney Thomey

Lead Consultant & Risk Ethnologist

Resource Type: Articles, Risk eNews

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

Every nonprofit that collects and stores confidential information, Personally Identifiable Information (PI), or Protected Health Information (PHI) is vulnerable to a costly data breach and its consequences. Data breaches, denial of service attacks, and phishing scams are a sampling of methods that cybercriminals use to steal and extort data.

Organizations must remain vigilant and implement security protocols to safeguard their missions and critical data. However, establishing secure technology protocols and having best-in-class technology solutions isn't enough. Nonprofits shouldn't only focus their efforts on how to prevent cyber risks from materializing; they need to plan for *when* cyber threats happen. Restoring lost data and systems and responding to lawsuits resulting from breaches are potentially costly and time-consuming tasks; your response could tap critical funds and staff resources away from programs and services that are the lifeblood of your mission.

Consider the following statistics:

- Breaches affect organizations of all sizes and can be costly. The NetDiligence 2019 *Cyber Claims Study* reported 96% of claims were made by organizations with less than $2 billion in revenue, and a maximum breach cost in the nonprofit sector could be as much as $1.6 million.[1]
- It can take a long time to discover a breach. A study by IBM indicates that it can take as many as 280 days to identify a breach.[2]
- Breach containment response time is a critical factor in associated costs. Unsurprisingly, the size of the breach affects containment time; a mega breach can take up to 365 days to contain.[3]
- The average cost of lost records in 2019 was approximately $146 per record.[4]

Cyber Liability Insurance is an increasingly affordable option for financing the cost and consequences of a data breach. However, whether you decide to purchase—or forgo—this coverage, taking time to understand how the coverage works and what it covers is well worth the time required. At a minimum, nonprofit insurance buyers should understand what types of claims are covered, claim limits, and how to file a claim.

NRMC invited a panel of thought leaders from the insurance and legal industries to explore key questions, common misconceptions, and how to avoid mistakes when filing claims. Our panel consists of:

- **Ryan FitzSimmons**, Divisional Vice President of Operations, Great American Insurance Group, Cyber Risk
- **Scott Konrad**, Senior Vice President and Not-for-Profit Practice Leader with Hub International Northeast,

and member of NRMC's Corporate Advisory Committee
- **Keith Moulsdale**, partner and co-chair of the Cyber Security, Information Management & Privacy practice at Whiteford Taylor & Preston

Q&A: What You Need to Know About Cyber Liability Insurance

NRMC: *What's the top misconception about cyber liability coverage?*

Ryan FitzSimmons: A common misconception is that you automatically have enough cyber liability coverage as part of your commercial package or Business Owners Package (BOP). If you're looking for the most tested, most encompassing coverages in the marketplace, you need to purchase a stand-alone cyber risk product. Not all cyber endorsements to other insurance products are created equal. While there is some additional expense and effort involved with a stand-alone purchase, it's well worth it to ensure the limits and scope of coverage are adequate for your organization's needs.

Scott Konrad: Many charitable organizations assume they're improbable targets because they're too small, don't have information that would be valuable to cybercriminals, or they outsource certain technology. All are naïve assumptions.

Although some breaches occur because of technology lapses or criminal actions, a surprising number are attributable to simple human error. The duty to safeguard data is non-delegable– so that, even if an organization outsources payment or CRM functions, it's the one ultimately responsible to regulators and victims. The May 2020 Blackbaud breach poignantly illustrates how easily nonprofits can wind up in the soup for events they didn't even cause.

Keith Moulsdale: It's a common misconception that all cyber insurance coverage is created equally and that all policies cover both first- and third-party losses. In fact, there can be vast and material differences in cyber-related policies that can have a real impact on the policyholder. For instance, some policies only insure incidents that occur on a server that is owned or operated by the policyholder and don't cover incidents that occur on servers hosted in the cloud or incidents that are connected to a vendor. With nonprofits moving rapidly to cloud-based solutions, this should be a key focus for organizations shopping for insurance.

Some policies don't cover acts of cyber "terrorism" or "acts of war." Those exclusions can be a real problem given the extensive and growing scale of incidents sponsored by nations such as Russia, China, and Iran, especially when the US or another Western government publicly recognizes that a particular hack was state-sponsored, such as in the case of the "NotPetya" cyber-attack in 2017 that was attributed to Russia.

Also, many cyber policies don't cover phishing-related financial losses. Such losses occur when a fraudster gains access to an email system and then tricks someone in accounts payable into paying the fraudster instead of a legitimate vendor; those types of losses are more likely to be covered under a separate crime policy. Some policies cover governmental or third-party fines, but others don't.

The list of possible material differences in policies goes on and on; this is why I routinely tell clients that perhaps the most important thing they can do when shopping for cyber liability coverage is to hire a broker that fully grasps the complexities and nuances of cyber risk. Ideally, this would be a broker specializing in such risk and who will suggest appropriate policies only after engaging in reasonable due diligence about the prospective policyholder's unique cyber-related first- and third-party risks.

NRMC: *What's the top mistake policyholders make when they have a claim?*

RF: Too often, policyholders don't involve their carrier soon enough in the event of a claim. Time is of the essence in cyber claims management, and while it seems like you need to get things moving right away with lawyers and vendors and consultants, bringing that all together in the midst of a crisis is difficult at best. Most carriers have a pre-contracted list of top-notch vendors at the ready. With one phone call, you can bring all of those resources to bear and secure the most favorable rates from those experts. Your cyber carrier is your most significant resource. Don't go it alone.

SK: Some tend to panic and act without reading their insurance policy terms and conditions. Most policies have strict requirements governing notice to the insurer and gaining its prior consent to engage professional services

or incur expenses. My strong advice is always to contact the placing agent/broker/risk advisor FIRST—and to be guided by its counsel; that intermediary can notify the insurer and mobilize resources.

KM: Three mistakes rise to the top of my list. One is failing to notify the insurer of a possible claim in a timely fashion. Failing to do so could cause the insurer to deny the claim.

Another common mistake is engaging lawyers or forensic specialists who aren't on the insurer's pre-approved list or have not been screened and approved by the insurer. Failing to get approval for the organization's preferred lawyer or other breach response professionals could cause fees and expenses charged by those professionals to be denied or limited.

But perhaps the biggest mistake of policyholders is trying to resolve an incident on their own without consulting with professionals who specialize in cyber incidents. Often, doing so entails a policyholder using a well-intentioned internal IT person to "remedy" an incident, but more often than not results in that person making mistakes that negatively affect the investigation, such as by reconfiguring logs in a way that actually deletes logs that include critical information about the incident.

NRMC: *What's the top uncovered claim that nonprofits submit?*

RF: One of the top uncovered claims is fraudulently induced payments from socially engineered scams like business email compromise. Often, the limited scope of coverage in cyber endorsements does not include this feature unless you ask for it and pay the additional premium.

SK: For organizations that buy cyber protection, I actually haven't seen any non-covered losses! The state-of-the-art in policy design has advanced tremendously over the past 15 years, so that today's breed of products generally address (1) civil liability and regulatory matters, including defense, fines, and penalties; (2) breach response costs; and (3) first-party loss to the policyholder's own network and digital assets, including direct and contingent business interruption. Even economic loss from reputational harm is often covered, as is Multimedia Liability (for both online and offline content).

KM: The top uncovered claim that we see are claims for losses arising out of a so-called "business email compromise" where an employee or agent of the policyholder was tricked into sending money to a fraudster.

NRMC: *Who are the top carriers covering cyber losses for nonprofits?*

RF: Given the frequency with which buyers are coupling their cyber risk insurance purchase together with other coverages, like their package policy or Directors & Officers (D&O) policy, it is likely that the top carriers covering cyber losses are also the leading writers of those other lines. However, as stand-alone products become increasingly available in the admitted marketplace, we expect to see movement toward specialty carriers to accelerate.

SK: There are over 100 markets playing in the space: a combination of the household-name mega-players and newer niche specialists. Everyone's vying for market share, and the cyber segment is one slice of today's turbulent market that's remained intensely competitive. Every broker has its favorites, but we've had great success with companies such as Beazley, Chubb, and AIG for stand-alone policies, and Travelers and Zurich when bundling Cyber with other companion lines such as Management Liability and Crime. There's certainly no shortage of options.

KM: There are a growing number of good cyber liability and loss carriers, but I routinely see suitable policies offered by Axis, Chubb, CNA, and Travelers.

Whitney Thomey is Project Manager at the Nonprofit Risk Management Center. She welcomes your follow-up questions about any of the topics covered in this article at 703.777.3504 or Whitney@nonprofitrisk.org.

---

[1] NetDiligence: Cyber Claims Study 2019 Report

[2] IBM: Cost of a Data Breach Study

[3] IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses

[4] CSO: What is the Cost of a Data Breach?