# NonProfit Trends

## Weak Cybersecurity Can Lead to Big Risks

2014 - Issue IV

Follow us on

Cybersecurity has long been a top concern for the private sector and government agencies, but not-for-profit organizations are now realizing the importance of cybersecurity to their operations. Cyber attacks are hugely costly in terms of both monetary loss and damage to an organization's reputation – it's most valuable asset.

Compromised security has long-term effects on not-for-profits due to bad press; breach of confidentiality; credit card company fines for failure to comply with security requirements; donors suffering identity theft; and the loss of donor confidence going forward.

While in the past, not-for-profit organizations often felt that cyber attacks did not happen to them, the increasing number of data breaches over the past few years has made cybersecurity and data privacy a Board-level governance concern. It is important that Board members, executives and directors recognize cyber risks as part of their duty to review risk practices, continuity planning, and disclosure of material risks. Not-for-profits handle significant amounts of sensitive information, including donor data, credit card numbers, allocation of aid, program information, employee and payroll records, and health insurance information. All of this data must be protected.

Failing to take adequate cybersecurity measures and a subsequent data breach can lead to loss of public trust in an organization, which endangers that organization's ability to effectively provide services to the people in need who depend on them.

Unfortunately, not-for-profits often have limited resources to invest in information security, leading to IT systems and security appliances that may be outdated. This makes organizations vulnerable to data loss and other cybersecurity breaches.

Organizations must approach cybersecurity holistically, as they would handle the financial health of the organization. It is the collective responsibility of everyone in the organization to protect it from cyber attacks.

Organizations should take all necessary precautions to avoid being the next news headline.

Now is the time to discuss the best way to address these cybersecurity issues and put your organization in a position of strategic advantage.

**Preventative Steps**

- Proactively address known and potential future threats
- Continuously monitor for and address human error
- Identify and prioritize customer data for day-to-day business demands
- Assess the relationship between physical security and cybersecurity
- Maintain internal communications about exposure to identity theft and take action to address vulnerabilities in data systems
- Acquire and implement good defensive technology to protect business networks - external consultants are highly recommended
- Be ready to face a breach with an incidence response plan.

**3rd Party Vulnerability Assessments - Cost-Effective and Essential**

- Minimize vulnerability to cyber attacks
- Reduce impact of and shorten recovery time from an incident
- Improve system performance
- Reduce resource load from automated solutions
- Interface with a single source supplier for turnkey security solutions
- Avoid large fines, shutdowns, and additional staffing

WeiserMazars has substantial experience with implementing privacy security initiatives, particularly with performing vulnerability assessments. We help you and your organization to implement the appropriate security measures to protect against cybersecurity threats and potential damage to your reputation.

For more information contact:

Nicolas Quairel
Principal
646.225.5983
Nicolas.Quairel@WeiserMazars.com

Mitch Lewis, CPA
Partner-in-Charge, Not-for-Profit
212.375.6723
Mitch.Lewis@WeiserMazars.com