Why Nonprofits Can't Afford to Ignore Cyber Risk

White Paper
Provided by HUB International
Published October 2020

HUB

In the Beginning

In 2007, a household-name nationwide nonprofit organization bought one of the first cyber insurance policies, over the objections of its CIO, who was convinced she'd built a bulletproof technology infrastructure. Not a week after the policy was bound, one of the organization's executives took a short cab ride from one side of Manhattan to the other. He alighted at his destination, paid his fare, and moments later, realized that he'd left a company laptop in the cab.

The accidental loss of an expensive device was, it turned out, the least of the organization's problems. Far worse was the potential leakage of sensitive data on the laptop's hard drive.

Even in those pioneer days of cyber liability, consumer protection law treated the loss of a device laden with personally identifiable information (PII) as a breach, triggering a host of obligations starting with precautionary notification to potentially-affected parties. By the nonprofit had completed its incident forensics and consumer notification, volunteered some credit monitoring services, and done PR damage control, it had burned through nearly $100,000 in breach response costs…in a matter of several weeks. Fortunately for the organization, it had the right insurance in place.

The Stakes Have Increased

Fast forward to present. Laws now exist in some 47 states, the District of Columbia, Puerto Rico, Guam, and the US Virgin Islands defining the circumstances that constitute a breach and prescribing the responsibilities and actions that the data owner must take in the wake of such an event. Predictably, the laws vary from state to state -- and, perhaps most complicating, the law of the affected person's home state is the one that governs.

This means that an organization with an interstate listserv can be trapped in a virtual spider web of conflicting laws, regulatory enforcement actions, and zealous attorneys general. The challenge is compounded for organizations pushing data through other countries with the advent of the European's General Data Protection Regulation (GDPR) and country-specific laws.

According to Ponemon Institute, which tracks cyber security incidents, today's cost of a data breach across all industry segments averages $150 per record, and nearly double that figure in healthcare and high education. The overall cost of an average breach – 'hard' costs plus financial ripple effects -- ranges between $1 million and $7 million, depending on the industry (IBM Cost of a Data Breach Report, 2020)

What's the Exposure?

Cyber risk takes several forms, including first-party loss (damage to the organization's own IT infrastructure and digital assets, and breach response costs); civil liability for damage to others' networks and digital assets, and for unauthorized release of private information; and regulatory fines, penalties, and defense costs.

CYBER MYTHS DEBUNKED

Despite high-publicity breaches affecting TJX, Home Depot, Anthem, Sony, JPMorgan Chase, eBay, Marriott, Equifax, and the federal government -- organizations with legions of IT engineers and huge budgets – a surprising number of nonprofit executives remain nonchalant about cyber risk. They explain that (1) they don't have many records; (2) they don't believe they'll be targeted by hackers; and (3) they outsource technology functions such as credit card processing, data storage, and cloud-based software-as-a-service (SaaS).

YET CONSIDER THAT:

- An incident compromising even a few records could thrust the organization into the harsh media spotlight, damaging brand, reputation, and threatening funding and stakeholder relations amid perceptions of lax business practices. A 2020 ransomware attack on Blackbaud, a specialty technology provider to the charitable sector, reportedly compromised data from over 100 nonprofits, blemishing the company's name and triggering class action litigation.
- Lost/stolen devices and human error account for roughly one-quarter of today's breaches, with system glitches representing an equal share and malicious attacks filling out the remaining 50%. (IBM Cost of a Data Breach Report, 2020).
- Outsourcing to a technology contractor doesn't absolve the data owner of its statutory responsibilities. At best, it simply provides another payment source --assuming the deal terms clearly affix liability with the contractor for its own acts, errors and omissions. Even if the technology contractor has agreed to indemnify its nonprofit client and hold it harmless, its ability to fulfill that commitment hinges on the integrity of the contractor's insurance and its own financial health. Consider, too, that a major breach on the contractor's end could affect its entire client base, exhausting even the most robust insurance protection and leaving the unwitting nonprofit without remedy.

Ponemon data indicates steady growth in malicious attacks, increasing risk of revenue disruption, and higher-than-ever breach response costs that increase in direct relationship to the time it takes to discover and address a cyber event.

Be the Prudent Steward

Nonprofit leaders have an obligation to be prudent stewards of the organizational assets entrusted to their care. Diligence is one of three core responsibilities of any director or officer -- and it includes informed decision-making.

The first step for any organization is to assess its information risk exposure by (1) determining the approximate number of records it owns that contain protected information -- from employees, clients, donors, contract partners, and other sources; and (2) assessing the integrity of its technical, administrative, and physical safeguards. Defensive measures can range from firewalls, antivirus protection, and encryption to background screening, access restrictions, regular equipment inventories, and physical security.

The second step is to explore the availability and cost of commercial risk transfer. Today's specialty insurance products have proliferated and evolved to modular offerings that can address up to half a dozen discrete risk exposures, including reputational damage, social engineering (fraudulent impersonation) and media liability arising from online and offline content.

Responsible stewardship thus requires looking at the whole picture: quantifying an organization's risk, the costs to address it, and adopting a thoughtful, holistic strategy.

Today's Cyber Market Landscape

Despite several high-profile breaches involving merchants, financial institutions, and a credit reporting agency, the cyber insurance marketplace has been intensely competitive for the past decade. Buyers have found ample market capacity, generous terms, and pricing that most first-time shoppers consider reasonable – especially compared to the prospect of an uninsured loss, no matter the scale.

The onset of the COVID-19 global pandemic unleashed a spike in ransomware and other attacks perpetrated upon remote workers, including one resulting in a $7.5 million loss to a community federation's endowment. This uptick in activity, coupled with firming of the global insurance marketplace at-large, has spurred single-digit percentage cyber rate increases.

A comprehensive information risk management program should be rewarded in better-than-average rates, however, and assumption of more front-end risk through higher deductibles/retentions will help to keep a lid on cost.

One caution: don't bet on traditional property, casualty, crime, and management liability insurance policies to solve a cyber problem. At best, they contain only fragmented, limited
protection, and mainstream underwriters are continually introducing new exclusions to shift the burden away from their policies and into specialty solutions.

Conclusion

It's common knowledge that most nonprofits manage their expenses rigorously in order to conserve precious resources for mission. But mounting evidence suggests it may be foolhardy to dismiss cyber insurance as a luxury. Committing to undertake a cyber risk review this year may be one of the most important decisions that you'll make.

For more information, please contact:

Full name and title

Phone number

Email address