CYBERSECURITY SOLUTIONS FOR NONPROFIT ORGANIZATIONS

CYBER ATTACKS: INCREASINGLY LIKELY, POTENTIALLY CATASTROPHIC

Nonprofit organizations are highly vulnerable to the increasing number of attacks from sophisticated cyber criminals. Protecting donor and member information is critical and large amounts of Personally Identifiable Information (PII) are of increasing value on the black market, surpassing even credit card data in value.

Information sharing is fundamental to virtually every aspect of business. As you focus on engaging others in your mission, information sharing with vendors, contractors, partners, members, donors and the public in general has grown and is essential to your success. And every one of these digital relationships presents a new set of cyber vulnerabilities.

The need for security and the way in which it is implemented must be balanced, thoughtfully, against the needs of an organization to operate effectively, and to actively pursue its mission.

While it is impossible to eliminate all risk of cyber attack, a well-designed program will minimize the negative impact on both short-and long-term business goals.

CYBER RISKS: UNIQUE TO EVERY ORGANIZATION BUT CRITICAL TO NONPROFITS

Answering the question, "Is an organization secure?" requires a comprehensive assessment of its operating environment and its specific business needs.

Ultimately, implementing a cost-effective cybersecurity framework includes careful consideration of how you identify, protect, and recover critical assets, as well as detect and respond to security breaches. Conducting risk assessments, planning incident response, and establishing governance structures – all begin by asking the right questions:

- How do we protect our donors' and/or members' information?
- How do we ensure that our agents and vendors do not compromise our systems?
- Who requires access to which data?
- Where are the particular points of vulnerability?
- Do you have an established definition of a security breach?
- What notification obligations do you have in the event of a breach?
- What are your current policies and procedures, and how are they governed and maintained?

Implementing a cost-effective cybersecurity framework includes careful consideration of how you identify, protect, and recover critical assets, as well as detect and respond to security breaches.

AN EXCEPTIONAL RANGE OF CYBERSECURITY SERVICES

Cyber Insurance Claim Preparation & Coverage Adequacy Evaluation

Identify and quantify incurred event response costs for inclusion and submission in an insured entity's insurance claim. Pre-loss services include measuring estimated response costs related to data breach scenarios to assist in evaluating cyber insurance coverage.

Cyber Risk Management Strategy & Program Design

Design and implement a comprehensive program aligned with an existing enterprise risk management framework. Includes strategy, organizational structure, governance, policies and procedures, training, and both internal and external communications.

Cyber Risk Assessment & Security Testing

Assess risks and identify vulnerabilities to digital assets to evaluate their potential impact and damage, prioritizing risks against the costs of protection. Includes assessments, security testing, remediation and deep experience in credit card risk mitigation.

Security Architecture & Transformation

Design and implement a cybersecurity architecture and framework tailored to business needs and the enterprise ecosystem. Encompasses access controls, entitlement, data protection, data privacy and monitoring.

Incident Response Planning

Develop and test comprehensive incident response plans to minimize the impact of a breach. Considers company processes, as well as roles and responsibilities of individuals throughout the organization.

Business Continuity Planning & Disaster Recovery

Develop and test company-wide business continuity and disaster recovery plans for critical systems, applications, infrastructure, facilities, people and business processes.

Digital Forensics & Cyber Investigations

Rapid response to breach incidents, including identification of cause and implementation of remediation measures for affected areas, as well as expert testimony when needed.

CONTACT

SHAHRYAR SHAGHAGHI
National Practice Leader
Technology Advisory Services

212.885.8453
sshaghaghi@bdo.com

Shahryar has developed and implemented IT strategy, risk and compliance optimization programs for a wide range of domestic and global organizations – with a particular emphasis on cybersecurity and business continuity. He leads the BDO Technology Advisory Services Practice.

BDO Consulting, a division of BDO USA, LLP, provides clients with Financial Advisory, Business Advisory, and Technology Services in the United States and around the world, leveraging BDO's global network of over 60,000 professionals.

BDO USA LLP provides audit, tax, and advisory services to the insurance industry. BDO is the fifth largest auditor of insurance companies in the USA.

Our culture is collaborative, with a flat organizational structure designed to minimize bureaucracy and maximize person-to-person interaction. Partners are approachable. Specialists are accessible. Everyone at BDO understands that at its core, our job is about helping – in thousands of different ways, for thousands of different clients – and that we measure the success of our client relationships not in dollars earned, but in years served.