TECHIMPACT®

NONPROFIT CYBERSECURITY INSURANCE CHECKLIST

Cybersecurity insurance is becoming a must-have for nonprofits. What do you need to know about the requirements providers will expect to see before issuing your organization a policy?

Here's a hard truth: Even if you identify the risks, weigh your tolerance for risk, and create a culture of security to keep your assets safe, your organization might still get hit by a cybersecurity attack or data breach. You can't protect against every possibility or every threat—there are too many of them, and they're evolving too quickly.

So what happens if a breach occurs? What are your organization's vulnerabilities? Will you have the resources and cash flow to recover quickly? What is the financial risk to your organization if data is lost or your operations are suspended?

Just like if you suffer a fire or robbery at home, you should have a plan for recovery from a breach or loss at your organization. You probably also have insurance to reimburse you for damages or losses at home—did you know you can also buy cybersecurity insurance to reimburse your organization if a catastrophic event becomes a reality?

No insurance policy will prevent a data breach or a technology failure, but it can help you protect your organization from downtime, reputation loss, and financial ruin. According to a Kaspersky study, the average loss to an organization from a single cyberattack has exploded from $34,000 to just under $200,000.

Insurance can defray many of those costs. It can cover the cost of replacing hardware, the time and consulting services needed to recover data and clean up an infection, lost

revenue, lost productivity, public relations and communications work, fines, litigation, and more. It can also cover third-parties—for example, injuries or harm to constituents as a result of your organization being unable to carry out its services.

Developing Your Policy

Every cybersecurity insurance policy is written specifically for the organization it covers, and the costs reflect the specific details of the policy. If you're interested in cybersecurity insurance, you'll work with a broker to evaluate your organization's risks and its systems to mitigate those risks. Every risk and every mitigation effort are reflected in the cost of your policy. If you have Multi-Factor Authentication (MFA) implemented, for example, the cost of your policy will go down, but if you don't have reliable backups, your costs will be higher. If you're not sure how to prioritize your security dollars, the insurance evaluation will help you see the benefits in terms of monthly premiums.

Choosing a Provider

The cybersecurity insurance market is barely two decades old, so many companies are still trying to figure out the actuarial liabilities and how they connect to prevention efforts. The good news for nonprofits is that the marketplace is growing and pricing is favorable. You'll recognize many of the biggest names in cybersecurity from other insurance markets, including Liberty Mutual, Travelers, AIG, Chubb, and CNA, each of which has an A rating or better from the A.M. Best Company and the Better Business Bureau.

As you evaluate providers, make sure to ask about the types of incidents the policy will cover and which events are excluded. You don't want to be surprised when your specific incident isn't covered. Also make sure to vet multiple brokers and policy options side-by-side so that you can be sure you're getting the policy that's right for your organization from a provider you trust.

Cybersecurity Insurance Checklist

When you apply to purchase cybersecurity insurance, the provider is going to want to know that you are taking certain baseline actions and following best practices to minimize risk. While every provider can ask for different things, some items are common across the board. We created this checklist to help you understand what those baselines are and what they mean.

Note that policy providers may have more stringent requirements for organizations that must comply with regulatory guidelines such as the Health Insurance Portability and Accountability Act (HIPAA).

Multi-Factor Authentication (MFA) for All Remote and Privileged Users

Passwords are so valuable to hackers because they're often the only barrier to essential systems. If you add additional barriers, you can significantly increase the difficulty of an attack succeeding. Multi-Factor Authentication, or MFA, adds at least one more step to the login process, forcing hackers to have additional "keys" to unlock the door to your network or systems.

One form of authentication is a text message or push notifications sent to your mobile phone when you log in that you must then enter along with your password to access the system. However, phones are becoming increasingly less secure, so a more secure option is an authenticator app or system-specific app that can generate a code synced to the system you're trying to log into.

For example, your CRM might require you to use the Microsoft Authenticator app as a second authentication step. The user can sync the two systems by scanning an onscreen QR code with their smartphone. When you log in to the CRM once the systems are synced, you get a prompt for a six-digit code. You can then open your authenticator app and type in the time-sensitive code to log into the system.

The most secure Multi-Factor Authentication option is a U2F security key, a device you plug into your USB port so that your browser can read the key before logging you into the system. The technology has many safeguards built into it to ensure that the key information can't be intercepted or cloned.

Cybersecurity Insurance providers want to know that you are following this basic best practice for all employees working and accessing systems and sharedrives remotely, as well as for all privileged users. Essentially, this means that providers may want to see an access policy that states the least amount of privileges be granted for access to files or systems, or a similar need-to-know policy. These policies should include process that monitors and reviews these privileges on a regular basis.

Email Filtering

Email filtering refers to a process of scanning an organization's inbound and outbound email traffic and classifying messages into different categories, such as spam, malware, bulk, virus, suspicious, impostor, phishing, etc... On the outbound side, the process is similar, scanning messages before delivering any potentially harmful messages outside the organization.

This service can be deployed internally, as an on-premises solution, or as a cloud service. Note that organizations required to comply with some regulatory guidelines must use on-premises solutions.

Email filtering techniques can determine the effectiveness of your mail routing, so your organization should consider solutions carefully. Some of the more common techniques include the following:

- **Reputation-Based Filters**, which block known spammers or approve trusted senders based on reputation databases or Reputation Block Lists that maintain records of domains, URLs, and IP addresses that have been deemed possible security threats.
- **Safelisting** is a way for organizations to determine which senders they'll allow email from by adding them to a list.
- **Blocklisting**, conversely, lets organizations determine which senders they want to block email from by adding them to a list.
- **Graylisting** is a means of defending against spam by temporarily rejecting email from a sender that the system does not recognize—if the mail is legitimate, the sending server will try again after a delay and the email will be accepted.
- **Antivirus Software** protects against new and existing viruses and other forms of malicious code included in emails.
- **Content Analysis** lets you block email based on the message content—for example, if a message contains certain words, the content filter can determine that it is a spam message, or if it contains an attachment.

Whatever form of email filtering you use, an insurance provider is going to want to know that you're not just letting email in and out without some sort of supervision.

Domain Name System (DNS) Filtering

A DNS is how IP addresses are translated into domain names—and filtering DNS is one of the most common methods of safeguarding against cyber threats. In simplest terms, DNS filtering is the practice of filtering specific sites for a particular purpose, often by content.

For example, your organization might block any domain that has been classified as a known threat. Often, these decisions are made based on content associated with malware, porn, illegal download sites, etc.., but some organizations might also block sites that stifle employee productivity, such as Netflix or Facebook. DNS filters maintain and update blacklisted site lists to block.

Endpoint Detection and Response

Perimeter defenses might miss more sophisticated that can cause serious damage to your network. But Endpoint Detection and Response solutions, or EDR, monitor your entire environment for threats and tracking their points of entry and behavior and providing insights about actions to take against them. By containing threats at the endpoint, they can help eliminate them before they spread throughout your organization. For example, an EDR could help you identify, contain, and remove a ransomware threat before it encrypts sensitive data and holds it hostage for financial ransom. These solutions are deployed and managed by your IT staff, security vendors, or security partners, and are a critical part of protecting your network against all types of dangers.

Backups and Testing

Backups are critical for the protection of your data, as well as the credibility of your organization. Most cloud-based document management systems such as Google Drive, Microsoft Office 365, Dropbox, and Box now offer a data backup add-on service. If you maintain your own network servers or want to make sure you have an alternative to your cloud service, there are many options to choose from.

However, backups that are not regularly tested are essentially useless. Without consistent testing, you run the risk of losing the data, applications, systems, and workloads that your backups contain, potentially with no way to recover them. Because of this, a comprehensive testing plan is a necessity to ensure your backups will perform as expected in a disaster scenario. Download our free article, *Disaster Recovery: Planning Ahead for the Unthinkable,* to learn more.

Policy providers want to know that you've taken the necessary precautions to safeguard and update data and that you're ready to restore it in the event of a loss.

Anti-Phishing

More than 90 percent of cybersecurity breaches are caused by human error: not IT staff failing to implement proper safeguards, but end users making unwitting mistakes. Thoughtless clicks, too much trust, or a simple lack of awareness can lead to incredibly costly security breaches. Phishing is when a hacker or scammer sends messages pretending to be someone you know or can trust—and all it takes is a single, innocent click to fall prey.

Phishing attacks typically take two forms. The first is meant to gather login information so that it can access your accounts or data. Typically, the hacker will pose as a company like Microsoft or Google and ask you to log in to your account but the link will be to a dummy website designed to capture your login information. The second most common form of phishing is to provide a link or attachment that, once you click it, downloads malicious software or injects malicious code into existing software. This is how ransomware typically infiltrates a computer or network.

Anti-phishing security measures can help prevent attacks or mitigate their impact. Some may block email containing phishing attacks from entering your email system at all, while others block users from clicking on links and attachments within an email they have received that might be dangerous.

Anti-phishing awareness training can protect users by educating them about how to recognize phishing attacks.

Security Awareness Program

Security tools and policies are important, but if the people at your nonprofit don't understand the threats that are out there and take them seriously, your organization is vulnerable to a major security incident.

No organization can ever be 100 percent secure, but nonprofits that create a strong security culture, one that actively promotes security awareness and a shared sense of mission around security, is much more likely to avoid many of the most common threats. As a leader at your nonprofit, you can create the conditions for a work culture that values security and vigilantly protects the organization's systems and data. These measures might include the following:

- Involving Staff in Writing Policies
- Providing Cybersecurity Training
- Providing IT Staff Ongoing Training
- Integrating Security into Daily Life
- Testing Your Staff
- Testing Your IT Response

Policy providers know that the human element is often the weakest point of any organization's security posture. By demonstrating that your nonprofit values security and works to integrate into your culture, you can show them that you are doing all you can to make yourself a harder target for threat actors. To learn more about how to increase security awareness among your staff, download our free article, *Creating a Culture that Values Security*.

Get Help

Considering the risk involved, taking your cybersecurity practices seriously is critical for all nonprofits—whether you're applying for an insurance policy or not. If you need help assessing or shoring up your cybersecurity posture, Tech Impact is positioned to help you create a secure computing environment.

We understand the complexity of compliance regulations such as PCI and HIPAA. Our cybersecurity services will help you balance user productivity with the security that gives you, your board, and your funders peace of mind.

Learn more about our services at https://techimpact.org/services/security-services-nonprofits/.

About the Contributors

This article was a collaboration between Chris Bernard, Managing Editor, and George Staton, Director of Centralized Systems and Cybersecurity

About Tech Impact

Tech Impact's mission is to leverage technology to advance social impact. We deliver workforce development programs that foster individual growth, economic mobility and a more diverse IT talent pool; and capacity building services that lead to stronger nonprofits delivering greater social impact. We believe when nonprofit leaders gain the skills, knowledge, and confidence to make smart technology decisions, their organizations become more effective—and communities thrive. Learn more at techimpact.org, or browse the hundreds of free publications and educational resources in our Technology Learning Center at techimpact.org/technology-learning-center.