THE NONPROFIT TIP JAR

Cyber Security and Insurance - Top 5 Questions and Answers

1. What are the biggest cyber threats in 2021?

Cyberattacks continue to mount despite increases in cybersecurity spending and training. The overall frequency and severity of cyber losses also continue to grow. Ransomware, Funds Transfer Fraud and Email Compromise are the three leading types of cyber incidents reported to insurers in 2020. As attacks grow in complexity, no organization should consider itself 100% secure from vulnerability.

2. What's all the fuss about ransomware and do we need to worry?

First, yes, you should worry. Criminal actors are exploiting vulnerabilities to deploy "ransomware", which takes an organization's data and systems hostage until a ransom is paid, usually in cryptocurrency, at which point the data may be unencrypted. The sophistication of attacks is increasing, as are the average ransom demands. One key lesson we have learned is that many incidents can be avoided (or at least mitigated) through thoughtful data security and backup practices.

3. What is the best way my nonprofit can prepare to avoid a cybersecurity incident?

There are many basic steps you should consider. Identify the data you collect, as well as how you store and use it. Identify potential weaknesses in how data can be accessed and procure the tools and knowledge to correct these weaknesses. Speak with professionals who can provide guidance about the types of cybersecurity software they recommend, including Multi-Factor Authentication (MFA). You should already have well-developed policies as to how your organization will respond in the event of a breach. Conduct table-top exercises and stress tests on a regular basis. Take what you learn from these scenarios to practice, train, and refine your incident response plan. Make sure you are training employees to recognize signs of phishing and other attacks.

4. What is the state of the cyber insurance market?

As a nonprofit, you should expect considerably more underwriting scrutiny of your cybersecurity practices on behalf of your insurance company. Most insurers will insist upon Multi-Factor Authentication (MFA), regular security updates and patches, among other requirements. Also, you should expect volatility in cyber insurance premiums and potential reductions in limit capacity, depending on the risk profile and data assets of your organization. It's best to start your renewal early and be proactive.

5. What additional services does cyber insurance offer?

Standalone cyber coverage will be the most robust and provide the broadest coverage. Most cyber coverage today will provide cyber services depending on your insurance company. With many policies, the insured will receive gratis or low cost additional resources, including cybersecurity training, system breach testing, and breach coaching. In addition, many insurers offer some basic training and resources, often through a login to E-Risk Hub or similar library of cyber resources.

AHT
INSURANCE
A BALDWIN RISK PARTNER

ahtins.com | 800.648.4807