Neighborhood Risk Management
CORPORATION
NWOs working to insure safer communities

TO: All NRMC Members and their Property Managers

FROM: Deborah S. Aschheim, Executive Director

DATE: October 2014

CyberRisk: Credit Cards and Secured Online Donations
CyberSecurity Best Practices

CyberSpace is a fact of life: business and personal. Today, almost every organization conducts business in CyberSpace. Our members are part of this trend. They are major repositories of confidential personal information ("CPI") for their residents, investors, vendors and staff, all of which is stored and maintained on office computers and in the cloud.

A day does not pass without a report of a business facing a computer hack or data breach, with Target, Home Depot and Chase Bank gaining the current headlines. What may not always make the headlines, however, is that nonprofit organizations face the same threats. While not-for-profits and for-profits have the kinds of valuable data that hackers target – resident data (such as bank account info, social security numbers, credit card numbers and private health information), employee data and even organization data (such as donor information) – not-for-profits have tighter operational budgets and even fewer resources to deal with IT infrastructure, online security, and secure data issues. They simply do not have the same resources, technology or personnel to defend and respond to cyber threats that for-profit organizations have.

Data breach threats come from many sources. An employee falls prey to email phishing. A laptop is stolen from an employee's car. A disgruntled employee leaves with credit card numbers and CPI. A zealous volunteer becomes overly inquisitive and intrusive. NWOs are not immune from attack. Recently a member of the NRMC program reported an identity theft: A staffer stole CPI of a resident to obtain illegal credit cards under that resident's name. This identity theft and the related losses were not covered by the member's general liability (GL) insurance, nor is such peril covered under the NRMC Program.

CyberAttacks have increased dramatically over the last decade, exposing sensitive and confidential personal and business information, disrupting critical operations, and imposing high costs on the economy. CyberAttacks are not limited by geographical boundaries or to certain industries. For 2013, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center

(IC3) received 262,813 consumer complaints with an adjusted dollar loss of $781,841,611.[1] From 2011 to 2012 there was a 44% increase in CyberAttacks and a 42% increase in average cost of attack. Expanding use of social media, mobile computing, and other emerging technologies add to this threat. Some of the most common cybercrimes include phishing, blackmailing, electronic harassment, copyright infringement and illegal access of stored information.

The consequences of a data breach can be severe, ranging from bad press and loss of trust, to financial penalties and liability for the financial harm to those people or entities whose data is stolen. There liabilities can include breach notifications (which can cost thousands of dollars) and assuming the cost for on-going credit monitoring for all potential injured parties for up to one year. Breaches can also entail governmental investigations and litigation against the organization that was hacked, as well as confiscation of computer equipment and systems. Reputational damage can be particularly deep and long-lasting, something that a not-for-profit cannot endure. Imagine how your organization would operate if 10 or 20 computers were confiscated to investigate whether a breach occurred or as evidence in a CyberCrime investigation or lawsuit.

CyberRisk liabilities are not covered under common General Liability insurance policies, including the NRMC program. CyberRisk insurance must be purchased separately. It is costly and in order to qualify for the insurance, the organization must adopt strict CyberSecurity best practices to protect data and CPI. The insurance carriers want to know that your organization is protecting itself.

This White Paper will provide your members with (1) a review the risks of on-line donation practices, and (2) basic CyberSecurity Best Practices for your Organization.

⊗ ⊗ ⊗ ⊗ ⊗ ⊗ ⊗

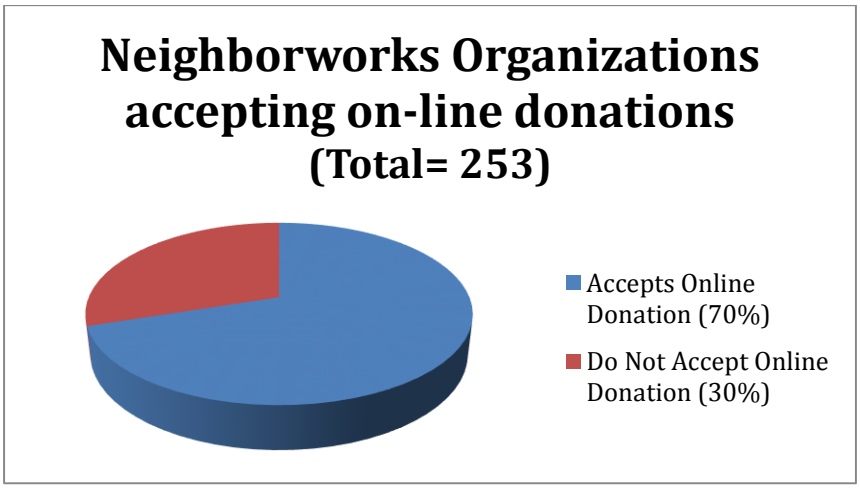
On-Line Donations

⊗ ⊗ ⊗ ⊗ ⊗ ⊗ ⊗

Soliciting donations is vital for not-for-profits. This summer NRMC visited the Websites of all our members and all NeighborWorks Organizations (NWOs) and reviewed their on-line donation solicitation practices. We considered whether the organization (1) solicits and accepts donations on-line; (2) takes donations by directly seeking credit card information from donors; and (3) takes on-line donations using PayPal or other secure payment processing system. Here is what we found (It is possible that members engage in additional payment safety practices which are not apparent from their websites.):

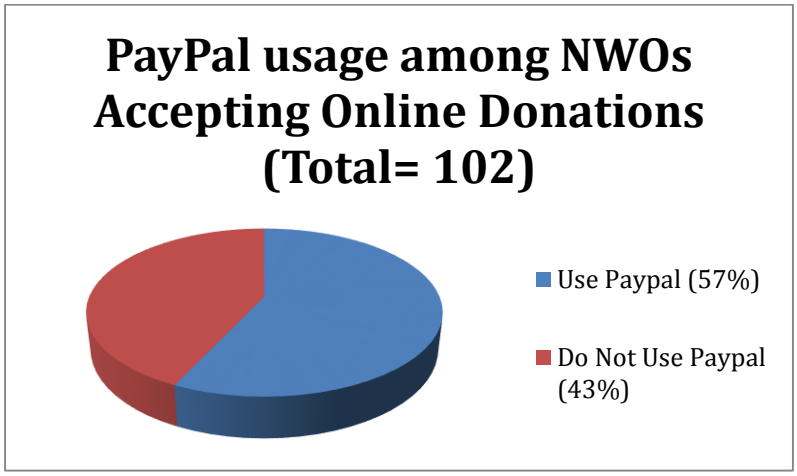
[1] http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

- Of the current 253 NeighborWorks Organizations (NWOs) in the NeighborWorks America network, 177 (70%) accept online donations on their website.



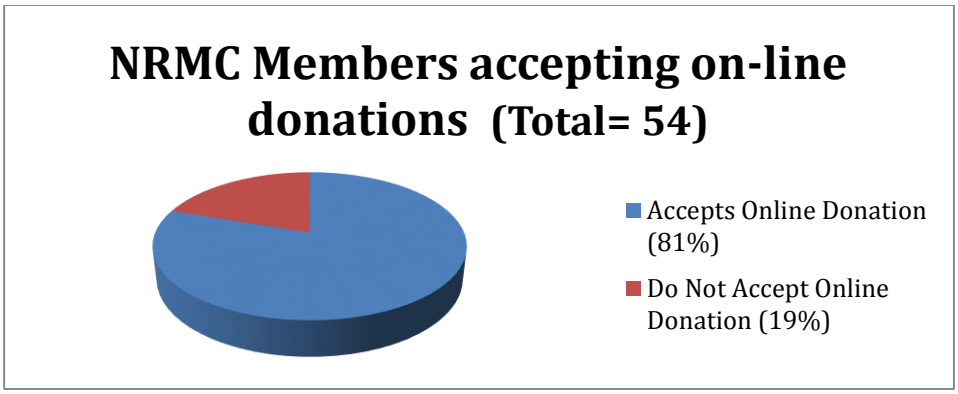
- Of these 177 NWOs that solicit on-line donations, 102 of them (or less than 41% of all NWOs) use PayPal as their donation payment processing system according to their websites.

- Therefore, it appears that at least 42% (75 of the 177) NWOs that accept on-line donations may be receiving credit card information directly from donors



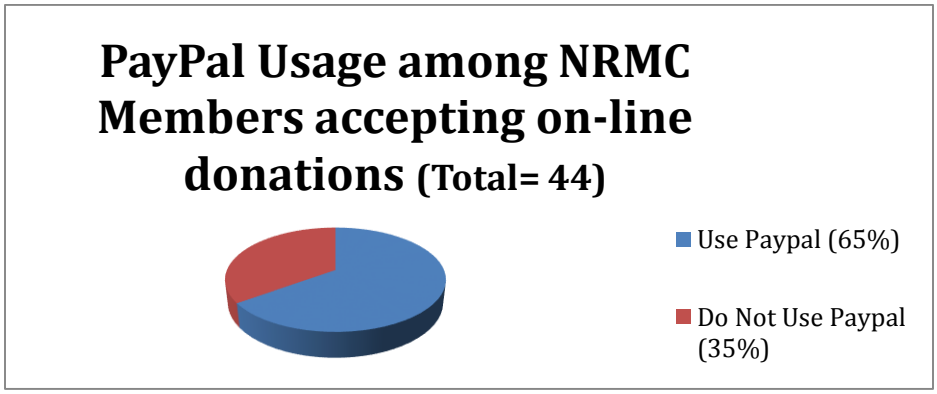
We then trended the Websites of NRMC members alone and observed the following:

- Of the current 54 NRMC Program members, 44 or 81% accept online donations on their websites.



- Of these 44 NRMC members that accept on-line donation, 29 of them (or slightly more than 65% of all NRMC Members) use PayPal as their donation payment processing system according to their websites, and an additional 7 (for a total of 36 NRMC members) use a modified on-line payment system that involves some security.

- Therefore, it appears that at least 25% (11 of the 44) of NRMC members that accept on-line donations appear to be receiving credit card information directly from donors.



While it is very possible that not all of these organizations are taking credit card information, the question of data safety cannot be ignored. And what about organizations that may be accepting payments by credit cards from residents or other third parties?

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?

When processing credit card transactions, all organizations must follow the Payment Card Industry (PCI) Security Standards [2]. These credit card industry standards ensure that all organizations that process, store or transmit credit card information maintain a secure environment to protect customer credit information.

As a busy, small organization – where your staff may have multiple responsibilities with limited IT expertise, or where you are relying upon volunteers – you may not even realize that you and your staff don't know how to properly handle a credit card transaction, or even worse, that a staffer has stolen a donor's credit card information. Without proper safeguards in place, your organization may be vulnerable to fraudulent transactions and the possibility of legal action, including possible liability for fraud and fines.[3]

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.

---

[2] https://www.pcisecuritystandards.org/security_standards/

The PCI Security Standard Council's mission is to enhance payment account data security by establishing payment standards by driving education and awareness of the PCI Security Standards. The organization was founded by American Express, Discovery Financial Services, JCB International, MasterCard, and Visa Inc.

[3] http://www.businessnewsdaily.com/6171-credit-card-security-risks.html

⊗ ⊗ ⊗ ⊗ ⊗ ⊗ ⊗

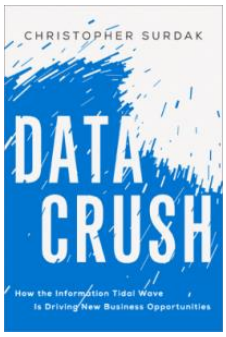
CyberSecurity

⊗ ⊗ ⊗ ⊗ ⊗ ⊗ ⊗

CyberSecurity is a vast and pervasive global issue in today's economy. Addressing CyberRisk entails a thorough evaluation of the many unique operating areas of your organization, which is beyond the scope of a White Paper. However, we draw our members to the following **NRMC Materials and Presentation**: Here is the link to NRMC's recent CyberSecurity Webinar (Sept. 30, 2014). Copies of CyberSecurity materials and the Webinar Presentation are available on the NRMC Website (Publications)

https://attendee.gotowebinar.com/recording/8397450049955730434

CYBERSECURITY BEST PRACTICES



From: Christopher Surdak, JD, CyberSecurity Consultant
chris@surdak.com / 714.398.4874
Author of Data Crush, published by AMACOM Publishing
Nominee for International Book of the Year, 2014

Best Practice # 1 - Identify your risks: Know *your* organization's risk profile! Critically evaluate yourself. Consider these factors that create or influence risk:

- Your physical facility set up and your office traffic. Where and how is CPI stored at your properties? At a central headquarters or at the properties?
- Your system: Computer Equipment; shredders; locked cabinets; on-line storage
- Your data management practices
- Your disclosures: What do you receive? What do you disclose to applicants, tenants, regulators, investors and employees about CPI?
- Your data collection processes and document retention policies
- Your human resources practices: Policies & Procedures for staff, temps and volunteers, use of Personal devices for business; what happens when staff departs the organization

Best Practice #2 - Passwords/Monitors

- Mandatory PW changes every 60 to 90 days
- Prohibit the posting and sharing of PWs. Check work stations for compliance
- Set computers to lock after 10 idle minutes

Best Practice #3 - Create a Data Security Plan. Include key contact people and protocols; Conduct periodic drills and tests. Tailor your plan for all aspects of your operation.

Best Practice #4 - Create a Culture of Security and enforce it

Best Practice #5 - Plan ahead. Plan for the inevitable and the unthinkable

Best Practice # 6 – Integrate Privacy in your Data Security Plan. Check with a privacy expert as you build your plan

Best Practice # 7 – Cautiously select IT Service Providers and Carefully Negotiate IT Service Contracts

- Engage an experienced Technology and CyberRisk consultant or attorney to investigate the vendor and review and negotiate the contract
- Include data breach provisions and protocols, indemnification; data ownership and transfer of data on termination; cooperation
- Know where your data will be stored and consider the impact of the location
- Require the vendor to provide evidence of GL and CyberRisk insurance. Coverage should be for $1MM/occurrence; $3MM in the aggregate. Consider additional insured status
- Develop Controls and conduct periodic Audits of IT Service Providers

Best Practice # 9 – Understand Clouds

Best Practice #10 – Never Accept Credit Cards --- use a secure payment system to process payments and donations

NEVER BE AFRAID TO ASK FOR HELP.
IF YOU CAN THINK IT …… IT NEEDS TO BE ADDRESSED