**Information Systems Management**
**Course 95-822**

**Spring 2006**

# Final Consulting Report

## Wireless Neighborhoods

**Suvrat Chakradeo**

# Wireless Neighborhoods
# Executive Summary

Student Consultant, Suvrat Chakradeo
Community Partner, Tony Lodico

## I. Background Information

Wireless Neighborhoods is a non-profit organization that provides access to information technology resources for low-income communities and faith-based organizations, so they can increase their capacity. Their mission (as it relates to technology) is -

> *To empower communities and faith-based organizations by providing access to information technology resources.*

They are located on 218 North Highland Avenue in Pittsburgh, PA. Their major activities include providing wireless broadband Internet access to organizations and running after-school programs for school children.

## II. Consulting Tasks

The first task was the creation of a list of information technology assets of the organization. This included desktop PCs, printers, routers, copiers, fax machines and other appliances. The list helped to evaluate the risk of information security threats against these assets.

The next major task was the creation of a template for conducting security audits. A checklist/template based on the ISO 17799 security standard was created by the consultant. With the help of the CP, this template was modified to fit the needs of the organization. Three different version of this checklist were created, each with a different level of complexity, so that they could be used to audit different types of organizations.

This checklist was used to run a trial audit on the organization itself. Furthermore, a simplified single-page questionnaire was created to assess the level of security skills of an organization. Using this, one can assign points out of 100, based on the level of security.

Finally, a list of best practices for information security was created in the form of a small document.

## III. Outcomes Analysis and Recommendations

To complete the first task, the consultant observed the different kinds of IT hardware and software owned by the organization and asked questions to the CP about it. He then estimated the approximate value of the assets.

For the creation of the security audit template, the consultant studied recent security standards including ISO 17799 and browsed various resources on the Internet for relevant information. Using these, he compiled a checklist of questions in order to conduct a security audit. This was discussed with the CP to eliminate questions which were not relevant or useful. Some questions were suggested by the CP and added to the checklist.

The CP and consultant used this checklist to conduct a security audit on Wireless Neighborhoods itself. To cater to the needs of the different profiles of customers and members of the organization, 3 different audit templates were created with varying levels of security awareness and complexity. An organization can progress from one level of security to the next higher level using these as guidelines.

A list of best practices for information security was created as a guide to the organization and its customers and members for future reference.

The first recommendation is to create a technology plan. A technology plan will bring structure to the hitherto ad-hoc technology planning. It will help to project a more professional image to their donors. It will also help to evaluate the achievements of the organization on the basis of what was planned.

The other recommendation is updating the website to include more information on information security. Since this is the public face of the organization, it will help to create a security-savvy image in the consumers' perspective. This will help members and customers to keep their knowledge on information security up-to-date and also attract more customers.


Community Partner
Tony Lodico
*antoniolodico@gmail.com*

Director of Technology
Wireless Neighborhoods
218 North Highland Avenue
Pittsburgh, PA
*www.wireless-neighborhoods.org*

Student Consultant
Suvrat Chakradeo
*suvrat@cmu.edu*

Graduate Student
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA
*www.cmu.edu*

# Wireless Neighborhoods
# Final Consulting Report

Student Consultant, Suvrat Chakradeo
Community Partner, Tony Lodico

## I. The Consulting Situation

### Organization

"The purpose of Wireless Neighborhoods is to empower communities - to provide access to resources to enable community groups and faith based organizations to become competitive in education, human development, workforce development, health care and economic opportunity. Many community groups and faith based organizations, especially those in low-income urban areas, lack the resources required to succeed in these activities, especially in the new era of information technology. Wireless Neighborhoods provides the resources to develop necessary human skills and network infrastructure to help community groups enhance their programs and work collaboratively with schools and other community groups."[1]

Wireless Neighborhoods became an independent organization in 2004.

There are 4 employees - Executive Director, Technology Director, Education director and 1 assistant. Its core operating budget is $250,000 and program budget is $1 million. Wireless Neighborhoods gets the bulk of its funds from the Heinz Endowment. It also gets funds from the state government, the federal government, Pittsburgh Partnership for Neighborhood Development and Pittsburgh Urban Redevelopment Authority.

### Facilities

The office is located at 218 North Highland Avenue, Pittsburgh PA in a low to moderate income community. It is easily accessible by local Port Authority Transit buses. Wireless Neighborhoods rents the 2nd floor of a small building. There are 4 offices and one large conference room. There is a color inkjet printer/scanner and a laser printer/photocopier. There is a small refrigerator and a microwave oven. Each office has a desk, chair, filing cabinets and a computer. The building is old but clean.

### Programs and services

These are the main programs Wireless Neighborhoods focuses on-

- Community Technology Center – This program provides education and support services to

[1] "Welcome to Wireless Neighborhoods – Wireless Neighborhoods". Wireless Neighborhoods Inc. April 2006. http://www.wireless-neighborhoods.org/

approximately 200 9th grade students at Peabody High School. The programs are offered through a network of five community technology labs, one at Peabody and the others at community and faith based locations around Peabody.

- 21st Century Community Learning Centers – This program serves 100 2nd grade students in 4 lower-income Pittsburgh communities including the Hill District, Garfield, East Liberty, and Oakland. Children will be engaged in a learn-through-play curriculum designed to complement their in-school curriculum.

- Parental Engagement – This project provides parental engagement activities to parents of the children in two after school initiatives. The families of the 2nd grade students in the 21st Century program and children in the Hill Learning Collaborative program are provided materials, training and support in their efforts to be more engaged in the children's education.

- Education Support – Through a grant from the Pittsburgh Partnership for Neighborhood Development, Wireless Neighborhoods is able to offer all of its member organizations support around electronic and traditional curriculum development in their efforts to align their curriculum with Pittsburgh Public Schools.

- Wireless Broadband – Wireless Neighborhoods provides high speed wireless broadband connectivity to 38 organizations. [2]

## Staff

**Stephen MacIsaac, Executive Director**
Stephen was appointed as the first Executive Director of Wireless Neighborhoods in December 2003. For day to day operations, the administrative duty falls on Stephen. He goes out and gets grants, handles the finances, convenes partner and board meetings and determines the overall vision and processes of the organization.

**Tony Lodico, Director of Technology**
Tony started work on the Wireless Neighborhoods Project as the Community Technology Coordinator for the East End area in July 2003. Tony handles the front-end technology of Wireless Neighborhoods and performs some administrative functions.

**Joyce Keyes, Director of Education**
Joyce creates curriculum for after school programs, distributes it and works with the schools and after school programs to implement it.

**Aimee, Educational Program Co-coordinator**
Aimee works as an assistant to Joyce. She helps in creation of the curriculum for school programs.

[2] "Programs and Services – Wireless Neighborhoods". Wireless Neighborhoods Inc. April 2006. http://www.wireless-neighborhoods.org:8080/WN/wnaboutus/wnprograms

## Technical Environment

Each employee has a personal computer with Windows XP. There are a total of 6 desktop computers (there are 2 computers in the public space). Each computer has Microsoft Windows XP and Microsoft Office 2003. The computers are used for word processing, managing finances, maintaining databases, emails, remotely managing routers at client locations and other office purposes. There is a copier/laser printer, another laser printer/scanner and a color inkjet printer. Although staff can use what they need, additional training may help. Wireless Neighborhoods has 3 servers at a colocation facility of AspStation (a for-profit ISP). One server with Windows 2000 is currently not being used. Another server has Windows 2003 and it is used for software hosting and file backup. The web hosting and email is done on a FreeBSD server. A Linksys RV042 router provides a wired Ethernet connecting the network printer, while a Netgear WGR614 wireless router provides an internal wireless network. The network uses 128 bit WEP encryption. All the computers have AVG 3 anti-virus software.

At each client location, Wireless Neighborhood installs a Tsunami MP-6 or MP-11 Subscriber Base Unit. It has a directional antenna which connects to Wireless Neighborhood's communications tower in Oakland. Internet connectivity is provided by a Linksys RV042 router which is connected to the antenna.

## Technology Management

The Director of Technology, Tony Lodico, is responsible for all the front-end technology management. He solves technical problems, trains the staff on technology related issues, fixes hardware and maintains the equipment. When other staff members have a problem with their computer, they come to Tony for help. Tony also provides technical support to customers and clients who use Wireless Neighborhood's Internet services. There is no specific maintenance plan or technical support strategy. Having a technology plan and a technical support strategy would be very useful.

## Technology Planning

There is no technology planning and actions are taken according to need. Tony, the Technology Director, is responsible for most technology decisions. Some amount of financial planning is done for technology and funds are allocated in the budget for proposed purchases. A network committee meets once every 2-3 months to discuss technology issues.

## Internal and External Communication

Day-to-day communication with staff members is mainly verbal. Informal communication with community member organizations takes place over the phone. Email is used for formal communication. Each employee has an email account on the Wireless Neighborhoods domain. Most information about customer records and financial information is stored in Microsoft Excel sheets. There is a useful and functional website, whose hosting is outsourced to AspStation.

### Information Management

Critical information such as financial information, formal documents, email, network information, school children's information is mainly stored in Microsoft Excel sheets. Backups are taken at regular intervals by the Technology Director. There is no encryption or any other security for this critical information.

### Business Systems

Accounting processes and payroll are outsourced to a member organization. The service provided is satisfactory. No major problems have been encountered.

## II. Consulting Task

### Improve the overall network security of the organization

Wireless Neighborhoods has a large and complex network. They have set up directional antennae and routers at client locations. These are connected to their servers at AspStation via a hub and spoke model of directional wireless links. In addition to maintaining the security of their internal network, Wireless Neighborhoods is also responsible for the security of its routers at remote locations.

An attack on one of their machines could potentially cripple their network. This would disable the Internet connectivity provided to the different clients all over Pittsburgh. This would directly impact their mission of providing access to technology to community organizations. It would also endanger the security of the internal networks of the clients and member organizations. Confidential files containing financial information, school children's information could be stolen. Additionally, Wireless Neighborhoods also needs to comply with HIPAA. Any successful attack on their network could nullify HIPAA compliance. Also, to preserve its image as a technology organization which helps other organizations to set up networks, security is absolutely necessary. Thus, network security is essential for the day-to-day functioning of the organization, and directly impacts its mission.

Approach-

- Gather information about the internal and external network of Wireless Neighborhoods.
- Obtain specifications of hardware and software on individual computers
- Prepare a list of information technology assets
- Evaluate the security risk against these assets
- Evaluate different possible solutions for increasing network security and select one or more suitable approaches for implementation

- Create a set of policies and procedures for network security and inform all users of the policies and procedures
- Create a template for performing security audits
- Set up a system to install and manage anti-virus software on different computer on a network from a single, centralized location
- Evaluate the need and feasibility of an Intrusion Detection System
- Conduct a security audit for Wireless Neighborhoods and for a member organization and explain the process to the community partner
- Work with the community partner to create awareness among staff members about information security This is critical to long term success
- Examine router and firewall settings and recommend secure settings and options

Expected outcomes-

- List of information technology assets
    - It can be measured by checking if the list is up to date and accurate
    - There is no current measure because no such list exists
- Risk matrix of IT assets
    - It can be measure in terms of dollar loss
    - No current measure
- A list of best practices for information security
    - Can be measure by comparing against current standards like IS 17799
    - No current measure
- A checklist for evaluating security
    - Can be checked to see if it is comprehensive
    - No current measure
- A template for conducting a security audit
    - One measure is whether they can produce a clear and agreeable plan for testing and maintenance
    - No current measure
- Improved information security skills in staff
    - Can be measured by interviewing staff and testing their skills

The intended effects on the organization are-

**Organization-**

It will enhance the image of Wireless Neighborhoods as a technology organization. The organization sets up routers for other organizations and connects them to the Internet. Since Wireless Neighborhoods provides technology services to its members and customers, it is also indirectly responsible for the security of their networks. Its work is closely related to technology, and so the improved image will help it market itself and increase its customer base. It will also help them present their case to prospective funders and donors.

**Facilities-**

The organization's facilities will be more secure and will have physical security countermeasures.

**Programs-**

The organization will be able to provide better information security to its customers and member organizations. In effect, the quality of its services and programs will be enhanced.

**Staff-**

The staff members will be more aware of security issues and will be better prepared to handle security risks and incidents. The solution will be sustainable because the technology director will know how to execute each step of the process.

**Technical Environment-**

The organization's computer systems will have up-to-date security countermeasures. They will be easier to maintain and diagnose in the event of a system compromise.

**Technology Management-**

The CP will be able to configure and maintain security settings on routers. The staff will develop an understanding of basic security issues and will be prepared for any eventuality. The CP will be able to reconfigure router and firewall settings as the organization expands and gets more customers and members. All the organization's systems will be regularly scanned for viruses and malware.

**Technology Planning-**

The technology plan will include planning for security investments and training and maintenance costs.

**Internal and External Communication-**

The organization will be able to share internal documents and other files in a secure way, if they use encryption.

**Information Management-**

The CP will take regular backups of critical data so that it can be restored in case of data loss or modification.

### Feasibility of work-

There are almost 2 months to complete the proposed work. The consulting partner is highly motivated and passionate about his work. The organization has the necessary resources for the proposed work, and it fits the CP's and consultant's skills. The CP will develop the necessary skills and will be able to sustain the security policies and procedures. The major risks involved are that the policies and procedures suggested will not be easily adopted by the organization. Another risk is the sustainability of these policies and procedures.

## III. Outcomes and Recommendations

Technology forms the basis of Wireless Neighborhood's Internet service. By ensuring that their own network is secure and their customer's networks are secure, Wireless Neighborhoods provides reliability and customer satisfaction. The routers installed by the organization have a built-in firewall, which protects the internal network against intrusions. The organization has good security practices and provides an example to other organizations about how to improve their own security level.

The CP and the consultant discussed ways to increase the security level of Wireless Neighborhoods and its members/customers. Together, they developed security audit checklists to measure the level of security of an organization.

Task – **Improve the overall network security of wireless neighborhoods**

### Results/Outcomes

**A list of information technology assets**

A list of information technology assets or an inventory list was prepared by the CP and the consultant. Details such as hardware, model number, serial number, cost/value were included in the list. This list is useful for the organization to be aware of its assets, so that it can measure what is at stake with respects to information security risks.

### A list of best practices for information security

A list of best practices relating to information security[3] was obtained from the CERT website and recommended to the organization by the consultant. The best practices provide a guideline to the organization for its day-to-day work with regards to network security and data security. It includes things such as using a firewall, antivirus protection, regular backups and simple user precautions such as not opening suspicious email, disabling ActiveX and JavaScript etc. The overall technology plan should take into account these best practices. The CP uses this list of best practices to decide the overall policies.

### A template/checklist for conducting a security audit

A checklist/questionnaire for conducting a security audit was prepared by the consultant and the CP. 3 different checklists were prepared with increasing levels of complexity. The simplest checklist has around 44 questions. The medium-complexity checklist has 84 questions divided into sections such as organizational security, personnel security, physical security, access control, systems maintenance and compliance. The most detailed checklist adds a few more sections and is meant to be used for large organizations. As organizations increase their level of security, the more advanced checklists can be used for auditing them. These checklists help to measure the level of security at an organization. An organization can then try to attain a higher level of security. Based on this checklist, a security audit was conducted on Wireless Neighborhoods by the consultant. This helped WN to assess what areas of security it needed to improve. The checklists will be used to conduct audits on other member organizations and customers.

### Improved information security skills in staff

Employees of any organization are crucial for its security. Security skills among employees have to be improved to improve the overall information security of an organization. By conducting awareness sessions and distributing security-related educational material such as a list of best practices, the CP improved the security skills of the employees of the organization. The improvement was measured using a questionnaire for employees.

## The state before the consulting partnership began

Before the consulting partnership, the organization did not have a comprehensive list of its information technology assets. No one had an accurate idea about the IT assets and their worth. The organization did not have any policies/practices for information security. After a security incident, a reactionary measure taken was to change all public IP addresses to private addresses using Network Address Translation. There was no way of conducting security audits or performing risk assessments. There was little or no awareness among employees about information security.

[3] "Home Network Security" Carnegie Mellon CERT Coordination Center, February 2006. http://www.cert.org/tech_tips/home_networks.html

## Concrete evidence of outcomes yet to be reached

The improvement in security skills among the employees has yet to be observed. There is a learning curve and this will take time. However, based on the list of best practices and the CPs expertise, this outcome will soon be observed in a span of a few months.

## Evidence of Extended Capacity

Since the organization now has a comprehensive list of its Information Technology assets, it can allocate necessary resources and prepare a plan to safeguard these assets from security threats. By following the list of best practices, the organization can gradually increase its level of security. It can apply the same to its member organizations and customers and help them attain higher levels of security capability. As a result, the organization can handle and respond to security incidents more effectively. Using the audit checklist, the organization is able to categorize its customers by assessing their level of security. It also helps in creating a technology plan for the organization which focuses on security. The organization can also assess its own level of security and maintain compliance with government regulations such as HIPAA. This has increased the quality of the services provided by Wireless Neighborhoods to its customers.

## Evidence of Sustainability

The list of IT assets/inventory list can be easily updated by the CP on a daily/weekly basis. The CP is responsible for most of the technology purchases, allowing him to update the inventory list when new purchases are made or old equipment is discarded. The CP was involved in every stage of creation of the security audit checklists. These were created keeping in mind the current profile of Wireless Neighborhoods customers/members. So the CP can update the checklists if the profiles of the customers/members change. The list of best practices has been created according to current industry standards. It will have to be updated as the organization grows and standards change. The CP was involved in the creation of this list, so he will be able to update it.

## Risks

There is a risk that the security skills of the employees may not be sustained. New security threats keep coming up every day. Therefore, employees have to adapt and develop the latest skills. Constant training is needed to keep up the level of awareness. This may not be an easy task for the organization to achieve. The CP will have to train new hires about security issues. The CP can provide new hires with some reading material on basic security skills and practices.

## Recommendations

**Vision**
Wireless Neighborhood's Internet service business heavily relies on technology. The organization takes care of the security of its own internal network and sets an example to other

organizations about security issues and practices. They have built-in firewalls on their routers, which are installed at client locations. This provides protection against hackers and viruses. The organization keeps its customers and members satisfied by providing reliable and secure services.

**Goals**

The following goals are recommended to help the organization move towards its mission within a time-span of 3 years.

- Create a technology plan
- Publish security related information on the organization's website

**Strategies**

*1. Create a technology plan*

Currently, Wireless Neighborhoods does not have a technology plan. There is a 'network committee' which meets roughly once a month to make decisions on technology issues. Technology decisions and purchases are made on a need-based basis. A technology plan will provide structure to technology related decisions and issues.

The technology plan would help the organization get rid of ad-hoc technology planning.

The organization needs to create a technology plan, which includes aspects of information security. The following steps can be taken to create a technology plan-

- Forming a technology committee - There is already a network committee, which may be considered to be the technology committee.
- Using various web resources for the technology plan
- Looking up sample technology plans on the Internet
- Creating a set of metrics to measure goals

Outcome: A formal technology plan document

The technology plan will help the organization plan its actions ahead of time. The plan can be revised every year, according to the observations in the previous year. At the end of each year, one can measure how much of the technology plan was accomplished. Documents such as project plan, task assignment, progress report, Gantt chart will be useful.

Resources:

Internal Resources-

- The board of directors and technology committee will form the group which makes the technology plan.
- Time spent on planning is a resources which will be used

External Resources-

- Web resources such as www.techsoup.com can be used to help in technology planning. Techsoup.com is a website targeted specifically at non-profits. It contains articles, discussion forums, message boards, donated products, news stories and many other useful resources for non-profits.
- An IT consultant may be consulted for the technology plan. The consultant would help in understanding the technology problems and creating a draft of the technology plan.
- The website of the Technology Consulting in the Community course at Carnegie Mellon University has a list of useful resources -

  http://www.andrew.cmu.edu/course/15-391/Resources/

  This website has links to other useful non-profit websites. There are links to technology planning websites and local resources.

*2. Publish security related information and current security news on the organization's website*

The organization's website is its public face. It is a medium to reach out to potential customers and members. In order to project a security-savvy image, Wireless Neighborhoods can publish information on its website about current security news and issues. Links to other security websites can be provided. The following steps can be taken for this goal-

Forming a team to update content on the website

- Using the existing content management system to create content from news articles, security literature and other resources
- Creating interactive content on the website which increases the level of computer security awareness. Links to free personal firewalls and anti-spyware software can be provided.
- Updating the website regularly with new content. This can be done using RSS feeds from Microsoft Onecare and Symantec Antivirus.

Outcome: A better website with more content on information security

Interactive content on the website will help users and members learn more about computer security. They will be able to better protect their computers against hackers and viruses. The impact of this outcome can be measured by counting the hits on the website and tracking the number of hours each user spends on the website. Online polls can also be created on the website to assess the popularity of the website.

Resources:

Internal Resources-

- The education director is already in charge of creating and managing web content. She can take over the task of adding new content on information security.
- The existing content management system can be used for this task

External Resources-

- Web-page creation software such as MS Frontpage, Dreamweaver, and Adobe Pagemaker will be required for the creation and publishing of this content.
- Also, a good Pentium-class computer will be needed to create the web content
- The organization can advertise security software products on their website and make money.

## References

Previous reports from the Technology Consulting in the Community class-
http://www.andrew.cmu.edu/course/15-391-reports/index.html

## About the consultant

Suvrat Chakradeo is a graduate student at the Information Networking Institute at Carnegie Mellon University. He is pursuing a Master of Science in Information Security Technology and Management. He is interested in systems engineering and security consulting, and aspires for a career in one of these areas.

# Appendices

## Appendix A – Simplified security checklist

| | | |
|---|---|---|
| **Management Information Security Forum** | Has a forum been established to oversee and represent technology issues? | Y___<br>N___ |
| **Cooperation between Organizations** | Is there a liaison with external information security personnel and organizations including industry and/or government security specialists, law enforcement authorities, IT service providers, telecommunications authorities? | Y___<br>N___ |
| **Security Requirements in Outsourcing Contracts** | Have the security requirements of the information owners been addressed in a contract between the owners and the partner organization? | Y___<br>N___ |
| **Inventory of Assets** | Do you have an updated complete inventory of your technology assets? | Y___<br>N___ |
| **Information Labeling and Handling** | Has a process been implemented for labeling information that requires security protection? | Y___<br>N___ |
| **Network Diagram** | Have you created a network diagram to show your equipment and how it is interconnected? | Y___<br>N___ |
| **Personnel Screening and Policy** | Are employment applications screened for jobs that require access to sensitive information? | Y___<br>N___ |
| **Confidentiality Agreement** | Are non-disclosure agreements required? | Y___<br>N___ |
| **Terms and Conditions of Employment** | Do the terms and conditions of employment include the employee's responsibility for information security, including duration after employment and consequences of failure to fulfill these terms? | Y___<br>N___ |
| **Information Security Education and Training** | Before they are granted access to IT facilities, are users trained in information security policies and procedures, security requirements, business controls and correct use of IT facilities? | Y___<br>N___ |
| **Reporting of Software Malfunctions** | Are users required to note and report to IT support any software that does not function correctly? | Y___<br>N___ |
| **Learning from Incidents** | Are mechanisms in place to monitor the types, volumes, and costs of incidents and malfunctions? | Y___<br>N___ |
| **Disciplinary Process** | Does a formal disciplinary process exist for dealing with employees who violate security policies and procedures? | Y___<br>N___ |
| **Physical Entry Controls** | Are entry controls employed over secure areas to ensure only authorized personnel can gain access? | Y___<br>N___ |
| **Equipment Location and Protection** | Is equipment located to reduce risks of environmental hazards and unauthorized access? | Y___<br>N___ |

| | | |
|---|---|---|
| **Power Supplies** | Is electronic equipment protected from power failures and other electrical anomalies? | Y___<br>N___ |
| **Equipment Maintenance** | Have procedures been established to correctly maintain IT equipment to ensure its continued availability and integrity? | Y___<br>N___ |
| **Clear Desk and Clear Screen Policy** | Has a clear desk/clear screen policy for sensitive material been adopted to reduce risks of unauthorized access, loss, or damage outside normal working hours? | Y___<br>N___ |
| **Removal of Property** | Are personnel required to have asked permission to take equipment, data or software off-site? | Y___<br>N___ |
| **Segregation of Duties** | Are sensitive duties or areas of responsibility kept separate to reduce opportunities for unauthorized modification or misuse of data or services? | Y___<br>N___ |
| **Capacity Planning** | Are capacity requirements monitored, and future requirements projected? | Y___<br>N___ |
| **System Acceptance** | Has acceptance criteria for new hardware and software been established, and have suitable tests been performed prior to acceptance? | Y___<br>N___ |
| **Controls Against Malicious Software** | Has anti-virus software been installed on all computers? | Y___<br>N___ |
| | Have user awareness procedures been implemented to prevent spread of viruses? | Y___<br>N___ |
| **Information Back-up** | Has a process been established for making regular back-up copies of essential business data and software to ensure that it can be recovered following a computer disaster or media failure? | Y___<br>N___ |
| **Fault Logging** | Do procedures exist for logging faults reported by users regarding problems with computer or communications systems? | Y___<br>N___ |
| **Disposal of Media** | Is a process in place to ensure that computer media is disposed of securely and safely when no longer required? | Y___<br>N___ |
| **Publicly Available Systems** | Is there a formal authorization process before information is made publicly available? | Y___<br>N___ |
| **Password Use** | Have users been taught good security practices in the selection and use of passwords? | Y___<br>N___ |
| **Unattended User Equipment** | Are all users and contractors made aware of the security requirements and procedures for protecting unattended equipment? | Y___<br>N___ |
| **User Authentication for External Connections** | Are connections by remote users via public or non-organization networks authenticated to prevent unauthorized access to business applications? | Y___<br>N___ |
| **User Identification and Authentication** | Do all users have a unique identifier (userID) for their personal and sole use, to ensure that their activities can be traced to them? | Y___<br>N___ |
| **Password Management System** | Is an effective password management system employed to authenticate users? | Y___<br>N___ |

| | | |
|---|---|---|
| **Use of System Utilities** | Are the system utility programs that could be used to override system and application controls strictly controlled and their use restricted? | Y___<br>N___ |
| **Terminal Time-Out** | Are terminals in high-risk locations set to time out when inactive to prevent access by unauthorized persons? | Y___<br>N___ |
| **Information Access Restriction** | Are people allowed to access information on a need-to-know basis? | Y___<br>N___ |
| **Event Logging** | Have audit trails that record exceptions and other security-relevant events been produced and maintained to assist in future investigations and in access control monitoring? | Y___<br>N___ |
| **Mobile Commuting** | Has a formal policy been developed that addresses the risks of working with mobile computing facilities, including requirements for physical protection, access controls, cryptographic techniques, back-up, and virus protection? | Y___<br>N___ |
| **Input Data Validation** | Is data that is input into applications systems validated to ensure that it is correct and appropriate? | Y___<br>N___ |
| **Message Authentication** | Has message authentication been considered for applications that involve the transmission of sensitive data? | Y___<br>N___ |
| **Encryption** | Is data encryption used to protect highly sensitive data during transmission or in storage? | Y___<br>N___ |
| **Intellectual Property Rights** | Is there compliance with legal restrictions on the use of copyright material ensuring that only software developed by the organization, or licensed or provided by the developer to the organization, is used? | Y___<br>N___ |
| **Safeguarding of Organizational Records** | Are important organizational records securely maintained to meet statutory requirements, as well as to support essential business activities? | Y___<br>N___ |
| **Data Protection and Privacy of Personal Information** | Do applications that process personal data on individuals comply with applicable data protection legislation? | Y___<br>N___ |

# Appendix B – Simple survey

Simple Security Survey

Physical environment safety

- All cords are tucked away out of accidental reach (2)
- All technology is away from areas that are prone to disaster or malicious action (2)
- All hardware is located on stable surfaces (2)
- All hardware is connected to surge protectors (2)
- Critical/expensive equipment is hooked up to a Universal Power Supply (3)
- Checks are made that all equipment is there daily (such as headphones) (5)

Backups

- There is a backup of organizational data (finances, payroll, inventory etc.) (6)
- Each individual employee has a backup of his/her critical data (5)
- There is a remote backup (off site) (3)
- The Backup is taken daily/weekly/monthly (3)
- The Backup is password-protected and stored in a locked private location that is not publicly known (2)

OS

- Windows Update is set to automatically download and install updates and patches (4)
- I run Windows update manually every ____ days
- All have valid licenses (3)
- All computers have the same operating system (XP if PC) (3)
- There is a password (passwords) for the Admin account (5)
- Only one person has administrative rights (2)
- Accounts are created and access is given on a need to know basis (2)
- The organization takes care that the admin password is not lost (3)

Software

- All have anti-virus (4)
- All have anti-spyare (2)
- All have the same anti-virus product (2)
- All have valid licenses (2)
- All are set to auto update (3)
- All are set to auto scan daily/weekly or more (4)
- All computers have a personal firewall (Windows XP has a firewall by default) which is turned on (4)
- All Applications have valid licenses (3)
- I check for Microsoft Office updates every week (2)
- I understand that Microsoft never sends out updates/patches/announcements via email

and I do not click on unsafe email links (4)

Passwords

- There is a password policy which is enforced and made know to everyone (4)
- All passwords are at least 8 characters long and have a combination of letters and numbers (5)
- Passwords don't contain names of people or other easily guessed strings (names of family members/ phone number / address) (4)

Total : _____ / 100 points