
NRMC
Neighborhood Risk Management
CORPORATION
NWOs working to insure safer communities
Visit us at www.neighborhoodrisk.org
CyberSecurity and Getting to the CORE of Technology Risks
NTI KC May 6, 2015

Agenda

Managing Cybercrime Risks

- **Background:**
  - **Recent Headlines**
  - **Legal Risks**
  - **Risk Management--ISO**
- **Best Practices—Steps to take Now!**
  - **The Plan**
  - **Dealing with Specific Threats**
  - **Third Party Arrangements**

Data Security is Headline News

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- In 2013, hackers had gained access to Target's network using credentials obtained from a vendor. The attackers ultimately got **40 million credit and debit card numbers** and **personal information on 70 million customers**. The breach also resulted in the resignations of Target's CEO and CIO.

- TJ Maxx loses **45.7 million credit and debit card numbers** over a period of 18 months.

- Sony loses **77 million PlayStation Network user accounts** that may cost over $24 billion to clean up.

- 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.

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.

Why Should You Care?

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- We know you care about protecting your residents' private information as a part of your public service mission to them.
- There are additional reasons to take action and implement a strong privacy and data security plan.
- You could face substantial legal liabilities for data breaches.
- Taking "reasonable" steps as defined by law and the market can limit these liabilities.

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 let's assume all of your customers.

- 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 another $165,000 per claimant.

- Investigation by a regulatory body will most certainly result in stiff fines and penalties, upwards of $150,000. And none of this is covered by general liability insurance. There is NO EXEMPTION FOR NWOs or non-profits.

Sources of Legal Liability

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Lawsuits and administrative enforcement actions by federal and state regulators, individuals and contract parties alleging breaches of:

- Federal laws on privacy and data security
- HUD requirements
- State laws on privacy and data security
- Disclosures
- Contracts

Legal Risks

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Federal Law**
  - Federal Privacy and Data Security protection for an individual's personal confidential information (PCI):
    - *Financial information: Gramm Leach Bliley Act (GLBA)*
    - *Health Information: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules*
    - *HUD: Subject to Privacy Act of 1974*

Legal Risks

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Federal Law**
  - GLBA does not provide detail on compliance the security standard—taking "reasonable" steps
  - Federal Regulatory Guidance--Some Highlights include:
    - *FTC red flags rule and privacy reports*
    - *Banking regulatory guidance (FFIEC)*
    - *SEC/CFTC recent identity theft red flags rule*
    - *HUD Manual requirements on disclosure and consent delivery*

Legal Risks

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **State Law**
  - States are generally free to impose stricter privacy and data security standards than federal law and some do.
  - **Massachusetts** has established a new higher baseline for a reasonable data security plan. It specifies detailed requirements for data security.
  - Holding information of just **one resident** of Massachusetts triggers the Rule! Not unusual for state law reach.
  - Service providers are also subject to it.
  - Other states should also be considered if they are relevant to your organization's operations. California data breach reporting requirements for example.

Legal Risks

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Contracts:**
  - By contract you or your counterpart (eg. Vendor) may be agreeing to protect information such as passwords, e.g. your electronic banking arrangements or service arrangements.

- **Disclosures**:
  - Your disclosures to others such as employees and residents and applicants about your privacy practices and those of HUD with the information gathered creates an expectation for the individual providing the information.

- **Courts/Agencies:**
  - Often it will be left to courts to determine whether an organization was applying “reasonable” security measures and finding the organization negligent and liable if its plan was deficient**.** Three key elements of successful case in this area (that are not typically difficult to show):
    - Breach of a relevant duty,
    - Breach as the cause of the loss, and
    - Actual loss.

Building the Right Data Security Risk Management Program for You

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- Background
- The elements of an effective appropriate risk management program for data security have been discussed by both government and other leading groups.
- We will present the process for creation of your plan through a series of best practices.

Building the Right Data Security Risk Management Program for You

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- These recommendations reflect our analysis of a number of critical sources defining what you are expected to do today:
  - Market events
  - Government guidance
  - Court decisions and
  - International standards

- Among the leading sources for guidance are the fundamentals for risk management provided by ISO, the International Organization for Standardization.

- Before starting the specific practices, we will go through these so our can consider them as you mange what is a fluid process in your organization.

Suggested Best Practices

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice # 1 - Identify your risks

- Know ***your*** organization's risk profile!
  - All organizations do not face exactly the same mix of risks, although there are some common risks.
  - Risks come from:
    - *People – the DOMINANT source of risk*
    - *Process – Or lack thereof*
    - *Paper – Properly management of hard-copy records*
    - *Technology – All forms of technology being used*
  - All of your protective measures should take all of these factors into account

Identifying your risks

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Consider these factors that create or influence risk:

- **Your physical facility set up:**
  - 1 or more locations? Shared space with other organizations or firms?
  - Configuration within office: open space, cubicles

- **Your system:**
  - what limitations exist on access to the PCI?
  - How do you transfer data to HUD?
  - Do you transfer the data to another third party's system, e.g., cloud recordkeeping service?

Identifying your risks

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Your data practices:**
  - What do you collect?
  - Do you collect only what is required by HUD?
  - Do you use the information for any purpose other than the applications?

- **Your disclosures:**
  - What do you disclose to applicants, tenants and employees about PCI?
  - What do you disclose to HUD in your arrangements with them about your policies for privacy and data security of the information being collected for HUD?

- **Your data collection process:**
  - How you collect the private information, electronically or paper (retained by you)?

Identifying your risks

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Your human resources:**
  - Who has access to the PCI within your organization--employees, temp workers or volunteers?

- **Your equipment arrangements:**
  - Where is the data stored? A cloud?
  - How is the data accessed?
    - *Equipment provided and maintained by you and/or equipment belonging to employees?*

- **Your contingency arrangements:**
  - Where/how do you backup the data?
  - Do you use third party services involving access to the data?

Creating Your Data Security Plan

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice #2 - Create a Data Security Plan

Create a written data security plan detailing administrative, technical, and physical safeguards, customized for your organization covering specified key areas.

- The level of detail of the plan should be sufficient to describe each of the key elements to allow for training and implementation through more detailed procedures.

Creating Your Data Security Plan

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Detail in Plan should at least meet the requirements of the Massachusetts Rule**
  - Establish responsibility within your organization with a person(s) who is responsible for the Plan
  - Identifying and assessing ***reasonably*** foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:
    1. ongoing employee (including temporary and contract employee) training;
    2. employee compliance with policies and procedures; and
    3. means for detecting and preventing security system failures

Creating Your Data Security Plan

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Detail in Plan should at least meet the requirements of the Massachusetts Rule**
  - Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
  - Imposing disciplinary measures for violations of the comprehensive information security program rules.
  - Preventing terminated employees from accessing records containing personal information.
  - Oversee third party service providers.
  - ***Reasonable*** restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.

Creating Your Data Security Plan

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Detail in Plan should at least meet the requirements of the Massachusetts Rule**
  - Regular monitoring to ensure that the comprehensive information security program is operating in a manner ***reasonably*** calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.
  - Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may ***reasonably*** implicate the security or integrity of records containing personal information.
  - Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Creating Your Data Security Plan

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Detail in Plan should at least meet the requirements of the Massachusetts Rule**

  - Secure user authentication protocols
    - control of user IDs and other identifiers;
    - a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
    - control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
    - restricting access to active users and active user accounts only; and
    - blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

Creating Your Data Security Plan

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Detail in Plan should at least meet the requirements of the Massachusetts Rule**
  - Secure access control measures that:
    - *restrict access to records and files containing personal information to those who need such information to perform their job duties; and*
    - *assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;*
  - **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.
  - Reasonable monitoring of systems, for unauthorized use of or access to personal information;
  - **Encryption** of all personal information stored on laptops or other portable devices

Creating Your Data Security Plan

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- **Detail in Plan should at least meet the requirements of the Massachusetts Rule**
  - For files containing personal information on a system that is connected to the Internet, there must be **reasonably** up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
  - **Reasonably** up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

Setting System Security Requirements

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

The Plan should include detail on certain system security measures you are adopting.

- The Massachusetts Rule specifies certain areas that at a minimum must be addressed.
- The following best Practices highlight these areas with suggested practical solutions.
- REMEMBER: EACH STATE HAS ITS OWN APPLICABLE RULES AND REQUIREMENTS. Contact a Cyber/Privacy Expert for assistance.

Creating A Strong Privacy/Security Culture in your Organization

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice #3 - Create a Culture of Security

Every member of your organization should integrate a strong privacy/security culture that is shown by consistent sensitivity to privacy protection.

- The value of any data security plan or specific security steps you choose lies almost entirely in the strength of your organization's privacy/security culture.
- Management must personally lead this effort.
- The responsibility of each employee in this effort must be stressed.
- The culture requires ongoing reinforcement.
- The Massachusetts Rule also requires this effort:
  - *Education and training of employees on the proper use of the computer security system and the importance of personal information security.*

The Inevitable

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice #4 - Plan ahead. Plan for the inevitable.

When a security breach occurs, respond promptly:

1. Confirm the breach has been fixed.

2. Size the breach in terms of time, accounts and data.

3. File any government notices as required.

4. Make any required notices to affected individuals.

5. Consider further action to address any potential damage to the individuals, even if not legally required.

6. Consider the impact on your organization.

Guiding Principles

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice # 5 – Integrate Privacy in your Plan

- Integrate privacy concern into each stage of operations (Privacy by Design)
- Simplify any choices available to consumers in controlling the privacy of their information, and
- Provide greater transparency to consumers concerning your collection practices and the information you have concerning them.
- These are three recommendations from the FTC to guide the creation of privacy policies and procedures. They are helpful in setting the right time internally and externally to confirm an organization's commitment to privacy.

Best Practices for Third Party Technology Contracts

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

These are best practices to be followed in your relationships and contracts with any third party technology service providers you engage that will have access to the PCI.

These practices are intended to provide these benefits:

- To limit the risk of data breaches,
- To limit harm to your residents, and
- To limit your liability *if there is a data breach.*

Third Party Technology Service Providers

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice # 6 – Cautiously select IT Service Providers

Choose your technology service company very carefully after following a disciplined diligence process.

- Under the Massachusetts Rule, you are required to take *reasonable* steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent
- Your diligence process for selecting a third party technology company should include review of these matters:
  - Historical records for privacy and breaches
  - Company's contingency arrangements
  - Whether the company has any familiarity with your regulatory environment

Third Party Technology Service Providers

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice # 7 – Carefully negotiate IT Service Contracts

Include clear terms in a written contract for privacy and data security compliance.

- Acknowledgement by the company of your ownership of the records, confidential status of data and applicability of privacy data security laws.

- Agreement to specified performance standards—including compliance with applicable federal and state(s) standard.
  - Reference the Massachusetts Rule as baseline
  - Also reference other states if they have special relevance to your organization such as California

Third Party Technology Service Providers

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice # 8 – Include breach protections in IT service contracts

Include clear terms for security breach scenarios, including notification deadlines and cooperation.

- Assume there will be security breaches because they are inevitable eventually.

- Be specific on the company's obligations to you: notice to you, timing of notice, responsibility for other required notices, and availability to respond to questions and support a joint response if you choose that.

Third Party Technology Service Providers

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice # 9 – Require controls and audits of IT service providers

Require the IT service providers to provide to you with a certification of adequacy of its security/controls annually, from a third party preferably.

- Technology service providers usually have their controls reviewed annually by an auditor because of the importance to their business.

Third Party Technology Service Providers

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice #10 – Identify contact people

Require the company to identify and provide full contact information for a person who will be your contact on an ongoing basis to address your concerns and to be available to you in the event of a breach.

Best Practice # 11 – Include secure data transfer

Include clear terms for secure transfer of your records when agreement is terminated.

Third Party Technology Service Providers

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice #12 – Include indemnification

Include a clause in the contract to provide for *indemnification* of your organization and directors, officers, employees and agents in the event of a breach for losses due to the company's security breaches.

Clouds

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Clouds can offer great benefits, including enhanced security in certain respects. However, there are some additional best practices to consider because of the further risks.

Special Best Practices for Clouds

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice # 13 – Understand clouds

Specify clearly in the contract the services you want to obtain to avoid any confusion leading to unanticipated dependence and loss of control.

- Studies have confirmed that many organizations do not really understand the package of cloud services they are engaging. There is risk associated with each service. Obtain only the services that you need.

Special Best Practices for Clouds

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice # 14 – Know where your data is stored

Understand where your data will be stored, in US or non-US locations, and in one or multiple locations so you can assess the risks related to data location.

- US laws generally allow storage of PCI outside the US, although it is considered to create an additional risk to be considered.
- Different countries have different privacy and discovery rules. Don't assume US law travels with your data overseas.

Special Practices for Clouds

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice # 15 - Transparency

Include terms for relative transparency on monitoring and incident reporting and contingency arrangements.

- You will be dependent on the provider for monitoring for breaches, but their monitoring typically covers all tenants in a multi-tenant cloud.
- Negotiate for information and a contact.

Special Best Practices for Clouds

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice # 16 – Know your providers' attitude towards security

Assess the data security approach of the provider and obtain information and assurances in the contract concerning their standards for matters such as identity sign on information and their security testing program.

- This would cover for example the risk that your internal system sign on information which you typically will share with the cloud provider to simplify access is protected within their system.

Special issues for Clouds

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Best Practice # 17 – Encryption

Assume that clouds will face increasing cyber attacks and consider additional steps to protect your most sensitive data even if not otherwise required, e.g., encryption.

,

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**
- **You are expected to take *reasonable* steps now!**
- **Ignoring this risk jeopardizes not your organization's reputation and economic viability, and key relationships.**

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.

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)*

,

Social Engineering

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

How do they obtain this information?

- Technical support impersonation: impersonating a technical support person requesting employee passwords via phone or e-mail
- Unauthorized building access: gaining unauthorized access to offices to steal computers, confidential documents, letterhead, or other proprietary material
- Information solicitation: requesting confidential company, client, or employee information
- Shoulder surfing: looking over someone's shoulder on airplanes, trains, etc. to read confidential information or passwords

What can they do with this information?

- Password grinding
- Exploit known applications (Outlook, Sendmail, IE)
- Use information gained to better future conversation and social engineering
- Gain knowledge of employee's (work habits, means of contact)
- Phishing / Fake e-mail

Social Engineering Flags

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Tactics that social engineers use

- Aggressive or authoritative behavior
- Overly friendly behavior
- Uncommon attempts to establish a trust relationship
- Unwilling to allow you to return their call or verify their information
- People who seem to be in an extreme rush and need information quickly
- People claiming to be vendors, temporary employees, contractors, and law enforcement personnel
- Pieces of factual information, with an attempt for you to fill in the blanks.

Signs that you have been had

- Very abrupt conclusion to a call after you have given a certain piece of information
- Wanting to know even more specific information about a topic that was not the original intent of the call
- Conversations about physical location, or physical orientation.

Prevent Social Engineering

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Tips on how to combat social engineering

- Know what information has value
- Ask for a callback number
- Write down the number if displayed on caller ID
- Be cautious of callers that block their number
- Ask for identifying information such as phone extension or office location
- Don't be afraid to challenge them
- Uniforms are cheap - keep your guard up
- Challenge them even if they have a "know it all attitude" or come across very authoritatively

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

Preventing Fraud

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- Be sure you know where you are transferring callers.
- Do not transfer unknown callers to an outside line.
- Use strong voice mail passwords.
- Change voicemail passwords often.
- Verify area codes before calling or faxing to unknown numbers.
- Be wary of faxes, emails, voicemails, and letters that require you to call a number you do not recognize.
- Be wary of people calling and claiming to be from the phone company asking you to enter any number combinations on your phone. Do not do anything that they ask until you have verified that they are legitimate.
- Do not give your calling card number over the phone to an unknown caller.
- Avoid leaving your cell phone unattended and place it out of sight if leaving it in a vehicle.
- Using the lock code on your phone can help limit the amount a fraudulent calls charged to your phone should it be stolen.

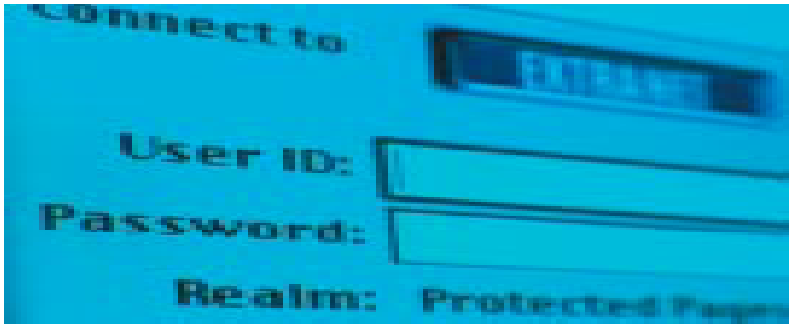
Password Requirements

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- Network access passwords must be at least 8 characters in length and must include at least 3 of the following four character styles:

Group	Example
Lowercase letters	a, b, c, ...
Uppercase letters	A,B,C, …
Numeral	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Special characters	( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /

- Do not use a password that can be found in a dictionary, or words associated with Client A, movie names, geographical locations and mythology.
- Passwords must be changed every 90 days.
- Consecutive passwords should not be cyclical (e.g. January, February or happy01, happy02).



Strong Passwords

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Strong password creation

We've all seen license plates that are customized with initials, names or personal messages. They are sometimes referred to as 'vanity' plates. By taking a combination of letters and numbers, a phrase can be spelled out without using complete words. You can use this method to create passwords, too.

Simple Phrase	Password
Too late again	2L8again
Music is for me	MusikS4me
Day after today	dayFter2day

Complex Passwords

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Complex Password Creation

Using the first letter of each word in a phrase can also help construct a good password. The object is to pick a phrase that is at least eight words long and then use the first letter of each word.

Complex Phrase	Password
Jack and Jill went up the hill to fetch a pail of water	J&Jwuth2fapow
I spent too much at the fair last night	Is2matfln
What I would give for a really good password	WIwg4argp

Protect Your Password

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Your password should be protected in the same way as the PIN number for your bank card or social security number.

- Never share your password with anyone.
- The Customer Service Center will never ask for your password.
- Never write your password down.
- Be aware of your surroundings while using your password.
- After receiving technical support, change your password.
- Don't allow PC or web browsers to remember your user ID or passwords.
- You will be held accountable for any actions that are performed under your user ID.
- Notify the IT department if you feel that your account has been compromised.

Phone Usage

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

While personal telephone use is not prohibited at Client A, we do ask that you make sure that your personal calls:

Do Not:

- Interfere with employee productivity
- Pre-empt any business activity
- Involve solicitation for or operation of a personal business
- Disclose your voicemail password

Do make sure that:

- Voicemail password length must be a minimum of 4 numbers
- Voicemail passwords must not be the same as (or subset of) the user's phone extension.
- The initial voicemail password must be a unique random number

Email Use

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

E-mail is a great business tool but it should not be used inappropriately. Emails that are potentially offensive or limit Client A's productivity have no place within our organization. They are a threat and a risk to the level of comfort we would like to maintain in your work environment. The following guidelines must be followed when using Client A email resources.

- Email communications should be limited to relevant Client A business.
- Use digital signatures, encryption or hush mail when sending sensitive emails.
- Email communications cannot be used to transmit information that may be considered inappropriate, e.g. of a sexually explicit, violent, vulgar, or criminal nature, or otherwise offensively address age, gender, sexual orientation, race, religious or political beliefs, national origin, or disability.
- Limit email use to trusted machines when transmitting Client A information.
- All Client A email is subject to monitoring.

Viruses

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

What is a Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses are usually transmitted via email attachments or downloaded from un-expecting internet users. Viruses are now being spread via instant messaging (IM) programs such as, AIM, MSN messenger and Yahoo IM.

Virus Prevention Tips

- Don't open emails from unknown source.
- Don't open emails with unknown attachments.
- Keep your anti-virus software up to date.
- Scan your full system for viruses regularly.
- Only download information from known and trusted sources.
- When downloading critical applications, check hash values.
- Back up files on a regular basis.
- Always err on the side of caution!!

Virus Infection

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

How to identify virus symptoms

- Unexpected sounds or screen images
- Unexpected files on your computer
- Sluggish performance
- Slow network response times
- You received error messages when starting an application
- Strange activity during the boot up process
- It has been a while since your last virus scan

What to do if you think you have a virus

- Immediately disconnect from the network.
- Contact your local technical support.

Making sure that your anti virus software is up to date is your responsibility!

What's in your Spam

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Unsolicited commercial email (UCE), better known as spam, is email that is sent to a list of users on the Internet with the intent to sell a product, participate in surveys, install malicious software, or gather information which may be used to commit illegal activities. Spam has the following negative impacts on businesses:

- Spyware
- Fraud / Phishing attempts
- Viruses
- Inappropriate content
- Identity theft
- Pirated material
- Illegal drugs
- Loss of productivity
- It is against the law in some states

Combating Spam

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- Guard your email address.
- Don't give out your Client A email address to non-business contacts (such as online shopping sites).
- Review web sites privacy policies before entering your email address.
- Don't respond to spam email.
- Don't use your email address in newsgroups, forum or Usenet postings, or chat postings.
- Contact your local technical support.
- Just hit the delete key without opening .
- Be judicious of the websites that you visit. Never browse to a site that contains inappropriate content.

Phishing

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Phishing is a type of deception designed to steal your identity. In phishing scams, scam artists try to get you to disclose valuable personal data—like credit card numbers, passwords, account data, or other information—by convincing you to provide it under false pretenses. Phishing schemes can be carried out in person or over the phone, and are delivered online through spam e-mail or pop-up windows.

Tips to catch phishing attempts

- Valid businesses should not ask you to send passwords, login names, social security numbers, or other personal information through e-mail.
- Phishing emails will usually ask for an urgent response such as: Respond within 48hrs or your account will be closed. This is an attempt to get you to respond without thinking.
- They are sent with no personalized heading.
- They want you to click a link that will allow you to access your account information.

Been Caught Phishing?

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

If you think that you have been a victim of a phishing attack there are a couple of things that you can do:

- To make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just "http://".
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.
- Ensure that your browser is up to date and security patches applied.
- You may report "phishing" or “spoofed” e-mails to the following groups:
  - *email*
  - *email to the Federal Trade Commission at Link*
  - *when forwarding spoofed messages, always include the entire original email with its original header information intact*
  - *notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: Link*

Phishing Example

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Online Banking Alert

Need additional up to the minute account information?
Sign In »

Change of Email Address

Your primary e-mail address for Bank Online Banking has been changed.

Did You Know? You can change your address, order checks and more online. Sign in to Online Banking and click on the "Customer Service" tab.

Because your reply will not be transmitted via secure e-mail, the e-mail address that generated this alert will not accept replies. If you would like to contact Bank of with questions or comments, please sign in to Online Banking and visit the customer service section.

Phishing Example

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

▸ Home ▸ Investor Relations ▸ Careers ▸ Privacy & Security ▸ En Español

Dear Cardmember,

As a customer of Bank, the security of your personal and account information is extremely important to us. By practicing good security habits, you can help us ensure that your private information is protected.

Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety.

Due to technical update we recommend you to reactivate your account.In case you are not enrolled for Internet Banking, you will have to use your Social Security Number as both your Login ID and Password.To reactivate your account please start by clicking on this webpage :

We appreciate your business. It's truly our pleasure to serve you.

Bank Customer Care This email is intended for Citizens Bank users only. Ignore it if has been arrived by mistake.
Member FDIC Equal Housing Lender © Financial Group. All rights reserved.

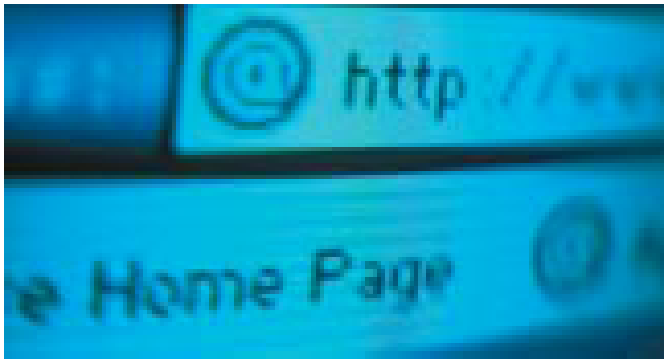
,

Internet Acceptable Use

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Web usage should be generally limited to business purposes. Web access to the following types of content is inappropriate:

- Online gambling
- Adult oriented material, and other obscene or offensive material e.g. of a sexually explicit, violent, vulgar, or criminal nature
- Offensively addresses age, gender, sexual orientation, race, religious or political beliefs, national origin, or disability
- Downloaded copyright material without appropriate consent
- Overuse of streaming media
- Solicitation of personal business
- Any illegal activity



Your Business may use computer programs that monitor or search computer use traffic, checking for particular words, patterns or activity, for the purpose of assuring system security and compliance with company policies.

Spyware

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

What is spyware?

Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent.

Tips on how to detect spyware

- You see pop-up advertisements even when you're not on the Web.
- The page your web browser first opens to (your home page) or your browser search settings have changed without your knowledge.
- You notice a new toolbar in your browser that you didn't want, and find it difficult to eliminate.
- Your computer takes longer than usual to complete certain tasks.
- You experience a sudden rise in computer crashes.

Software Usage Guidelines

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Official reports show that as much as 40% of software used in businesses today is not properly licensed. Violating software licensing can result in hefty fines and negative publicity.

- Only obtain software through our approved methods.
- Install software in accordance with its licensing.
- Don't share software with others unless authorized to do so.
- Maintain receipts for purchased software.
- Do not install software from your home computer onto your work computer and vice versa.

All software downloaded from the Internet must be scanned for viruses.

Risks to Mobile Computing

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

- ***Stolen or Lost Devices***
  The small size of modern handheld devices makes them easy to carry around. It also makes them easy to lose and a common target for theft. In addition to the replacement cost for the device, there is risk of unauthorized access.

- ***Unauthorized Access***
  Individuals may be inclined to store confidential information on their mobile devices that could be accessed by unauthorized users. This can include project information, client information, passwords, credit card numbers, PIN codes, phone numbers, etc.

- ***Removable Memory Media***
  Handheld devices may support external memory media (Compact Flash, Smart Media, Memory Sticks, etc.) that can be used to expand the limited storage capability of the standard device. These memory cards may contain confidential information, such as email, financial information, or Knowledge Exchange content that can be accessed with any compatible device without authentication.

- ***Viruses and Other Harmful Content***
  Viruses and Trojan horses (or Trojans) can infect mobile devices and possibly destroy the contents of the device. A virus is a program or piece of code that is loaded onto a device without the user's knowledge and runs against the user's wishes almost always causing damage. Viruses can also replicate themselves. A Trojan is a program that appears to be legitimate, but actually does something malicious. Trojans are often used to gain back-door access to a device, but do not replicate themselves.

Laptop Security

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

According the Computer Security Institute (CSI) and FBI survey, more than 6.7 million laptops were stolen last year alone. This is a drastic increase from the previous year which resulted in 600,000 laptops were stolen. The following list are places where employees need to be more cautious and aware of your surroundings.

- At an airline or rental car counter
- While waiting for your plane
- When going through the airport x-ray
- While at your hotel
- As you are loading your luggage into a taxi
- While using a public pay phone
- On a crowded train or bus
- If you stop to help a stranger (decoy)
- At a meeting or a conference

It's Just a Laptop?

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

The major concern of laptop theft is not the loss of a physical asset. The major concern of laptop theft is the intellectual information that resides on the laptop. According to the CSI/FBI 2002 survey The theft of a laptop results in an average financial loss of **$49,246**; only a small percentage of the sum actually relates to the hardware cost. Laptop theft came in 3rd for financial loss from attacks or misuse in organizations.

Computers are stolen for the following reasons:

Cash Value: Some PCs are simply taken to be sold for the cash value. Often, the information on these machines is passed along in the transaction and has no interest to any party involved. If the thief has some technical knowledge, then the computer may have its information wiped out to prevent it from being traced back to the original owner.

Value of Information: Corporate or personal information gathering tactics could include the theft of a computer for the data that resides on it. Some foreign governments openly accept this practice to obtain intellectual properties. Be particularly careful when traveling internationally

Competitive Information: Unscrupulous companies or organizations may resort to computer theft to obtain information about their competition. This could include stealing computers from the competitors themselves or from other organizations that work with or for their competitor. In some industries, knowledge about the competition can be worth billions of dollars.

Securing your Laptop

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Tips for securing your laptop

- Use cable locks or lock your laptop in a drawer or cabinet during off hours.
- When traveling, always keep visual contact with your laptop.
- Never put your laptop on the airport security x-ray machine until you have an unobstructed path to retrieve it on the other end. Your laptop should be the last item to go through the x-ray machine.
- Never leave your laptop in plain sight while it is in your car. Lock it in your trunk (Avoid leaving your laptop in extreme hot or cold environments).
- Make sure all vital information on your laptop is backed up frequently.
- Never check your laptop as luggage when traveling.
- Use disk encryption where available.
- Choose an inconspicuous carrying case.
- Be aware of your surroundings!
- Never remove any assets tags from our equipment.
- Write down your model and serial numbers of your devices.

Portable Device Security

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

Many computer users, especially those who travel for business, rely on laptops and smartphones because they are small and easily transported. But while these characteristics make them popular and convenient, they also make them ideal targets for thieves. Make sure to secure your portable devices to protect both the machine and the information they contain.

- Keep them with you at all times.
- Use a keypad lock.
- Use power-on passwords.
- Shut off IR transmission when not needed.
- Don't allow Bluetooth connections.
- Keep your portable device software and patches up to date.
- Use encryption.
- Be aware of your surroundings; don't allow shoulder surfing.
- Back up your information.
- Display contact information on the device.

Wireless Networking

Neighborhood Risk Management CORPORATION
NWOs working to insure safer communities

There are two aspects of WLAN security: data protection (encryption) and network access control (authentication). Breaches can occur at the network level via the wireless access point (AP), or at an individual PC - either attached to a network or operating in ad hoc mode and communicating in a peer-to-peer fashion.

Requirements for secure wireless use

- Make sure that your personal firewalls are up to date.
- Make sure that your anti-virus software is up to date.
- Don't configure your laptop to run in ad-hoc mode.
- Use your VPN connection especially when using public access points.
- Use Client A approved encryption.
- Do not install wireless equipment unless authorized by Client A Network Team.
- All Client A networks, including wireless networks are subject to monitoring activities.

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.

Contact Information for Speakers

Deborah Aschheim

NRMC – Executive Director

212.509.6762

debaschheim@neighborhoodrisk.org

Guy Gioino

Vice President, Risk Services Leader, East Region

HUB International Ltd.

908-790-6868

guy.gioino@hubinternational.com


Thanks…
QUESTIONS