ASSESSING RISK TO MAXIMIZE CYBER INSURANCE COVERAGE

By Mark Millard

It's 8 a.m. on Monday. You open the doors to the office, preoccupied with tasks for the week: grant applications that need review, donor phone calls to make, staff disagreements to manage, current program execution and strategy for the future. As you settle into your desk and turn on your computer, the startup screen displays a simple message: "Pay 100 Bitcoin to 123 account number in the next 12 hours or lose all of your data." Panic sets in, your mind races, all thoughts from two minutes ago have disappeared. What do you do next?

These days, this type of scenario is all too common. Some make headlines, but most don't and are dealt with quietly and quickly. The challenge with many nonprofits is they reside in a place of reaction when it comes to IT infrastructure, security and crisis management. Many nonprofits walk the tightrope of pressure to reduce administrative expenditures and improve programmatic spending. Often, donors look at operating percentages when choosing where they will make their gifts. This challenge creates difficulties in determining how much to spend on IT infrastructure and cybersecurity.

The exposure to cyber intrusion for a nonprofit is often not adequately understood and, as such, marginalized by thinking that because we do work for the "greater good," the entity won't be a target. Unfortunately, cybercrime focuses on the ease and reward of opportunity, thus making many nonprofits a perfect target.

Before COVID, it was typical to find remote access driven by individual employees trying to find solutions to the work challenges and not organizationally driven by strategy. COVID and the exodus to a remote work environment have only exacerbated the issue. Many organizations have strung together technology solutions to meet the need for remote work. This rush to operationalize has been fraught with missteps and increased the risk for intrusion.

So what do you do with finite administrative dollars to spend? Do you spend the dollars on IT security and testing, training employees on proper cyber hygiene (e.g., “Don't click on that link”), crisis management and business continuity planning, or insurance? The answer is all of the above, while strategically prioritizing where you can't have everything on the shelf. Depending on your organization's IT security maturity, the quickest and most reliable risk mitigation you can take will be insurance. When adequately structured, it will be your most crucial risk mitigation effort.

Cyber insurance has been one of the fastest-growing and evolving products in the insurance market during the past decade. News of the mega-breaches that readily come to everyone's mind has driven this growth with many organizations recognizing the tremendous exposure to liability and business interruption resulting from a cyber intrusion. And what have we learned about cyber intrusions through the countless breaches we've read about over the years? They have many sources, are ever-evolving, impact organizations in different and unique ways and are challenging to stop, making a case for spending dollars on a cyber insurance policy that much more significant.

The problem we find with many organizations is their insurance approach and, more specifically, cyber insurance approach. Insurance is often a check the box mindset. Buy it once a year, pay a premium, receive an insurance policy and promptly place it in the drawer. This approach is always problematic, but less so for certain insurance types than others such as auto or workers' compensation insurance policies. Cyber insurance is the exact opposite of these aforementioned policies where there are standard forms and definitions and decades of claims experience providing a guide to what is and is not insured. Cyber insurance is the new kid on the block that everyone is still figuring out.

The cyber insurance marketplace is a highly fractured space that lacks a standard definition set and coverage provisions. There are over 100 insurance companies that underwrite the product with common coverages but little standardization.

For cyber insurance, most start with a basic coverage form. However, that form's value will depend on how well you understand your unique risk and negotiate the insurance policy's appropriate coverage. Many organizations have purchased cyber insurance, put it in the drawer, checked the box and moved on with their lives. Then the claim showed up.

Surprise, coverage denied. The conversation from there is typical: "Denied?!? I bought insurance for this." Yes, but you didn't buy the right insurance. You didn't understand your unique type and amount of risk, leading to the coverage gap. So what steps can you take to avoid this dreadful scenario and not spend precious funds doing so? Start by looking at the risk.

Broadly speaking, we bucket cyber risk into two categories; first-party and third-party losses. Or, in other words, damage to your organization's property and ability to conduct business (first party), and injuries to others due to your negligence (third-party). When determining the type of cyber insurance needed, we begin with risk management 101, identify the risk.

Risk can originate from an insider, whether intentionally or not, criminal hackers, hacktivists or third-party compromise. To understand your threat areas, start with a simple whiteboarding session with the key stakeholders in your organization—CEO, chief financial officer, Operations lead, IT, HR and others, and play through a few what-if scenarios to determine what would happen and the resulting operational and financial impact. Areas to focus on can include:

- Computer system damage and loss
- Data loss
- Business shutdown
- Fines and penalties
- Liability associated with data loss
- Reputational damage
- Theft of funds
- Extortion

It is essential to understand where these risks can stem from as insurance policies will have exclusions that limit coverage due to cause. For instance, an insurance policy might require that you provide all IT vendors' names that offer your organization services. The simple error of omitting one vendor can void coverage should the loss result from their services. Next, you will want to assign value to your risk areas to determine exposure to one or multiple impacts. Consider:

- The cost to replace your computer systems if required due to system bricking (damaged beyond repair, making the device unusable) for the first-party loss.
- Would you need to spend money to recreate data?
- Would you be subject to a business interruption where revenue generation would be reduced or ceased?
- Would you incur extra expenses to have temporary fixes or accelerate your recovery?
- How many personally identifiable information (PII) or protected health information (PHI) records do you maintain and what is the potential liability for losing these records?

As more and more entities are moving data to cloud storage, do not believe that this relieves you of liability exposure. In these instances, assessing risk transfer and protection through your contractual agreements will be important in addition to the protections you might take with insurance. Once you've built an understanding of individual risks and their value, you are ready to consider the type and amount of insurance to purchase.

Here is the good news. Cyber insurance options are plentiful, with broad coverage and reasonable prices compared to its early years. Obtaining a base cyber insurance policy for $1 million in limits can often be done for minimal cost. When purchasing cyber insurance, it will be critical to have a partner who understands the insurance coverage—further making this point. A recent advertisement from an insurer for NFP cyber insurance provided a listing of the policy coverages: Privacy Liability for release of PII or other corporate confidential data, network security liability, media liability and breach response costs. At first glance, this might look great. The policy will cover the third-party liability aspects. Also, it has coverage for breach response costs, which we will explore in a moment. But what is missing? There is limited first-party coverage and no coverage for system damage resulting from the breach. Given the check-the-box insurance approach discussed earlier, these insurance policies' deficiencies often go unnoticed until a claim arises.

So what should you look out for in a well-structured cyber insurance policy?

Privacy liability – coverage for damages associated with the release of personal information

Network security liability – coverage for failure to prevent an attack against your network

Media liability – coverage for liability associated with content you create and distribute

Breach response costs – coverage for direct costs associated with a breach (This can include credit monitoring, forensic and remediation services, and public relations costs.)

Property damage directly resulting from the breach – coverage for replacement and repair of systems damaged from the breach

Income loss, extra expense and dependent business income – coverage that protects against lost revenue due to a service disruption or network outage

Data recovery – coverage for costs associated with recreating data lost or stolen

Extortion – coverage for payment for a demand placed by the cybercriminal

System failure – coverage for unintentional outage resulting from an error

Regulatory fines and penalties – coverage for payment of fines assessed by a governing body associated with a breach

In addition to these coverages, cyber insurance policies have evolved to provide liquidity relief and a service tool with crisis management, breach response and even some systems diagnostic services. Many cyber insurance policies offer a specific panel of specialists on call and available for the insured's use in a breach. For the nonprofit community, these additional services can be worth as much as the insurance policy's liquidity relief.

So as you look to spend your finite administrative dollars, a key part of your cyber risk mitigation strategy should focus on the purchase of a cyber insurance policy. When properly structured, it is the one protection you can count on when all other security measures put in place fail.