Neighborhood Risk Management
CORPORATION
NWOs working to insure safer communities

October 2014

CyberRisk: Credit Cards and Secured Online Donations

Soliciting donations is vital for not-for-profits. And, accepting donations by credit card is easy. But is it safe?

ISSUE: **What practices are in place at organizations that do not use secure payment processing to ensure that donor credit card information is protected? What are organizations doing to protect the integrity of the credit card information that is provided by donors and other third parties?**

Who is monitoring your IT Activities?

Here are some Best Practices for your organization to consider to reduce or eliminate Credit-Card security and related CyberRisk exposure:

1. Avoid accepting credit card information directly from donors, residents or vendors. Always use a secure payment processing system.
2. Never store credit card information from donors, residents or vendors. Each subsequent transaction should require the resubmission of this information.
3. Always use a secure payment processing system, such as PayPal or Square Reader, to eliminate the need for your organization to handle credit card information. While these services may have a fee associated with their services, those fees are relatively nominal in relation to the potential risks and liabilities to your organization for a credit card data breach.
4. Screen all personnel that are given access to CPI with background checks, and conduct screening as frequently as necessary or required by your organization's guidelines. Volunteers and interns should be screened as well.
5. Secure all donor lists and CPI that you receive by using passwords and other protections. Consider encryption whenever possible.

For Further Information and Tips contact Deborah Aschheim of Neighborhood Risk Management Corporation, 212.509.6762 daschheim@neighborhoodrisk.org