Neighborhood Risk Management
CORPORATION
NWOs working to insure safer communities

CyberSecurity and Legal Risk Management:

An Overview presentation on behalf of Neighborhood Risk Management Corp. for NeighborWorks America

Margaret Paradis, Esq. and Christopher Surdak,
April, 2013

Agenda

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Recent Headlines**
- **Security Risks for Small & Medium Businesses**
- **Legal Framework: Your Responsibilities and Risks**
- **Steps to Take Now**

Victim #1: Sony Corporation

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Sony of America's director of communications said that "an illegal intrusion" in their system has caused a “compromise of personal information.”

And while Sony officials don't believe credit card information was taken, they say that hackers may have taken names, addresses, email addresses, birthdates and passwords among other things.

A study from security think tank Ponemon Institute estimates that it costs $318 per compromised record for a data breach. With **77 million PlayStation Network user accounts** that adds up to the $24 billion estimate.

Victim #2: TJ Maxx

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- US Securities Exchange Commission filings by the firm show that **45.7 million credit and debit card numbers** were stolen over a period of 18 months.
- A West Virginia woman filed a class action lawsuit against the company. She accuses the retailer of negligence for not doing enough to secure customer data, and for keeping quiet about the breach for a month.

- "Because of TJX's actions, hundreds of thousands or even millions of its customers have had their personal financial information compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identity theft, and have otherwise suffered damages," according to the lawsuit.
- The lawsuit seeks credit monitoring services and **any damages incurred by millions of affected customers.**

Victim #3: The U.S. Federal Reserve

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

February 7, 2013: The Federal Reserve has acknowledged that an outside party gained access to its website and a limited amount of data, raising questions about the central bank's cyber-security measures.

PHOTO: KAREN BLEIER/AFP/GETTY IMAGES

The notice, sent via the Fed's Emergency Communication System, warned that email addresses, phone numbers and other contact information had been stolen and published.

Similarly, the IRS stands to lose as much as **US$21 billion in revenue over the next five years** due to identity theft, according to a TIGTA's audit.

Why Worry About Security?

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

What Can Happen if Information Security is Compromised?

- Loss of confidentiality, integrity & availability of data (and time)
- Risk to integrity of confidential information, e.g., data corruption, destruction, manipulation, etc…
- Embarrassment, bad publicity, media coverage, news reports
- Loss of community confidence
- Internal disciplinary action, and possibly termination of employment
- Penalties, prosecution and sanctions, lawsuits, and regulatory infractions
- ***Personal liability for business leadership potential under applicable law***

Why Worry About Security?

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

According to software company Symantec, nearly 75% of small and midsize businesses fell victim to a cyber-attack within the past 12 months, resulting in lost productivity, lost revenue, and direct financial costs.

In 2011 11.6 million U.S. adults were victims of identity theft in 2011. That represents 4.9% of all adults. The total cost of identity theft in 2011 was $18 billion. The average victim spent $354 and 12 hours to resolve the problem and clear up their records.

The Adversary

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Today's intruders rarely fit the image of a lone wolf probing corporate systems for bragging rights.

- Adversaries are smarter, better organized, more persistent. Many are part of criminal organizations; some are agents for nation-states.
- Attackers have a huge advantage. In cyber, offense is far cheaper and easier than defense, which must be 100% effective. The adversary needs only to find one weakness.
- Varieties of adversaries and motivations lead to different attack types.

Methods of Attack

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Adversaries only need to find one vulnerability— their methods of attack are multiple and rapidly changing

- Advanced Persistent Threats are targeted, “low and slow” attacks that stealthily move through a network without generating regular or predictable network traffic.
- The U.S. military’s worst attack was launched from a USB thumb drive bearing a malicious program from a foreign intelligence agency.
- Virus hidden on legitimate websites infected British bank customers’ computers; stole money from their online accounts.
- Google attack began with instant message sent to Google employee, who clicked a link to a poisoned website.
- Some attackers infect commercial software and hardware with “logic bombs” before it is sold.

Threats From Within

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Many of today's cyber security threats result from the behavior of organizations' employees.

- Using popular social networking websites, possibly exposing employers' computers and networks to worms, malware, etc.
- Checking corporate email from unsecured personal devices, including smart phones and home computers.
- Self-provisioning potentially unsecure cloud-based applications.
- Accessing organization data from unsecure WIFI hotspots.

The Scope of the Issue

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

According to the study by Ponemon Institute and sponsored by Check Point:

- 77% of the 2,426 IT professionals questioned in five countries admitted their organizations suffered a data loss in the past year.
- Of those, 52% say they lost customer data and 44% say they lost consumer information.
- Other intellectual property and employee information were cited as stolen by 33% and 31%, respectively.

- ***Twenty-two percent (22%) of small businesses*** have experienced the loss or theft of customer or employee information, according to another study by the Ponemon Institute.

The Scope of the Issue and NWOs

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Considerations for NWOs and other providers of Affordable Housing:

- HUD4350 and applicable state and local laws.
- Qualification for Affordable Housing is dependent upon “verification” of confidential information presented by applicants / residents. NWOs receive a host of “Confidential Protected Information”, including tax returns, employment verification, bank and brokerage account information, credit reports, and lots more information.
- Confirmation of “Disability” entails the presentation of medical information and HIPAA compliance.

Consequences can impact funding: Potential and actual

Why Should You Care?

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- Assume that you digitally record your customer records and at some point thereafter someone gains access to those records.

- Compromised are the names, birthdates, and social security numbers of all of your residents.

- By law, you must notify each of the customers of this data breach, via registered mail, at an average cost of $10 per registered mail piece. The cost for this action alone is not covered by your general liability insurance coverage.

- If just a handful of these records result in stolen identities, resulting lawsuits could push the tab up per claimant to substantial levels.

- Investigation by a regulatory body will most certainly result in stiff fines and penalties. And none of this is covered by general liability insurance.

- DO NOT EXPECT ANY SPECIAL EXEMPTION BECAUSE OF STATUS AS PROVDER OF AFFORDABE HOUSING.

Legal Liabilities of the Hacked Business

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- In addition to the direct damage done to your organization by the cyber criminals, your organization faces two additional types of loss due to legal liabilities linked to these risks:
    - Liabilities that face all businesses from these crimes under contract and market standards and
    - Additional liabilities to regulators and consumers because your activities subject you to certain special federal and state privacy and related data security regulations imposing standards on your organization for the protection of private information you collect, generate and hold concerning individuals
- Some background on these sources of liability is helpful in understanding effective control measures.

General Commercial Liabilities

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- When confidential information is provided to you in the course of your business operation, the person or company. Some level of protection against unauthorized disclosure or usage of the information.

- Other organizations can set high standards and specific security obligations by contract.

- Courts will interpret standards and fill in gaps by reference to market security standards—what is negligent, grossly negligent?

- Three key elements of successful case: breach of relevant duty, breach is cause of loss, and actual loss to show damages.

Regulatory Liabilities

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- Personal information concerning individuals receive protection today under a network of federal and state laws.
- Your activities trigger regulation under at least some of these laws because of the type of information you gather and your responsibilities to HUD
- HUD is subject to the Privacy Act of 1974 in the handling, use and disclosure of the personal information you gather and transmit to HUD.
- As detailed in the HUD Manual, a disclosure statement and consents are required in obtaining the information from the individual applicants you handle.

Regulatory Liabilities

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- Generally, businesses considered to be providing a financial service are subject to the Gramm Leach Bliley Act (GLBA), the federal financial privacy law. GLBA protects the personal financial information of individuals obtaining goods and services for their personal or family use. There are two key requirements—privacy (involving prior notice and for certain usage consent) and security to provide confidentiality.

- GLBA does not provide detail on compliance with the security standard.

- GLBA does not bar any state from adopting tougher privacy protections. Some states have done that. Most notably Massachusetts.

State Laws on Data Security: Massachusetts

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

•The Massachusetts law has created a new model for state laws because of its detail on security requirements.

•Generally the law applies to companies with data on even one Massachusetts resident.

•It covers not only to the principal organization involved, but also their service providers handling the data.

•Purpose of Massachusetts Law and Regulations:

> *"to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer. "*

State Laws on Data Security: Massachusetts

- The key requirements are:
  - **Written security plan** detailing administrative, technical, and physical safeguards customized for the company, covering several specified areas
  - Most controversial is the requirement that the plan include a computer security system with at a minimum certain elements, including among others, **encryption** of:
    - all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly and
    - all personal information stored on laptops or other portable devices.

The Legal Risk Response

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- Regardless of the size of an organization or the limited resources available to it, there are minimal legal steps every organization should take to manage this risk in addition to the IT and other steps we will describe:

  - Limit the information you collect to what you must collect
  - Comply with the HUD Manual on Privacy Act matters
  - Follow best practices to comply with other laws
  - Create detailed written program (See Massachusetts guidance)
  - Review current and proposed contracts and service arrangements
  - Do periodic assessment of full program to confirm you are still meeting market and regulatory standards.

Specific Threats, Specific Actions

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- There are threats that are more likely in smaller organizations
- For these threats, there are specific actions that you can take to protect yourself
- These threats include:
    - Social Engineering
    - Password Hacking
    - Phone Fraud
    - Email Fraud
    - Mobile Attacks
    - Wireless Attacks
    - Document Security

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

What is Social Engineering?

Social engineering is the practice of obtaining confidential information by manipulating legitimate users.

Social Engineering is behind upwards of 90% of all successful security breaches

What information are they looking for?

- *Passwords*
- *Phone Numbers*
- *Names*
- *System information (dial in numbers)*
- *Physical Access*
- *Locations of equipment rooms*
- *Naming conventions*
- *Application information (mail/browser/platforms)*

Phone Fraud

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- Over $10 billion of phone fraud is perpetrated in the U.S. each year. Unauthorized access to a phone system or phone account number can result in a financial nightmare. It takes only minutes to begin accumulating thousands of dollars in charges to a compromised phone system or calling card.

- There were nearly 1.3 million instances of phone fraud, in the U.S from January – June 2012. This is a 29% increase over the prior period, July – December 2011.

- 9 out of the Top 10 Banks and 34 of the Top 50 Banks either had their name spoofed in Caller ID data or were impersonated by fraud callers.

There are four basic areas of telephone fraud

- Toll fraud
- Calling card fraud or theft
- Cell phone fraud or theft
- Abuse of 1-800 calling service

Desktop Security

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Log-off - before leaving a workstation unattended.**
  - This will prevent other individuals from accessing the Client A network under your User-ID and limit access by unauthorized users.
  - User timed password protected screensavers.
- **Lock-up! – Offices, windows, workstations, sensitive papers and PDAs, laptops, mobile devices / media.**
  - Lock your workstation (Ctrl+Alt+Del and Lock).
  - Encryption tools should be implemented when physical security cannot be provided.
  - Maintain key control.
  - Lock up sensitive information.
  - Never remove any assets tags from our equipment.
  - Lock away any laptops, PDAs or computer peripherals overnight.

Document Security

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

One of the most overlooked areas of security often involves physical documents. These are also information resources and require the same level of protection as their electronic counterparts. Follow these guidelines to make sure your files are where you need them, when you need them:

- Maintain a "clean desk" and keep your work space secured; i.e., lock up any sensitive files and diskettes.
- Don’t leave documents unattended on the copier or fax machine.
- Shred any confidential documents when you are discarding them.
- Remove papers and wipe boards clean when finished using conference rooms.
- Don’t just throw away unneeded floppy disks and CDs, destroy them.
- Lock filing cabinets when you leave.

Summary

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- Threats are increasing in frequency and sophistication
- Liability falls to the organization, and can even fall to individuals
- Individual identities are rarely worth more than $50 on the open market; volume matters
- ~90% of penetrations occur due to social engineering
- Appropriate policies are the key starting point, and cost little

Steps to Take Now

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

1. **Create and implement information security policies**
   - Follow industry best practices
   - Ensure all people who access information are aware of policies
   - Implement some form of compliance review
   - Be sure to address issues such as social media use, personal emails and mobility
2. **Implement basic information security procedures**
   - Secure physical copies of customer information
   - Setup and enforce complex passwords
   - Train employees on common threats such as social engineering, phone scams, phishing, etc.
3. **Leverage Available Solutions**
   - Deploy Anti-Virus, Anti-Spam and keep them up to date
   - Consider key-logging of employees with access to particularly sensitive data
4. **Consider Cyber-Risk Insurance**
   - Insures items not covered by traditional liability insurance
   - May provide coverage of officers' individual liability

Summary

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

$$B < P \times L$$

Best Practices and NRMC

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- NRMC will be working with NWOs to develop appropriate best practices for our members.

- Portland NTI: We will be holding workshops at CFO Convening and again on Wednesday May 8 at our one-day Risk Management Program to develop feasible and cost effective practices for NWOs and other providers of Affordable Housing.

- CyberRisk Insurance.

Contact Information for Speakers

Deborah Aschheim

NRMC – Executive Director

212.509.6762

debaschheim@neighborhoodrisk.org

Margaret Paradis

Special Counsel - Morris Manning & Martin

202.701.9310

mpar2@optonline.net

Chris Surdak

Senior Manager, Accenture

714.398.4874

chris@surdak.com