



Neighborhood Risk Management  
C O R P O R A T I O N  
*NWOs working to insure safer communities*

October 2014

## 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.

**ISSUE: What practices are in place at you organization to ensure that your CPI and business data is protected? Who is monitoring your IT Activities?**

# CYBERSECURITY BEST PRACTICES



**Christopher Surdak, JD, CyberSecurity  
Consultant**  
**[chris@surdak.com](mailto: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**

For Further Information and Tips contact Deborah Aschheim of Neighborhood Risk Management Corporation, 212.509.6762 [daschheim@neighborhoodrisk.org](mailto:daschheim@neighborhoodrisk.org)