Identifying a weak link in the network chain: Determining how prepared Dominican IT administrators are to confront today's security issues

Héctor Henríquez Badía

Follow this and additional works at: https://scholarworks.rit.edu/theses

Recommended Citation
Henriquez Badia, Héctor, "Identifying a weak link in the network chain: Determining how prepared Dominican IT administrators are to confront today's security issues" (2010). Thesis. Rochester Institute of Technology. Accessed from

This Thesis is brought to you for free and open access by RIT Scholar Works. It has been accepted for inclusion in Theses by an authorized administrator of RIT Scholar Works. For more information, please contact ritescholarworks@rit.edu.
Identifying a weak link in the network chain:
Determining how prepared Dominican IT administrators are to confront today’s security issues.

By

Héctor Henríquez Badía

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Networking and Systems Administration

Rochester Institute of Technology
B. Thomas Golisano College of Computing and Information Sciences

May 23\textsuperscript{rd}, 2010.
Thesis Approval Form

Student Name: Hector Omar Henríquez Badía

Thesis Title: Identifying a weak link in the network chain: Determining how prepared Dominican IT administrators are to confront today’s security issues.

Thesis Committee

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charles Border, PH.D</td>
<td></td>
<td>04/22/2010</td>
</tr>
<tr>
<td>Chair</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jeffrey Lasky, M.S.</td>
<td></td>
<td>04/22/2010</td>
</tr>
<tr>
<td>Committee Member</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arlene Estevez, M.S.</td>
<td></td>
<td>04/22/2010</td>
</tr>
<tr>
<td>Committee Member</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Identifying a weak link in the network chain:
Determining how prepared Dominican IT administrators are to confront today’s security issues.

I, Hector Henríquez, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: 5/25/2010  Signature of Author: Héctor Henríquez
© Copyright 2010 Hector O. Henríquez

All Rights Reserved
Abstract

Enterprises in Dominican Republic are growing in size; this means that sooner or later these enterprises will have the necessity to create an IT department to manage their systems and networks. This research studied how secure an enterprise can be with Network administrators from the mentioned country. This study used mixed methods to get more deep results about the mentioned problem. This research discovered that Dominican IT administrators are well versed in network security theory, but when it comes to apply this knowledge at work, according to the qualitative part of this research they are slothful, and take things lightly; they usually believe that the network of the company they work for can’t be the target of an attack resulting in a high threat. In the end, the last conclusion that this research gives, is that for IT Administrators in Dominican Republic it depends more on the network security policies that the enterprise impose than the skills of the IT administrators.
**Table of Contents**

1- Introduction: ................................................................................................................................. 8
2- Literature Review: ............................................................................................................................ 10
3- Purpose Statement: .......................................................................................................................... 18
4- Methodology: ..................................................................................................................................... 18
5- Results: ............................................................................................................................................. 19
6- Appendices: ....................................................................................................................................... 53
7- References: ....................................................................................................................................... 79
Special Thanks

To my parents for giving me my life, and for supporting me in each step that ultimately led to the completion of this degree, to my fiancée for being that special person that accompanied me through the complete degree, to Prof. Charles Border for giving me all those good counsels that led me to do a good research, and as the last but not the least to Prof. Mario Sanchez for helping me to get inscribed in this Master’s of Science degree.
1- Introduction:

Enterprise Network Security is hard to achieve in these days and for business to have a reasonable level of network security not only they need to invest in technology but also in employee education to help reduce threats to their data assets. One of the problems that many organizations confront is that people assume that the only threat to a network system is the end user and no one analyzes if the practices of IT administrators are really healthy for the Enterprise network. What if the IT administrator doesn’t have enough knowledge about security threats or has limited information about them, well it really becomes a threat to the entire company, because they compromise its information assets. This research studied about Dominican Enterprise IT administrator’s security practices. This included their criteria when evaluating the security of new software that will be implemented in the company. The main purpose of this research was to know what considerations Dominican IT administrators take in order to give certain software enough trust to implement it in the company, and if they are aware of the security breaches this new software could generate, and the impact it could give to the company in case a security breach is exploited, an example to this could be the implementation of a new accounting software that doesn’t receive updates.

Since, generally speaking, this research seek to understand the security practices of Dominican IT administrators, this involves behavior and psychology, which is better done with a qualitative method study, but, to get a more complete view of the issue the research needs to also know the behavior of the population, and this is better done with a quantitative method study. In conclusion the best approach for this study is to do a mixed methods study, in order to get the best of both methods and to have a more deep perception of the problem in the Dominican Republic.
This study focused on Dominican enterprises that have their own IT department, that manages more than 500 employees, and that have spent a significant amount of money in their IT infrastructure, evaluated by the Dominican National Ministry of Work. This research made personal interviews to the chosen enterprises IT administrators, and after these interviews were done, a set of two surveys were done according to the knowledge acquired from the interviews; these surveys were distributed to different IT administrators so they helped to get a broader sense of the situation of this problem in Dominican Republic. This study deliverables included the interview questions, the unrefined results of those interviews, the results of the surveys, and the formal report that analyzed the results.

This study is very important for the Dominican Republic, and the world, because it demonstrates how prepared are IT administrators in this area, and when concerning about security, how secure can an enterprise be with the local IT administrators. Since almost every enterprise in the mentioned country is having the necessity of creating an IT department, and global enterprises that might want to invest in the country, will also have the need to create one, or the like, this study helps them have an idea about how prepared are local IT professionals in the data security area.
2- Literature Review:

2.1 – Introduction:

Related work on this subject is mainly focused on end users instead of IT professionals, people usually think that IT administrators are aware of all security problems that may exist, and that their practices are secure, mainly because they are professionals, but this might not always be true, there is a possibility that there could be IT administrators working in Dominican enterprises that have not studied network security, and so aren’t completely aware of what are the best practices to help diminish possible security breaches. This review is structured as follows: The first topic treated will concern user security management, next is the concern for human factors and software vulnerabilities, followed by the concern for password management security, finally the conclusion of this literature review.

2.2 – Concern for user security management:

A study by [1] Jeffrey M. Stanton et. Al. (2004) interviewed 110 people with end user security-related behaviors, a conduct ranking exercise with 49 IT experts and ran a US survey of 1167 end users, with the objective of acquiring self reports of their password-related manners. The results of their research demonstrate that six categories of end user security-related behaviors appeared to fit well, these six categories can be seen on the table depicted on picture A. The US survey results showed that password hygiene was very poor and that good password hygiene is related to education, consciousness, monitoring, and enthusiasm. The difference between this work and the study mentioned above is that this thesis is focused in a different culture, creating the possibilities of discovering different behaviors.
The study by [2] Gross et. Al. (2007), describes a research that the authors did by interviewing end users to determine their security practices. The result of this research is that end users are getting more and more concerned about security; they also found that users that have a closer contact with the IT administration tend to be more aware of security problems, created from certain practices. The difference between this work and the study mentioned above is that this thesis is focused on the IT professionals that work on the country, it also uses a mixed methods approach, with the objective of getting more deep palpable results, and it is focused in the Dominican Republic specifically, which creates a new example on how IT professionals manage security in the mentioned country.
In a paper by [3] Joshua B. Gross et. Al. (2007), their research was based on a survey done on a broad group of internet users, the results of this study demonstrated that users are more concerned with security problems than they are with other types of computer problems. The difference between the current research and the above one is that it is focused on the network security knowledge level of the IT professionals of the Dominican Republic, and it also uses a mixed methods approach instead of quantitative methods.

A research paper done by [4] Rachna Dhamija et. Al. (2006), provide pragmatic evidence about malicious strategies that has success at misleading general users. In their study they examined a large set of captured phishing attacks and then they created a theory about why those tactics may work, they also did an experiment in which 20 websites were exposed to 22 people, this experiment consisted in making these people choose whether the website was or wasn’t fraudulent. The results of this experiment established that 23% of the volunteers did not look at the address bar, status bar and security indicators, this lead to incorrect choices 40% of the time. They also found that visual deception attacks can also fool even the most experienced users, which demonstrates that everyone can become fooled by an attack like this. The main difference between this research and the current one created on this document is that the last one uses mixed methods instead of only using quantitative methods.

A research paper done by [5] Dourish et. Al. (2004), examined how people experience security as an aspect of their daily life, and how people each day ask themselves “is this system secure enough for what I want to do?” [5]. They present an amount of results relating to the scope of security, position towards security, and other concerns that point in the direction of new technical solutions. The main differences between this research and the current on this document are that the last one uses mixed methods to obtain the results, and that it was focused to IT administrators in Dominican Republic.
A paper done by [6] Greiner et. Al. (2008) depicts discoveries found at the SECtor conference in which Microsoft’s Steve Riley spoke about that the OSI model should have an eight layer, this layer is called the wetware or the human being using the computer, this component of the network is one of the most vulnerable components of all the seven layers. While a large quantity of money is invested in technological security solutions, users still get tricked with old fashioned con jobs.

This happens because every system, including a network, relies on human beings to some extent, and since it is becoming harder to hack systems, why not hack the network administrator instead? After this question the author describes that Steve Riley spoke about a series of techniques that could be used to trick even the most cynical IT administrator, these techniques were: diffusion of responsibility, chance of ingratiation, trust relationships, moral duty, guilt, identification, desire to be helpful, cooperation.

It is important to denote that each of these techniques could be used against systems administrators in the Dominican Republic:

a) Diffusion of responsibility: When a scammer convince a system administrator by saying that it is really not his responsibility and that a superior individual in the company agreed with the malicious action. This could happen in the Dominican culture because in the grand enterprises sometimes there are too many contracted individuals, and these ones could say that certain high positioned person permitted them to do certain type of action.

b) Chance of ingratiating: Could happen when a scammer offers to pay a high amount of money for information that the system administrator has. This is possible to happen in the Dominican culture since many people tend to be very greedy.

c) Trust relationships: These might happen when the scammer creates a trust relationship with the system administrator; it can be so well done that the system administrator would end saying all the secrets of the security vulnerabilities of the enterprise networks without even noticing it. In Dominican culture this could happen when a scammer is very clever and start speaking with the system administrator, or even makes a plan to get to know the IT administrator and with time gain confidence to leech important information.
d) Moral duty: Happens when a scammer convinces the system administrator that the system has something is incorrect, and that he could solve it. This might happen in the Dominican culture since the scammer could say that he/she is an expert in solving a type of problem.

e) Guilt: The technique is about convincing the individual to think that if the system administrator doesn’t cooperate then this person will feel guilty. A scenario where a parent of the scammer is dying if he/she doesn’t gets what he/she wants is an example of how could be an intention to scam a Dominican system administrator, since everyone in this country greets everyone warmly they could feel guilty if they don’t help the scammer.

f) Identification: The scammer creates a connection with the victim that really helps him to gather information. This can happen in the country by creating a bond between the scammer and the victim; maybe they get to go out to drink beer, play dominoes or something that could help the victim believe that the scammer means no harm.

g) Desire to be helpful: This technique is all about tricking the system administrator to help the scammer to log in to certain account, but this leads to exploitation. People in the Dominican Republic are of a very warm nature and normally they done believe that someone is trying to scam them, so this could really be a good technique to try to trick a Dominican in general.

h) Cooperation: This technique is all about forcing the victim to comply with the orders that the scammer gives, sometimes with terror, this is a very poor technique but it sometimes work. It is very possible that this technique doesn’t work with Dominicans because when a Dominican sense a troubled people, will try to stay away from the trouble.

The most interesting thing noticed about this paper is that it is one of the little few that takes under consideration that the IT professional is vulnerable to social engineering and other types of pranks.

A paper done by [7] Stevenson et. Al. (2004), describe that security best practices are characterized as a procedure that has performed remarkably well in business. To educate how to design and implement security best practices is crucial to students that will eventually become IT professionals. These security best practices are taught in a security lab, under the direction of a
student security team and faculty advisor. The paper also points that this security lab is a realistic learning model in training and educating IT undergraduates and graduates in proper security practices. The approach proposed by [7] Stevenson et. Al. (2004), poses a good way to diminish security breaches provoked by the IT professional, but with time people get slouch and starts not follow security best practices. The cited research differs from this thesis in that the last one uses surveys and interviews, in a mixed methods approach, instead of the quantitative methods used in the cited paper. This means that this thesis could bring new discoveries that could be found on both qualitative and quantitative methods.

2.3 – Concern of Human factors and software vulnerabilities:

The research paper done by [8] Islam et. Al. (2008), discuss the recognition and categorization of human factors that affect the results and efficiency of software risk management. Categories of individual, team, management and stakeholder, as well as for the activities of security risk identification, analysis and mitigation are used to classify the mentioned human factors. The difference between the cited research and the current thesis is that the last one analyzes the security knowledge of the Dominican IT professionals with a mixed methods approach and delivers a theory that shows how much these individuals know about network vulnerabilities.

A paper done by [9] Collins et. Al. (1994), says that perfect programs for complex systems cannot be achieved empirically, this is because every part of a program could contain errors, and also people who use the program could use it incorrectly. The response to the question posed by the article is related to the time of the release of the software and the form of safeguarding the users from the inevitable errors. The cited research differs from the current thesis in its objective, which is to know the level of security knowledge that the Dominican network administrators have, but they have similar subjects, and also both describe human factors as a source of vulnerabilities to software (in the case of the cited research) and networks (in the case of the current research).

A research paper done by [10] Ohringer et. Al. (1990), affirm that in computer security the phrase “A chain is only as strong as its weakest link” is not always true, because if there are parts of the organization’s security practices that challenges the IT best efforts, you could compensate
by improving other parts of the system. In his paper the author states that one of the links of the computer security chain is the software which is very weak, but another is the user which it also is one of the weakest links. The author describes that by improving user awareness, it is possible to compensate the weakness in this link of the computer security. Differences between the cited research and the current thesis are on the methodology used the last one uses mixed methods to obtain the results, meanwhile the cited research uses qualitative methods to obtain them.

2.4 – Concern for password management security:

The research paper done by [11] Gaw et. Al. (2006) focuses in the vulnerability that poses poor password management that users tend to have. According to the paper people reuse their passwords in distinct accounts, increasing their vulnerability. This means that if a password is compromised, the attacker could take in possession of all the accounts that share the same password. According to a study made in the paper that involved 49 undergraduates, the majority of users had three or fewer passwords and passwords that were reused twice. The reason for this to happen is that users created new accounts but did not create new passwords for those new accounts. The paper also discusses on what are the best password management practices. This research differs from the cited research paper in that it uses mixed methods to get more deep results and in that it is focused to the Dominican Republic IT administrators, which can lead to a different approach because of cultural manners.
2.5 – Conclusion:

After reviewing the literature in this subject, the author of this research was able to determine that human factor is a frequent cause, if not the main cause of many of the vulnerabilities that a network has. Because what can the technology do to avoid vulnerabilities if the professional in charge of using it is very easy to trick by con jobs. The most important idea to take under consideration is that even after training the user to help avoid security problems, they still are vulnerable to scams and other type of frauds. So when speaking of network security it is possible to conclude that while there are people using the computers there will always be a possibility of vulnerability.

Something also noticed by the author of this research when reviewing the literature is that the majority of the research papers found used quantitative or qualitative research methods only, but almost none used mixed methods to obtain their conclusions, which is the methodology used in this research. This is one of the causes why this research may create a different approach, since not only the subjectivity of the qualitative methods is used nor only the exactness of the quantitative methods, but it instead uses both of them to create a deeper thought of knowledge that can create a more profound theory of the problem itself.
3- Purpose Statement:

This investigation sought to better understand the security practices used by Dominican system administrators.

4- Methodology:

The methodology used in this research was a mixed method which is a combination of a qualitative method research and a quantitative method research. This type of research was made in order to get better results. Since the interests of the author is to know the extent of the problem in the Dominican Republic, finding a solution to the problem was not contemplated, but only the extent of the problem. The author’s objective in this research was to know what kind of security practices or customs Dominican IT administrators currently have, and if they are conscious of the possible threats a software or a website could generate, and what are the facts that make them decide if a website or a program can be trusted enough to be used in the enterprise network. The outcome of the thesis was a theory about the extent of the problem described and possible reasons about the causes of it, which are included in this document.

The qualitative part of this research was done by making face-to-face interviews to six Dominican IT administrators. The interview questions helped to determine the way the individual makes decision about security practices and the best way to maintain the security of the company’s data assets. The objective was to analyze people’s minds, which can be quite subjective, so the questions were focused to the IT administrator’s opinion, with the objective of getting a feel of their knowledge about network security, the author took notes about the responses and developed the material for the subsequent survey that was done to other enterprises. The process to make the quantitative survey was to use a website called www.surveymonkey.com where the IT administrator entered and then answered questions to get a wider idea of the situation in the Dominican Republic. The IT professionals were invited by an email sent to them by the author of this research.
5- Results:

5.1- Qualitative study data collection:

See 7-Appendices.

5.2- Qualitative study data analysis:

5.2.1- Introduction:

In this section the qualitative study data analysis is made. The instrument used to gather the information was in the form of interviews, this instrument was composed of a questionnaire of 10 network security related open questions. The author interviewed six IT professionals from the Dominican Republic. With these interviews the author was able to obtain valuable information about the network security practices of a sample of the information technology professionals that work on the island. The questions used in the interviews where created to make the interviewed people to speak openly about what they believe that is the best response to each question, in this process the author took notes of any important network security related practice that was found. Notes were taken of what each interviewed professional said about what they do in their current work, this was very important to capture, because this demonstrated whether they were organized or not, all these factors were taken under consideration on each interview that was handled. Also the author was able to record digitally each interview for further analysis of the exact situation and each answer of the interviewed professionals.

Qualitative instrument construction:

The qualitative instrument used in this qualitative study is an interview formed by a questionnaire of open questions. The questions used in the interview were made to evaluate different topics related to network security knowledge, to vulnerabilities and attacks, knowledge that should be known by every network professional.

The questions used in the interviews where:

1. What facts you consider to be important when deciding that a program or website is trusted enough to be used in the enterprise?
2. For you, what is the importance of company data assets?
3. In your words, what must be done to diminish malware?
4. What do you think is the difference between spyware and virus?
5. What practices you consider that you can do, to help secure the enterprise data assets?
6. In your opinion, what is the importance of maintenance in network security?
7. What do you think about social engineering? Is it an issue for the network security?
8. Do you consider that to have a disaster recovery plan is important for the enterprise? If yes, why? If no, why?
9. When speaking about passwords, what is your strategy for maintaining it secure?
10. Do you believe that a company needs to apply network security policies? If so, why?
Questions description:

In this section each question will be described by the author in order to know what is being evaluated, what is the purpose of the question and an example of what should be the answer.

The first question is about what facts should the information security professional take under consideration, in order to trust a program or website to be used in the company. This question tries to see the important facts that the IT administrator believes that make a program secure enough to be implemented in the enterprise network. The response might be that it is certified by a prestigious company, that has support, and that cares for detecting vulnerabilities in the code by creating frequent updates to it to diminish possible threats to the company that uses it. Or the case of a program made by a local developer or a program developed internally, that at least it should have proper support and good maintenance, focused in the elimination of vulnerabilities in it and in efficiency of the program or website.

The second question tries to evaluate the response of the interviewed professional when speaking about the importance of the company data assets, this means what this individual believes whether they are important or not. Sometimes people think that the enterprise data is not important because the enterprise is not theirs, but this could demonstrate that the people is not very happy with their job, this is surely a very subjective question, since the answer may vary with the mood of the interviewed towards the company this person works. A possible answer to this question might be that the data assets are very important for the enterprise, if not the most important asset that an enterprise can have since without it companies would be working like in the twentieth century, with lots of paperwork and lots of space occupied with them.

The third question tries to evaluate the interviewed individuals to try to speak of what they consider to be important to reduce the malware threat to the company. This question is very easy to understand, since it’s about what can the IT personnel do to help eradicate malware in the company’s network. In this question the interviewed could demonstrate their security knowledge regarding malware, since to really keep malware to its minimum level it is needed to have a good combination of network security software, network security policies, and network best practices training to each user of enterprise network equipment. So if the interviewed doesn’t know what does it really takes to keep them to its minimum then this could help evaluate their network security knowledge level.

The fourth question asks the interviewed professional to cite the main differences between a spyware and a virus. It is important to know that if the interviewed doesn’t know the exact difference or says that they have nothing in common, it can be two things, and one is that this person doesn’t know anything of malicious programs like viruses and malware, or two this person really knows but is currently confused and doesn’t know the exact differences. The author believes that it is important to see the difference between both causes of bad answers and to notice the real truth behind it. A possible answer to this question is that spyware are a type of virus that its only objective is to gather information and send it to a hacker, then virus is generally known as a term for malicious software, but in fact any kind of software that reproduce itself can be named as a virus, so a virus can be a software that reproduces itself without exactly having any kind of malicious purpose.
The fifth question is about what the interviewed professional can do in order to help secure the enterprise data assets. The objective of this question is to gather a list of possible practices that the IT professional would do to assure the security of the enterprise data, this could lead to further know what have done the interviewed professional in order to create a secure environment for the data of the enterprise where this individual works. A possible answer might be to create network security policies that limits the people that enters the data center, trainings for the end users for them to learn what they must do to avoid phone scams, network security trainings for the IT professionals to keep them actualized with the latest security knowledge, network security policies that makes users change passwords on a monthly basis, between others.

The sixth question is about the importance of maintenance in the security of the enterprise network. This question puts the interviewed professional in the position of judging if maintenance is important or not for the enterprise network security. A possible answer to this question might be that maintenance is very important for the enterprise network security, in both senses, this means physical maintenance and software maintenance, the physical maintenance will help keep the data secure since a clean physical environment will make the equipment work better and make them last longer and in consequence the data will be safe, meanwhile the software maintenance is about discovering vulnerabilities and patching them with upgrades, it is very important to keep all network equipment up to date to have a network free of network security problems.

The seventh question is about what the interviewed thinks about social engineering and if it is considered as problem for the security of the network. The objective of this question is to learn if the interviewed professional knows anything about social engineering and the dangers it brings to the enterprise network. A possible answer to this question could be: I consider that social engineering is a very important issue to the enterprise network, since every employee can become hacked as a computer and can give important information to strangers. A possible solution to this great network problem is to train all the employees to avoid being scammed.

The eighth question is about what is the interviewed opinion regarding the importance of having a Disaster Recovery Plan (DRP) in the enterprise. The objective of this question is to obtain a clear image of what does the interviewed IT administrator knows about DRP and to try to see if the interviewed says something about the implementation of DRP in the enterprise this person works. A possible answer to this question is: I consider DRP to be very important, in this company we usually consider each step that each one of the IT department must do in case of a disaster, and we even take under consideration natural disasters like earthquakes and hurricanes.

The ninth question is about the strategy that the interviewed IT professional use in order to keep secure passwords for the equipments that are in use in the enterprise network. The objective of this question is to obtain a clear understanding on what the IT administrator believes that a secure password is, and what does this individual do in order to keep it safe from strangers have their grasps on them. A possible answer might be: I believe in having an authentication key that generates a new password every 5 minutes, with the key combined with a password that is changed every month, it is virtually impossible for people to know which password is the current one, but it is also important to have a responsibility policy for the authentication keys.
The tenth question is about if the interviewed individual believes that the company needs to apply network security policies. The objective of this question is to learn what does the interviewed IT individual thinks about network security policies, this way the author can gather knowledge about if the company this person works does apply network policies. A possible answer can be: I consider that network security policies are a necessary to be applied on each company network in order to keep their data safe and sound, because with network security policies it is possible to create policies that control the access of certain users physically to the datacenter or by software to the servers, policies that enforce the training of each user to learn how to use their computers without exposing them to a vulnerability, policies to train IT administrators to keep them acknowledged with the latest security threats, summarizing network policies are the best form of network administrators to control not only the network but also the people who uses them.

Qualitative responses analysis

After analyzing the questions responses of each interview, the researcher was able to notice common qualities on almost all of the interviews; these common qualities can be identified as: Bad network security practices, Organized IT department, don’t have organized disaster recovery plans, Slothfulness, Carelessness, Bad password security, good level of theory knowledge, and good level of practice knowledge. For more information about which interview had which quality and what other details had been noticed in the interviews, be sure to check table 1, which has a summary of the valuable information gathered from the interviewed IT professionals.
Table 1: Qualitative study qualities Table which depicts which interviewed IT had which qualities and what level.

<table>
<thead>
<tr>
<th>Interview</th>
<th>Bad network practices</th>
<th>Organized IT dept.</th>
<th>Organized Disaster recovery plan</th>
<th>Slothfulness level</th>
<th>Carelessness level</th>
<th>Password security level</th>
<th>Theory knowledge level</th>
<th>Practice knowledge level</th>
<th>Industry of the interviewed employer</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. 1</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Medium to high</td>
<td>Medium</td>
<td>Low to medium</td>
<td>Medium</td>
<td>High</td>
<td>Construction</td>
</tr>
<tr>
<td>No. 2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Medium to high</td>
<td>High</td>
<td>Very High</td>
<td>Medium to High</td>
<td>Medium to high</td>
<td>Contact center</td>
</tr>
<tr>
<td>No. 3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Low</td>
<td>Medium</td>
<td>Medium to high</td>
<td>High</td>
<td>Medium to high</td>
<td>Telco. &amp; ISP</td>
</tr>
<tr>
<td>No. 4</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Food</td>
</tr>
<tr>
<td>No. 5</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Medium</td>
<td>Medium to high</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>ISP</td>
</tr>
<tr>
<td>No. 6</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Academic institution</td>
</tr>
</tbody>
</table>

5.2.2- Bad network security practices:

According to the information gathered from the interviews, there were a number of the interviewed individuals that weren’t security focused, which demonstrates that in Dominican Republic there exist individuals that are currently working in its enterprises that are almost never thinking of the possible threats that could affect the network they work. According to what the author obtained from this study most of them rely merely on antivirus to eliminate malware, which is good, but they never think on how to avoid malware infection on computers, nor do they almost never try to implement policies that control the users, in case that they get to implement any policy, it doesn’t last too long, with time they don’t maintain it. What was discovered is that in several of the interviewed individuals the company had serious malware problems, and the cause of this was because of the poor security that is applied by their IT professionals.

Another problem that the researcher was able to discover in at least one of the interviews, is that not only people that study an IT related career work in the IT field; this is also a cause of bad security practices, because these people don’t have any kind of network security related preparation. As an example of this, one of the IT administrators, that the researcher was able to interview, was still an undergraduate and wasn’t studying an IT related career, the researcher was able to ask him how he was able to get the job, he answered that he worked at a company that normally repairs computers, so there he got his experience, but after the interview the researcher was able to notice that this individual didn’t have almost any knowledge of network security and instead of avoiding the problems, or foreseeing the problems before they arrive he simply waited until they happen and reacted to fix the problem. The big question is why the enterprise doesn’t fire him, well because most of their owners don’t know much about computers and
they simply think that these problems are part of the computer technology and doesn’t really know that it is incompetence of the IT in charge.

According to the information gathered from the interviews, it is possible to deduce that in Dominican Republic exists the possibility of encountering IT administrators that their academic profession is not compatible with their job, this could mean that a construction engineer, or a lawyer can be found working as an IT administrator, and the like. Many causes are behind this problem; one of the possible causes could be that jobs in Dominican Republic can be gained by influences and not only by skill. With this said, is possible to affirm that this is one of the main reasons why companies are plagued with bad network security practices.

5.2.3- Carelessness and slothfulness:

The researcher was able to interview people that were professionals in the IT industry, and that knew some network security in theory, but in their actual labor, they failed to apply most of the network security best practices. A common reason of this issue was slothfulness and in some cases the excess of confidence on thinking that the company network is not vulnerable or carelessness. This shows that they have certain degree of recklessness. The researcher noticed that some of these qualities where found in at least 5 of the 6 interviews in total. One of the most interesting interview was the second one, in which the researcher interviewed an IT admin, who demonstrated that he knew enough about network security to actually maintain it quite safe, but when the researcher asked further specific questions about the importance of maintenance and security policies, the interviewed was able to indicate the researcher indirectly that most of the security practices that this person knew, weren’t applied in the enterprise. The main cause of the problems described in this paragraph, according to the information gathered from the interviews, was because of slothfulness and in some cases carelessness; it is possible to affirm that the interviewed individuals, that showed these qualities, tend to take things lightly.

Even though there might be exceptions to this quality, since there are businesses in the country that have strict security measures, these businesses are mainly banks, Telecommunications Service providers, and financial related enterprises. They have such security policies that it is even hard to get an appointment with their IT administrators, because of their fear of being tricked by a social engineering scam. This can demonstrate that Dominican enterprises that their income depends on the health and neat state of their data really invest on network security. This is consequently traduced in them training their IT administrators with network security knowledge, or they contract professionals abroad that have good experience and knowledge in network security. These IT administrators are the ones that work on companies like: The leading Telco Codetel, on banks like “Banco Popular”, and on “Orange” another Telco. The main point is that the best network security practices can be found on enterprises like these, as well as the best IT professionals.

The researcher was able to interview one IT Admin from an academic institution that is really focused in the security of their data. The researcher not only noticed the experience that the interviewed had but also noticed that what this person said was true and most of the security practices that this person knew was being applied in their network, at least the majority of them. The IT administrator was mainly focused on making policies that help the common user be conscious enough to avoid possible threats to the network system. This person demonstrated that not only IT administrators with bad practices can be found on the
country but also well prepared individuals that have knowledge about the main security threats that the internet world provides. But it also can demonstrate that this type of IT administrators is a minority in the total population.

5.2.4- **Disorganized IT departments and bad password security:**

In three interviews the researcher was able to notice that IT’s had all the network privileges in the enterprise, and in some cases only one password was used for them to access any equipment in their network, it’s also curious that the researcher was able to notice this being a foreigner in the enterprise, which could demonstrate that it is also easy to obtain critical information from these companies by using social engineering tricks. In two of the 6 interviews the researcher was able to notice that each time an IT administrator gets fired from the department they have to change all server passwords, meaning that they don’t do it very often, and showing that every time that they fire an IT professional it becomes a vulnerability for them since it was somebody that could enter any of the equipments of the network, this means that in case they forget to change the password of an equipment they could get hacked easily by the person who was fired. This was the case of the first interview in which the interviewed told the researcher that it was hard to know why they didn’t get hacked by the IT that got fired since they had their main servers vulnerable for about a week, and this person was talking about the database servers of the enterprise.

5.2.5- **Good theory knowledge and Good practice knowledge:**

The author of this research wasn’t only able to determine all the bad qualities that Dominican IT administrators have, but also the good qualities that can be found in them, these good qualities are that the majority of the interviewee demonstrated that they have good theory knowledge at least 4 out of 6 had good theory knowledge, and good empirical knowledge was also found in at least 3 of the 6 people that were interviewed.

5.2.6- **Don’t have organized disaster recovery plans:**

It was very interesting that of all of the interviewed IT administrators only the interviews number 3 and 6 really are that organized enough to have a working disaster recovery plan, and it was focused mainly in resiliency, which the researcher considers to be more adequate for every type of disasters that could occur in the enterprise.
5.2.7- Conclusion:

In this section of the research, the author was able to interview 6 Dominican IT professionals, from whom the researcher was able to obtain personal information about how these individuals work and what are their level of knowledge of Enterprise network security. The final conclusion for this section is that in Dominican Republic exists 2 types of IT administrators, the ones that work on the grand enterprises (enterprises that manage more than 1000-600 users in their network) which have high knowledge of Enterprise network security, and the ones that work on medium to small business (companies that manage 500 or less users in their network) that have low Enterprise network security knowledge. The professionals that work on the big Enterprises, in the author’s perception, are prepared for the challenges that today’s networking world presents, meanwhile the other group, which could be the majority, aren’t prepared for today’s networking challenges. The majority of the interviewed individuals were working for enterprises with 500 or less users in their network, and they sounded like they know much of security but the researcher was able to identify bad practices in them which can describe that the majority of the IT professionals in Dominican Republic, that are currently working, have bad network security practices and vices that are common when people take things lightly. Qualities found on the interviewed where: Bad network security practices, no control over other fellow IT’s, slothfulness, good theory knowledge, good practice knowledge, carelessness, don’t have disaster plans.

Of all these qualities found in the interviews, the researcher considers that it is good to add that all the people that were interviewed were working in Dominican Republic’s private sector, this means that there should be more research in the public sector, as an opinion of the researcher of this thesis, all these problems found in the private sector of the Dominican Republic’s IT workforce, it is possible to find them intensified in the public sector because of politics, cronyism and influence peddling, these are common practices in the public sector, which every citizen of the country know.

The author of this research invites any reader of this paper to do further research on the behavior of networking IT professionals, a good approach for continuing this research is to interview a wider group of IT professionals to discover more qualities that weren’t covered in this section of the thesis.
5.3- Quantitative study data collection:

See 7-Appendices.

5.4- Quantitative study data analysis:

5.4.1- Introduction:

After surveying about 50 out of 350 Dominican IT administrators, this total population refers to PUCMM graduate IT Administrators; the researcher was able to acquire a portion of the population of the IT administrators that work in the country. This survey is divided in two sections which are Network Security Best Practices and knowledge of Vulnerabilities and Attacks, in both surveys the researcher’s objective is to define if the IT administrators are capable of determining which answers are the ones that provide most security to the company they work with. With this approach, the author of this research can acquire true valuable information, as it pushes the IT administrator to really think on what is the best answer, and not to evaluate their web searching skills.

Before the statistical analysis of the responses it is very important to describe and define what type of questions the survey has, and how they can be called, after this the analysis of the responses follows. Both surveys only have 3 types of questions these questions are called by the researcher as: one answer questions, opinion questions and multiple answer questions. Each type of question is described on the next paragraphs:

5.4.1.1 - Select one answer questions:

As the name describes a select one answer question is a question that only has one answer, surveyed individuals must read the question and respond with the answer they consider is the correct. As an example of a one answer question, is the first question of the best practices for network security survey is shown, this question starts: “What do you understand by password privilege hierarchy?”, this question has three answers, only one of them is the correct answers and really demonstrates if the surveyed have knowledge about what it is asked.

   a) That common user must have less privilege than IT users.
   b) That always there should be someone, which has all the privileges that supervise the access of every user.
   c) That a type of privilege pyramid exists, on which only a few have maximum privileges, but also these don’t have totalitarian privileges.

This question answer is c, if the surveyed answers this question correctly, demonstrates that have some password related best practices.
5.4.1.2 - Opinion questions:

Opinion questions are one answer questions that ask the surveyed to read an opinion and answer with the response that best describes their opinion. As an example of opinion questions, the second question of the survey is demonstrated, this question is: “How much do you agree with this expression: ‘It is considered a good practice to have an universal password to access all network equipment’?” this question has three possible responses, each one of them demonstrates a level of security, in this example the responses say:

a) I agree, because if everyone of the department of IT knows the password it will help to work more efficiently when they find a problem.
b) I disagree, because it could be discovered very easily since all network equipment use the same password.
c) It depends, because if the password is unique and universal but it is changed every certain amount of time, then it sounds as a combination of security and efficiency.

As it is possible to see in these responses, response “a” is the one that has the least security implied, “b” is the response that has more security implied, and “c” is the one that has some security.

5.4.1.3 - Multiple answer questions:

The last type of questions that can be seen in both surveys is the multiple answer questions, which generally ask the surveyed to select which answers are the correct. As an example of multiple select questions, question number eight of the first survey is analyzed, this question says: “Could you differentiate which of the options aren’t network policies?” the responses of this question can demonstrate if the surveyed really have knowledge of the subject asked in the question, since even if the people surveyed searches on a search engine will not necessary have the real answer, or could find no answer.

a) Check if the backup was correctly done.
b) Give training to each new user about how to use the equipment that they’ll use.
c) Don’t give information of the company computer systems to people that doesn’t belong to the Business.
d) Work with honesty and commitment.

It is possible to notice that the only of the options that is not a network policy is the last one. In this case if the surveyed choose any of the other options can have 2 possibilities, a) they didn’t understand the question, or b) they don’t really recognize the answer.

5.4.1.4 - Source of responses:

As part of the introduction of this section it is appropriate to demonstrate how the researcher was able to obtain these responses, what portion of the population it was focused and the actual total quantity of responses.
In picture 1 is possible to see the email sent to the possible graduate IT administrators, in this email the researcher was able to convince the IT administrators to enter the survey website and to fill both surveys.

Picture 1: Email sent to the listed PUCMM graduates that could be IT administrators.

In picture 2 is possible to observe the list of emails given by PUCMM, these emails were used exclusively to collect responses for the surveys. The total numbers of PUCMM graduates that can fit the description of IT administrators are 350, of this quantity this research was able to collect responses from 50 individuals, and it is possible to confirm this on picture 3.

Picture 2: List obtained in PUCMM, of the possible graduate IT administrators.
After knowing how this survey works, and how the results were collected, it is now possible to analyze the statistical results of each question, to have an idea of what portion of the surveyed IT administrators recognize network security and best practices related responses. On the next section each question is discussed and the responses analyzed, in order to have a complete statistical knowledge of the level of understanding of security issues that Dominican IT administrator have.
5.4.2 - Surveys responses

In this section both survey responses will be analyzed, this will be done by creating a histogram of each question, and discussing what does mean each answers. But first it is good to have an overview of the total responses of each survey. The responses of both surveys were compiled in two tables which will be shown and explained next.

Table 2 shows the percentage of responses to the Network security best practices survey questions. Notice the percentage of people that answered the best answers of the survey, this will be important for the conclusion of this quantitative research. Question number 8 is a multiple answer question and it is better explained further down in this document.

<table>
<thead>
<tr>
<th>Survey questions</th>
<th>Best answer</th>
<th>Regular answer</th>
<th>Worst answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. 1</td>
<td>94%</td>
<td>6%</td>
<td>0%</td>
</tr>
<tr>
<td>No. 2</td>
<td>60%</td>
<td>38%</td>
<td>2%</td>
</tr>
<tr>
<td>No. 3</td>
<td>44%</td>
<td>14%</td>
<td>42%</td>
</tr>
<tr>
<td>No. 4</td>
<td>56%</td>
<td>22%</td>
<td>22%</td>
</tr>
<tr>
<td>No. 5</td>
<td>70%</td>
<td>30%</td>
<td>0%</td>
</tr>
<tr>
<td>No. 6</td>
<td>90%</td>
<td>8%</td>
<td>2%</td>
</tr>
<tr>
<td>No. 7</td>
<td>74%</td>
<td>18%</td>
<td>8%</td>
</tr>
<tr>
<td>No. 8 (multiple answers)</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

Table 2: A table depicting the Network security best practices survey results.
Table 3 shows the percentage of people that responded each question in the network vulnerability and attack survey. It is possible to notice that the first three question received a high percentage meanwhile in the last 2 questions the regular answer received the majority. Multiple answers questions like the fourth and the fifth are better described further down this document.

<table>
<thead>
<tr>
<th>Survey questions</th>
<th>Best answer</th>
<th>Regular answer</th>
<th>Worst answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. 1</td>
<td>94%</td>
<td>30%</td>
<td>12%</td>
</tr>
<tr>
<td>No. 2</td>
<td>96%</td>
<td>4%</td>
<td>0%</td>
</tr>
<tr>
<td>No. 3</td>
<td>80%</td>
<td>8%</td>
<td>12%</td>
</tr>
<tr>
<td>No. 4 (multiple answers)</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>No. 5 (multiple answers)</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>No. 6</td>
<td>20%</td>
<td>64%</td>
<td>16%</td>
</tr>
<tr>
<td>No. 7</td>
<td>30%</td>
<td>66%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Table 3: A table showing the Network vulnerability and attacks survey results.

After this overview it is good to start analyzing each question of each survey and its responses, and specifically the meaning of these responses. The first survey named Network security best practices survey will be first analyzed, afterwards the network vulnerability and attacks survey will be deeply analyzed.
5.4.3 - Network security best practices survey:

Question 1:

In this question the author of this research was able to evaluate how important is to Dominican IT’s to have an organized user access structure, this question was inspired from the interviews, since the researcher was able to notice that 2 of the interviewed people slipped that they didn’t have an organized password hierarchy, then the objective was to know if they can identify a good definition to this term.

The question goes like:

What do you understand by password privilege hierarchy?

a) That common user must have less privilege than IT users.
b) That always there should be someone, which has all the privileges, and supervises the access of every user.
c) That a type of privilege pyramid exists, on which only a few have maximum privileges, but also these don’t have totalitarian privileges.

The question results, that can be observed in picture 4, demonstrates that a 94% of the surveyed population recognize that, of the responses written in the survey, the one that defines that a privilege pyramid is what best describe an access privilege hierarchy, a 6% of the surveyed thinks that someone that have all privileges is, and 0% thinks that privilege hierarchy is described as that common users must have less privileges than IT.

<table>
<thead>
<tr>
<th>1. ¿Qué entendiste por jerarquía de privilegios?</th>
<th>Response Count</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Que los usuarios comunes deben tener menos privilegios que los de IT</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Que siempre debe de existir alguien con todos los privilegios que supervisa los accesos de los demás</td>
<td>6.0%</td>
<td>3</td>
</tr>
<tr>
<td>Que existe un tipo de pirámide de privilegios, bajo la cual solo unos pocas tienen los mayores privilegios, pero que también todos los demás no tengan privilegios totalitarios</td>
<td>94.0%</td>
<td>47</td>
</tr>
</tbody>
</table>

Picture 4: First question responses histogram of the Network security best practices survey.

It is considered a good network security practice to have an organized user access structure. It is important to notice that 47 of the 50 IT administrators surveyed recognized the answer that is more recommended. This clearly demonstrates that they understand the question, and that they know what the term means.
Question 2:

The second question results of the Network security best practices survey, which can be observed in picture 5, tries to lure the surveyed IT administrator to a bad practice as it says that:

*How much do you agree with this expression: “It is considered a good practice to have a universal password to access network equipment”?*

a) I agree, because if everyone of the department of IT knows the password it will help to work more efficiently when they find a problem.

b) I disagree, because it could be discovered very easily because all network since use the same password.

c) It depends, because if the password is unique and universal but it is changed every certain amount of time, then it sounds as a combination of security and efficiency.

This question has three answers, which for the purpose of the research have these meanings:

a) Less secure answer.

b) Most secure answer.

c) Intermediary secure answer.

A 2% of the total responses were less secure, 60% of the answers responded the most secure, and a 38% responded the medium secure answer. This can demonstrate 2 main things the first is that 30 of 50 of the IT administrators clearly identify the most secure answer, and second a 98% of the answers had some security in their answer, which affirms that this question is well understood by the surveyed IT’s, and that they also tend to choose the securer way to do their work. Even though this doesn’t demonstrate that they really use a well structured password policy in their work.

<table>
<thead>
<tr>
<th>Answer Description</th>
<th>Response Count</th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>I agree, because if everyone of the department of IT knows the password it will help to work more efficiently when they find a problem.</td>
<td>1</td>
<td>2.0%</td>
</tr>
<tr>
<td>I disagree, because it could be discovered very easily because all network since use the same password.</td>
<td>30</td>
<td>60.0%</td>
</tr>
<tr>
<td>It depends, because if the password is unique and universal but it is changed every certain amount of time, then it sounds as a combination of security and efficiency.</td>
<td>19</td>
<td>38.0%</td>
</tr>
</tbody>
</table>

Picture 5: Second question responses histogram of the Network security best practices survey.
Question 3:

The third question results of this survey, depicted in picture 6, also tries to situate the surveyed IT administrators in the position of thinking about an opinion that most suits their personal point of view. The question goes like:

*How much do you agree with this expression: “The value of the data is proportional to the size of the company”?*

a) *I disagree; because the data has the same value whether is a grand enterprise or a small company.*

b) *I agree; it’s not the same to manage the data of a small company than the data of an enterprise, because the last one handles more critical data.*

c) *It depends on the business of the company, because there are businesses that support loss of information, meanwhile others do not.*

The answers can have these meanings:

a) Network Security oriented.

b) Intermediate security oriented.

c) Non-security oriented.

This question answers were a bit close to a draw between “a” and “c”, “a” had a 44% of the responses, meanwhile “c” had a 42% which is traduced to 22 responses for “a” and 21 responses for “c”, “b” had a 14% of the answer which can be traduced to 7 responses. These results mean that there is a divided answer between the ones that clearly know the importance of data and the ones that think that the loss of information is not a threat to every company.

<table>
<thead>
<tr>
<th></th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>En desacuerdo, porque los datos para una empresa pequeña son tan importantes como para una empresa grande.</td>
<td>44.0%</td>
</tr>
<tr>
<td></td>
<td>De acuerdo, porque no es lo mismo manejar los datos de una empresa pequeña que una empresa grande, y por ende sus datos son más críticos.</td>
<td>14.0%</td>
</tr>
<tr>
<td></td>
<td>Depende del negocio de la empresa, pues hay negocios que soportan la pérdida de información, mientras que otros no.</td>
<td>42.0%</td>
</tr>
</tbody>
</table>

*answered questions: 50
skipped question: 9*

Picture 6: Third question responses histogram of the Network security best practices survey.
Question 4:

The fourth question of the Network best practices survey covers the view of the IT administrators about what is the cause of the majority of the problems of the network, this question goes as follows:

How much do you agree with this expression: “Most common networking problems come from misconfigured network equipment”?

a) It depends, because it is not possible to determine what provokes more problems, if misconfigured network equipments, non trained users, or bad network administration.

b) I agree, because the network equipments get misconfigured frequently, and this is a constant problem.

c) I disagree, because the most common reason of network problems comes from non trained users.

d) I disagree, because the most common cause of network problems comes from a bad network administration, including not applying network policies.

This question has 4 responses that for the purpose of this research have these meanings:

a) Low network knowledge answer.

b) No network knowledge answer.

c) Medium network knowledge answer.

d) High network knowledge answer.

According to the response details listed in Picture 7, a 20% of the surveyed population answered the response “a”, 2.0% answered “b”, 22% answered “c”, and 56% answered “d”, which means that 28 out of 50 surveyed individuals recognized the high network knowledge answer. According to answer “d”, surveyed Dominican IT administrators agree that the most common cause of network problems comes from a bad network administration, including not applying network security policies.

![Fourth question responses histogram](Picture 7: Fourth question responses histogram of the Network security best practices survey.)
Question 5:

This question covers proactive maintenance, the question puts the surveyed in the position of thinking what’s the opinion that most fits theirs. The question goes like:

*How much do you agree with this expression: “It is considered a good practice the proactive maintenance of the network”?*

  a) I agree, because by giving proactive maintenance it is possible to foresee and solve problems before they happen.
  b) I disagree, because I consider that the proactive maintenance is a waste of time, I prefer to solve the problems when they appear, because it is cheaper and efficient.
  c) It depends, because it is possible to do a proactive view to solve future problems and a reactive view to solve problems that happens by surprise.

For the purpose of this research the responses mean:

  a) Security oriented answer.
  b) Non-security oriented answer.
  c) Medium security answer.

An incredible 70% of the surveyed responses to this question were on option “a” which means they understood the question objectives and also knew the answer, 0% answered “b”, and a 30% answered “c”. A 70% of the total surveyed IT administrators responded “a” which demonstrated that these individuals know what a proactive maintenance means and recognize its importance as part of the good practices the IT must know. This doesn’t mean though that they really apply them in their work.

An incredible 70% of the total surveyed IT administrators responded “a” which demonstrated that these individuals know what a proactive maintenance means and recognize its importance as part of the good practices the IT must know. This doesn’t mean though that they really apply them in their work.

<table>
<thead>
<tr>
<th>5. ¿Cuántan de acuerdo está usted con la siguiente expresión: “Se considera una buena práctica el mantenimiento proactivo de la red”?</th>
<th>Response</th>
<th>Percent</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>De acuerdo, porque al dar mantenimiento proactivamente se pueden detectar y solucionar los problemas antes de que sucedan.</td>
<td>70.0%</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>En desacuerdo, porque considero que el mantenimiento proactivo no es el mejor uso del tiempo, prefiero solucionar problemas cuando aparecen pues es más barato y eficiente.</td>
<td>0.0%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Dependiendo, pues si existe una manera de tener una visión proactiva para resolver problemas futuros y una visión reactiva para los problemas que suceden de sorpresa, pues no se es perfeccionista y en la realidad las cosas no son tan fáciles. Entonces se tendrá una visión más clara para los problemas urgentes y una visión más clara para los problemas futuros. Al ser así, una manera más completa de resolver problemas.</td>
<td>30.0%</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

An incredible 70% of the total surveyed IT administrators responded “a” which demonstrated that these individuals know what a proactive maintenance means and recognize its importance as part of the good practices the IT must know. This doesn’t mean though that they really apply them in their work.

Picture 8: Fifth question responses histogram of the Network security best practices survey.
Question 6:

In this question, the disaster recovery plan practice is covered, the question goes as follows:

**What do you understand for Disaster Recovery Plan?**

a) To only make backups of all the information of the enterprise.

b) To create a list of instructions that depicts all possible forms that the enterprise could survive a disaster.

c) To install redundancy on all servers, and connections of the enterprise.

d) To not think on what is the worst that could happen, before it happens, apply it on a plan and execute it when necessary.

For the purpose of this research the meanings of these responses are:

a) Low knowledge of what is a DRP.

b) Truly knows what a DRP is.

c) Medium knowledge of what is a DRP.

d) Best response if it wouldn’t have a “no” in the beginning.

After receiving the responses of this question, which can be seen on picture 9, response “a” had a 2% of the surveyed population, response “b” had a 82% of the total responses being the majority, “c” had a 8%, and “d” had a 8% also, it is important to know that “d” is a test to know the quantity of the individuals that were really reading the survey, so what this response means is that 4 of the 50 surveyed weren’t paying full attention to the survey, but for the study it is possible to add the responses of “d” to “b”, this concludes that a 90% of the responses were correct, meaning that the IT administrators that were surveyed really know what is a Disaster Recovery Plan. Even though it is important to notify that this doesn’t mean that they get to apply a DRP on the company they work.

![Sixth question responses histogram of the Network security best practices survey.](image-url)
Question 7:

In this question the researcher was able to evaluate how the surveyed IT administrators could respond to the implementation of policies that control the IT administrator activities on the company, the answers may tempt the IT administrator to choose a bad response, specially because these answers were taken from opinions found in the Qualitative interviews. The actual question goes like:

Do you consider important the existence of policies that control the activities of the IT administrator?

a) Yes, because it is considered a good practice that the company could control in a pyramid like form, for the access and modification of the important data of the business.

b) No, I believe that the IT Admin must have all privileges, in order to solve all network problems without having any obstacles.

c) I consider that it depends on the business, because there are businesses that operate independently from the network, so network policies applied to IT become less important.

For the purpose of this research the meanings of these responses are:

a) Knows the importance of the implementation of policies in the company network.

b) Could know the importance of policies but sees them as an obstacle.

c) Doesn’t care about implementation of network policies.

After observing the responses on picture 10, it is possible to see that a 74% of the surveyed colleagues responded the correct answer which is “a”, an 18% responded “b”, and the last 8% responded “c”. It seems that 74% of these individuals know the importance of policies that control every user of the network including IT’s.

<table>
<thead>
<tr>
<th>Response</th>
<th>Responses</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Yes, because it is considered a good practice that the company could control in a pyramid like form, for the access and modification of the important data of the business.</td>
<td>37</td>
<td>74.4%</td>
</tr>
<tr>
<td>b) No, I believe that the IT Admin must have all privileges, in order to solve all network problems without having any obstacles.</td>
<td>5</td>
<td>10.2%</td>
</tr>
<tr>
<td>c) I consider that it depends on the business, because there are businesses that operate independently from the network, so network policies applied to IT become less important.</td>
<td>4</td>
<td>8.0%</td>
</tr>
</tbody>
</table>

Picture 10: Seventh question responses histogram of the Network security best practices survey.
Question 8:

In this question the author of this research wanted to evaluate if the IT administrators really know how to differentiate which of the responses aren’t network policies, the question goes like:

*Could you differentiate which of the options aren’t network policies?*

  a) Check if the backup was correctly done.
  b) Give training to each new user about how to use the equipment that they’ll use.
  c) Don’t give information of the company computer systems to people that doesn’t belong to the Business.
  d) Work with honesty and commitment.

It is possible to notice that all of the answers except option “d” can be considered network policies. This means that there was only one answer, but the objective was to know if the surveyed IT administrators consider as network policies the ones that are applied to network users. The results can be observed in picture 11, the responses for the questions were: 7 IT administrators considered that “a” is not a network policy, 14 considered that “b” isn’t a network policy, 11 thought that “c” is not a network policy, and the majority, 38 decided that “d” is not a network policy. The graph on picture 8 may confuse a little, but the information is clear, the colleagues that responded “b” and “c” didn’t consider user oriented network policies as network policies themselves. This can lead to think that IT administrators in the country don’t consider users as part of the network.

<table>
<thead>
<tr>
<th></th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revisar si el backup se realizó correctamente.</td>
<td>14.0%</td>
<td>7</td>
</tr>
<tr>
<td>A cada nuevo usuario decirle un entrenamiento sobre cómo manejar el ordenador que utiliza.</td>
<td>29.0%</td>
<td>14</td>
</tr>
<tr>
<td>No brindar información de los sistemas a personas que no pertenezcan a la empresa.</td>
<td>22.0%</td>
<td>11</td>
</tr>
<tr>
<td>Trabajar con honradez y empeño.</td>
<td>76.0%</td>
<td>38</td>
</tr>
</tbody>
</table>

Answered questions: 56
Skipped questions: 6

Picture 11: Eighth question responses histogram of the Network security best practices survey.
5.4.4 - Network vulnerability and attacks survey:

Question 1:

In this question the author tries to see which quantity of the surveyed IT administrators have some knowledge of what is cross-site scripting, and the threat that it imposes to the company they work. This question goes like:

How much do you agree with this expression: “Cross-site scripting attack happens with more frequency on websites that manage money”?

a) I agree, because this type of attack it’s focused on website vulnerabilities, and it happens with more frequency on websites that permits the user to manage credit cards and bank accounts.
b) I disagree, because this attack doesn’t occur with much frequency on those websites, because they have enough security.
c) It depends, because it is not necessarily used to obtain money, the attacker may have many different objective, since the principal objective is to trick the website user and to obtain any information that it is inserted on it.

For the purpose of this research this question answers have this meaning:

a) Doesn’t know the real purpose of cross-site scripting.
b) Reckless answer.
c) Knows the real purpose of cross-site scripting.

After observing the responses on picture 12, it is possible to see that: 15 of the 50 surveyed individuals responded that “a” was the correct answer, meaning that a 30% of the total population believed that this was the right answer, 6 of the 50 people surveyed responded that answer “b” was the correct answer, this means that a 12% of the 50 surveyed IT’s believed that these attacks aren’t so frequent on these websites, 29 of the 50 surveyed IT professionals thought that “c” was the answer, leading the percentage by achieving a 58% of the total population sample, this mean that 58% of the surveyed individuals know the real purpose of the cross-site scripting attack.
Question 2:

In this question the researcher was able to evaluate the knowledge that the surveyed individuals have of the infamous Denial of Service attack. This was done with a simple question:

What it is known as a Denial of Service Attack or DoS?

a) It is a group of computers that combine themselves to send virus and spam.
b) It is an OS made by Microsoft.
c) It is known as DoS to an attack made by one or more computers to a specific target computer, with the objective of squandering all its resources, so it wouldn’t keep delivering its service.

For the purpose of this research the answers of this question have this meaning:

a) Confused the term with Zombie computers.
b) Doesn’t know at all what a DoS is.
c) Have knowledge of the term.

After viewing the responses on picture 13, is possible to notice that: 2 of the 50 surveyed professionals responded “a”, which means that a 4.0% of the total population confused the term with zombie computers, none of the surveyed individuals responded “b”, meaning that a 0% believed that DoS is a OS from Microsoft, 48 out of 50 of the surveyed professionals responded that “c” was the correct answer, meaning that a 96% of the total surveyed population knew what a Denial of Service attack really is.
Question 3:

In this question the researcher was able to lure the surveyed professionals to think that installing a good antivirus on all the equipment of the network will do to eliminate completely all malware from it. The objective is to know if the surveyed population really knows that malware is a big problem that cannot be eliminated completely, but instead, it can be reduced, with other good practices that include: network user training, software maintenance and the implementation of network security policies, all these including an antivirus and if possible a good firewall, are the recommended measures to be taken in order to diminish malware in a network maintaining it secure and healthy. This question goes like:

*How much do you agree with this expression: “It is possible to completely eliminate all malware existent in the network with a good antivirus”?*

a) *I agree, because by having an antivirus that is from a recognized brand, that has a proper support, and that the IT administrators maintain them with the latest update installed it is possible to eliminate all malware threats that could affect the network.*

b) *I disagree, because for diminishing malware in the enterprise a quantity of measures must be taken, these measures includes a good antivirus, network software maintenance and the implementation of network security policies.*

c) *I disagree, because malware is very difficult to eliminate, there is always a virus in the servers, there is always a curious user that breaks the rules without one noticing it.*
For the purpose of this research, the answers of this question can have this meaning:

a) If the surveyed professionals selected option “a”, it means that this person doesn’t know much about how hard it is to eliminate malware completely, or at least they are very confident of the antivirus technology.

b) If the surveyed professionals selected option “b”, it means that they truly know what it takes to help diminish malware in an enterprise network.

c) If the surveyed professionals selected option “c”, it means that they are truly disorganized and that they aren’t really network security focused, but they know that only with an antivirus is hard to achieve the total removal of malware.

After revising the responses on picture 14, it is possible to see that: 6 out of 50 selected option “a”, meaning that a 12% of the total population where confident that antivirus technology is enough to eradicate all malware from a network, 40 out of 50 people responded “b”, meaning that an 80% of the total surveyed professionals knew that not only with an antivirus is needed to reduce malware to a low level, 4 out of 50 people responded “c”, meaning that an 8% thought that only with an antivirus is not enough, but it is very hard to achieve because of the lack of organization.

<table>
<thead>
<tr>
<th>Response</th>
<th>Percent</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>12.0%</td>
<td>6</td>
</tr>
<tr>
<td>b)</td>
<td>80.0%</td>
<td>40</td>
</tr>
<tr>
<td>c)</td>
<td>8.0%</td>
<td>4</td>
</tr>
</tbody>
</table>

Picture 14: Third question responses histogram of the Network vulnerability and attacks survey.
Question 4:

In question 4, this research author wanted to evaluate if the surveyed professionals could differentiate which of the answers didn’t have any relationship with the definition of Phishing. The question goes like:

Select the options that don’t have any relationship with the definition of phishing:

a) It is a technique for gathering information from the computer.
b) Apply redundancy in all connections and network terminals.
c) A branch of social engineering
d) A type of vulnerability that permits a malicious attacker to inject a script, provided by his own domain, to a website that is open to the public.
e) It is called phishing to e-mails sent with the objective of obtaining critical information by tricking, scamming or exploiting a vulnerability of the system.

In picture 15 is possible to observe how the surveyed population responded the different questions. It is possible to notice that:

a) Option “a” was selected 15 times, which means that a 30% of the surveyed professionals considered that phishing is not a technique for gathering information from the computer, which is false since phishing really tries to obtain information whether tricking the user in front of the PC or exploiting a vulnerability on the computer.
b) Option “b” was selected 40 times being the most selected option, this is not related at all to phishing, but 10 of the surveyed individuals or a 20% of the total considered it to be related to it.
c) Option “c” was selected by 20 people, meaning that a 40% believed that phishing isn’t part of social engineering.
d) Option “d” was selected 17 times, this is the definition of cross-site scripting, and this means that a 34% of the total confused phishing with cross-site scripting.
e) Option “e” was selected 8 times, which means that the 8 people who selected this didn’t know the true objective of phishing or they misunderstood the question.

<table>
<thead>
<tr>
<th>1. ¿Seleccionar las opciones que no tengan relación con la definición de phishing?</th>
<th>Response Count</th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Una técnica de sacarle información al equipo</td>
<td>15</td>
<td>30.0%</td>
</tr>
<tr>
<td>Aplicar redundancia en todas las conexiones y terminales de la red</td>
<td>40</td>
<td>80.0%</td>
</tr>
<tr>
<td>Una rama de la ingeniería social</td>
<td>20</td>
<td>40.0%</td>
</tr>
<tr>
<td>Tipo de vulnerabilidad que permite a un atacador malicioso inyectar un script proporcionado por su equipo a una página web vista por el público</td>
<td>17</td>
<td>34.0%</td>
</tr>
<tr>
<td>Se llama phishing a e-mails enviados con el objeto de obtener información crítica yendo mediante engaños o explotando una vulnerabilidad del sistema</td>
<td>8</td>
<td>16.0%</td>
</tr>
</tbody>
</table>

Answered questions: 50
Skipped questions: 0

Picture 15: Fourth question responses histogram of the Network vulnerability and attacks survey.
Question 5:

In this question, the research author was able to evaluate if the surveyed IT professionals can identify reasons why malware enters the enterprise network. The question and its option answers are:

Select the possible reasons why malware enters to the data network of the business:

a) Outdated Antivirus and Operative Systems.
b) Good network policies.
c) Banning the users to install any software on the network.
d) No control over the user’s removable devices.
e) Bad implementation of network security policies.

The survey responses can be observed in picture 16, is possible to see that: answer “a” was selected by 45 out of the 50 surveyed professionals, this means that a 90% considered that outdated antivirus and operative systems is a reason why malware invades the network, none considered that “b” was a good answer, which was correct, 1 person answered that “c” was a reason, 48 people out of 50 selected “d”, this means that 96% of the total population considered that no control over the user’s removable devices is a cause of malware entering the company, which is true, because users can use these removable devices for personal use, increasing the chances that malware infects it and finally enters the company’s network when the user use it on a company PC, continuing with the responses 47 out of 50 surveyed individuals thought that bad implementation of network security policies is also a reason for malware to invade the company’s network, meaning that a 94% of the total was very clear in that this is a correct answer.

<table>
<thead>
<tr>
<th>Reason</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outdated Antivirus and Operative Systems.</td>
<td>90.0%</td>
<td>45</td>
</tr>
<tr>
<td>Good network policies.</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Banning the users to install any software on the network</td>
<td>2.0%</td>
<td>1</td>
</tr>
<tr>
<td>No control over the user’s removable devices</td>
<td>96.0%</td>
<td>48</td>
</tr>
<tr>
<td>Bad implementation of network security policies</td>
<td>94.0%</td>
<td>47</td>
</tr>
</tbody>
</table>

Picture 16: Fifth question responses histogram of the Network vulnerability and attacks survey.
Question 6:

In question 6 the author of this research was able to evaluate if they can recognize a possible reason why people are generally tricked by phishing, the question in English goes like:

*Why are common people generally tricked by phishing?*

a) Because users don’t know it exists.
b) Because scammers use very effective methods to trick the victim.
c) Because the user doesn’t know that is a scam.

The responses of this question can be seen in picture 17, the distribution of the answers are: 8 out of 50 people surveyed responded that “a” was the answer, meaning that 16% of the total population believes that the cause is because users doesn’t know phishing exists, 10 out of 50 professionals believe that “b” is the correct answer, this means that a 20% of the surveyed individuals thought that it is because scammers user very effective methods to trick the victims, and 32 out of 50 professionals selected “c” as the answer, meaning that they believe that the main cause is that the user generally doesn’t know that it is a scam, this was the most selected answer with a 64% of the total answers. The result of this question is that the professionals believed that it is because the user doesn’t know that is a scam, but the real true answer is that the scammers are becoming everyday more creative with the phishing scams, which means that the true answer is “b”, the cause is that scamming is becoming a business, and as a business, it gets better everyday, because getting better makes you gain more profits. So the reason why users doesn’t know that it is a scam is because the scammers are becoming better and better everyday. This means that only a 20% of the total surveyees were able to recognize that the real answer was “b”.

Picture 17: Sixth question responses histogram of the Network vulnerability and attacks survey.
Question 7:

In this question the author of this research was able to evaluate if the surveyed professionals consider a Distributed Denial of Service attack as a risk for the networks of Dominican Republic Enterprises. The question goes like:

Do you consider a Distributed Denial of Service attack (or DDoS) a risk for the enterprise networks of Dominican Republic? Why?

a) Yes, because technology is no longer a mystery and anyone can pay hackers to do a DDoS attack to a certain company server, with the objective of removing it from the market.

b) No, it is not a risk for our country because we have never seen an attack like these on our country, and I consider that here there aren’t hackers with the enough level of knowledge to create an attack of such magnitude.

c) It depends on the business that the company has, and how necessary is its online presence, because is possible that they don’t need any presence on the web.

It is good to know that these three possible answers were obtained from the qualitative section interviews, and then the objective is to verify the distribution of what the surveyed population believes about this subject.

The surveyed Network administrators that selected “a” can represent the professionals that know that networks are vulnerable to this attack and so are professionals that have security in mind.

The surveyed professionals that selected “b” as their answer can represent the amount of professionals that are careless about security issues, and specifically this attack.

The surveyed IT administrators that selected “c” as their answer can represent the quantity of IT’s that know the amount of business in Dominican Republic that doesn’t need online presence, and that also know that the risks of an attack increase when the importance of the business online presence is high. This means that these individuals know about network security and about the enterprises situation in the country.

After analyzing the results of this question on picture 18, the researcher was able to notice that: 15 out of 50 of the surveyed selected “a” as their answer, meaning that a 30% of the total surveyed population have security in mind, 2 out of 50 surveyed IT’s selected “b” as their answer, this means that a 4% of the sample population are careless in security measures, and 33 out of 50 selected “c” as their answer, showing that a 66% of the sample population know about network security and the enterprises situation in the country.
Conclusions:

After the analysis of the survey questions, the author of this research was able to obtain information about the population’s behavior towards questions about networking best network practices principles, and also was able to determine if this sample was or not prepared to deal with the security challenges of today’s networks, with the questions of the second survey which was related to network vulnerabilities and attacks. This section of the research was able to complement the qualitative section by giving a wider knowledge of the population behavior. With the information obtained from both surveys the author created a theory about the level of knowledge that the IT administrators in the Dominican Republic have. Taking under consideration the behavior of the surveyed individuals on the first survey “Network security best practices”, it is possible to notice that on each question the surveyed were able to respond the correct answers, this survey can demonstrate mainly that the sample population of Dominican IT administrators are well versed in the theory of networks and network security, this means that they can see the difference whether an answer is more secure than another. Now analyzing the behavior of the surveyed individuals on the second survey demonstrated that these individuals where able to differentiate the answers that were the most secure for the network’s health and to avoid any type of vulnerability.

So in conclusion Network administrators in the Dominican Republic have theoretical knowledge about the best practices to maintain a network secure and also know about network vulnerability and attacks. It is important to know that this doesn’t mean that they do apply this knowledge in their work though.
5.5- Mixed Methods Conclusion:

In this part the author takes the most important things learned from both studies to create a theory based on both studies conclusions, the objective is to complement each study with both qualities found in the qualitative study, and the statistical sample view of the quantitative study.

Dominican IT administrators according to the quantitative study know about security problems and what are the best practices to help maintain a network safe from attacks or at least to diminish them, but according to the qualitative study, Dominican IT administrators can be careless and take things lightly when it comes to apply the knowledge they have about network security and the like to the network of the enterprise that they work, except for the enterprises that have strong network security policies, which is the case of the large enterprises of the country used in the research.

Lessons learned in this document:

This study included very valuable information about the tendencies of the network security practices that the Information Technology professionals of the Dominican Republic have. It is important to describe that the human factor in the network is the weakest link in the network chain, since humans can fall for old con jobs. So what it is important to notice that as part of the possible solution of the problem described in this whole document not only the network administrators are responsible for the security of the network, but also the enterprise administration, and the end users. It really depends on the interests of the enterprise administration to focus their efforts on the security of the data, if they don’t believe that data must be maintained safe then how their employees (including the network administrators) can think or work based with network security in mind.

The lessons learned, in the enterprise administration point of view, are that they need to care more about the security of their data assets and also to start considering the implementation of network security policies as the solution to the network security problems that they confront. Network security policies not only are the ones that are implemented on the equipment of the network, but also the policies that affects all users including the network administrators, an example to this can be to give each user, on a weekly or monthly basis, a small training about how to avoid practices that creates vulnerabilities to the network, this includes the network administrators because they are users, and more important, humans, that can make mistakes that could affect the enterprise network negatively. This training will not completely eliminate all the possible security threats that affect the network but they will surely be diminished. Even the enterprise administrators need to receive this training on how to learn to avoid security threats when using computers in the company.

Lessons learned in this document, in the network administrator’s point of view is that it is important to do an auto evaluation and verify which practices are good for the enterprise network security and which aren’t, with this exercise network administrators can identify the bad network security practices and avoid doing them, and they will further implement the practices that are good for the enterprise network and so this will not only help the enterprise but also will help professionals to advance further in their career by becoming better prepared to confront the next generation of network security problems.
Lessons learned in this document, in the end user’s point of view is that end users aren’t the only source of network security problems and that it is important to them to have motivation to help as much as they can to secure the company’s information, this can be done as simple as avoiding scams, viruses and using social networks websites on the enterprise.

It is important to notice that, according to the qualitative research conclusions, the IT administrators that work on the smaller companies of the country can be a weak link in the network chain, meanwhile the ones that work on the bigger enterprises are a strong link in the network chain. This happens because the latter ones work in enterprises that have implemented strong network security measures, and also they give them constant training.

It is important for global companies that plan to start a division in the Dominican Republic to know about the results of this paper, since it can clearly help them reduce costs by knowing beforehand what they need to do to assure the network security of their enterprise data assets.

Meanwhile for higher education in the Dominican Republic the results of this research means that theoretically our IT administrators are really well versed, but they lack the organizational skills they need to really implement a serious schedule of good network security practices, higher education institutions should focus more on teaching these professionals what they need to do to keep a network safe from outsiders and from themselves.

**Future research**

Future research should be done in the Dominican Republic in the form of a wider research, this means by interviewing and surveying a wider quantity of individuals, to get better results, also this research couldn’t interview many of the IT administrators of the grand enterprises of the country, this means that there should be enough material to create a full research only based on these enterprises. It should be interesting to confirm if the Dominican IT administrators, which work in the grand enterprises, really have good practices. It would be a good subject to notice if these grand enterprises really are as secure as they look.

This research should be replicated in each country, since it is important to know if the practices of the IT professionals are truly good for the enterprises they work for. This would create a baseline of knowledge that could really help to get a better understanding on how are the network administrators practices in the world, and also it creates consciousness to the people and enterprises that get to read these documents, helping them to be aware of the security problems that the digital world represents to the interests of the enterprises, contributing this way to create securer networks. The author of this research invites everyone that reads this document to do further research on this area, not only on the Dominican Republic but to each country of the world.
Author’s last comment

For people that wish to do research on this topic, a good counsel, if the methodology selected includes qualitative methodology, is to try to make the interviewed comfortable, try it to not be a questionnaire, change it into a conversation type interview, the best results are obtained when the interviewed starts talking honestly and doesn’t feel like if taking some sort of an oral exam. In case that it includes a quantitative research methodology, when creating the quantitative instrument, try to not evaluate the surveyed individual’s web searching skills, because your objective is to learn something about the surveyed and not to learn something that is already written on the internet.
6- Appendices A:

6.1- Qualitative study Data Collection section:

In this section all 6 interviews, upon which the qualitative study was done, are displayed. All interviews were done to enterprise network administrators that manage more than 500 employees in their enterprise. For ethical purposes the identities of the IT administrator and the enterprise are not displayed, since some internal information of their enterprises may be exposed.

6.1.1- Interview number one:

1. What facts you consider to be important when deciding that a program or website is trusted enough to be used in the enterprise?

In my point of view, if it is a program that the company will use, it involves security risks for the company, so I would recommend it to be a desktop program, and not as a website. Website’s security is very difficult to manage, not only because of the threats that come from the WAN, but also the high risks found on the LAN. If we were to include a financial application or an administrative application in the enterprise, would not trust it to be web, however, I would recommend Intranet. For example if we have different branches, you can implement a high-security administrative intranet.

2. For you, what is the importance of company data assets?

They are very important, some companies invest heavily in data backups, for example imagine a telecommunication service provider enterprise, a lot of data is manipulated every moment, therefore, it must have high security policies. As an example of the mistake of not having a good data security policy we can speak of the local aqueduct that was flooded and all their equipment was damaged, and thus, all their data was lost. In other words data is the most important asset in any enterprise in order to assure business continuity. There are companies that can be handled as a grocery store, but there are other companies that are striving to maintain their datacenter online in order to keep their data safe.

3. In your words, what must be done to diminish malware?

This starts from the company’s internal users, you can put policies that restricts all possible damaging user’s actions, but there is always a curious one that learns how to overcome security, there is always a virus on the servers that you do not know where it came from, and we made policies to reduce the entry of these problems, but in time they are no longer applied. We have a plan that is currently in its baby state, with the objective of reducing all possible malware
infection to its minimum, the plan consists of installing Linux OS on all machines, so we are making an effort to let all users learn how to use Linux with the intention of that when the change is done, the new users will have the idea on what it is going to be handled. Sometimes we from the IT department often make mistakes that can cause the entry of a backdoor or other malware. We know we should be careful but as human beings we make mistakes, or simply do not realize because of another problem we are having on mind and do not take into consideration that this will happen. There are policies within the same Windows servers OS, which makes it easier to include security in a place without having to travel to that place, on the same servers are registered and these are spread policies that are applied to all teams, but as I said above is difficult. The only way to decrease the malware is adding security standards without affecting the user's work. User education on which are the best practices for maintaining safe procedures in the network, is one of the most important things, because when human values are involved in something these are tend to develop problems and mistakes, and this goes not only for the common user but also involves the technology team.

4. What do you think is the difference between spyware and virus?

To my understanding spyware are viruses too, in my opinion it fits the definition of a virus, but spyware, as the name says, is software that serves someone to obtain data and information of your company, and viruses is something that damages your files. There are different types of viruses that will harm your company.

5. What practices you consider that you can do, to help secure the enterprise data assets?

The first practice I consider to be important is a backup policy, another good practice I think is most important is to have a backup outside of the company building, therefore we have a local server that keeps the company data safe but also a second server with the same data as the main one, so in case something happens to the main server the backup enters in function and maintains data availability. There are companies that can afford to have their server’s offline but there are others that cannot. For example, if the main server’s hard disk gets damaged, what could you do, try to retrieve the data?, if the company doesn’t has a department of data recovery or forensics, would have to contract an external firm to recover the information and this can be a risk since the data is being managed by externals, because we do not really know if the data is treated 100% confidentially. It really depends on the company, for example for this company data is not that important, but for the competition it is very important. There are more practices that help protect data assets that I don’t remember now.

6. In your opinion, what is the importance of maintenance in network security?

When speaking of maintenance, as of the windows OS having it as an example, Microsoft forces you to perform maintenance with money involved, I do not speak of the weekly updates that we
often do, but of the complete system upgrades that must be purchased, so the company does not see it feasible. That is the reason why the company considers installing Linux on all computers, because when the company needs to change the operating system it only needs to install it without any cost involved for the company. But we know that these changes are very risky also, so the IT department really should test the OS working with all the company’s system, before migrating to it, to see if it doesn’t damages a system. We do maintain computer systems actualized with the latest version possible.

7. What do you think about social engineering? Is it an issue for the network security?

Of course it is; social engineering is one of the biggest problems that affect enterprises. These are people who are dedicated to get information from you, via telephone, via web, via email. For example an email that says you won EUR 700,000, but to claim it, you need to give the account number for deposit, but you do not know if it is a trick to get money. The user have to recognize which websites are safe and which aren’t, in order to use his credit card, for example I have had no problems using credit card in the web, because I login to websites with prestige that assure me that the procedure is safe.

8. Do you consider that to have a disaster recovery plan is important for the enterprise? Why?

Ochoa hardware 10 years ago had a disaster and they hadn’t a disaster recovery plan, the same as here, we do not have one, resulting in a serious risk for the company’s data. If this datacenter burns, a lot of work and effort must be done to return to the point that was before the disaster. The money of an enterprise is in its data, and the absence of a contingency plan creates the risk of losing it all to the first disaster that occurs, having serious loss of economic resources as well of time spent on repairing the damage done by the disaster.

9. When speaking about passwords, what is your strategy for maintaining it secure?

Password management gets much easier when you use windows server, because in this OS you can build profiles with policies that force users to change passwords every so often. If you don’t have a secure password policy, anyone from outside could enter and damage your data, as well as people from the inside. We have a password here that everyone knows, and we don’t know why we haven’t had any problems with it, this means that no one has ever done any damage to the servers that use this password, but we know that is a risk. An example could be when an IT engineer gets fired; it’s a big problem, because all passwords must be changed in order to keep servers safe to avoid the possibility that he could damage the enterprise data.
10. Do you believe that a company needs to apply network security policies? If so, why?

I believe that it is mandatory to apply network security policies, unless it is a grocery store and still minor security must be placed, network security policies must be the main priority, if the company believes that its data is valuable. Policies begin from the entrance door; it is not possible to let everyone enter where the datacenter is located. Even if you already have a standard procedure to notice that someone entered without permission to the network, network policies must prohibit user’s access to places that they shouldn’t be accessing.

6.1.2- Interview number two:

1. What facts you consider to be important when deciding that a program or website is trusted enough to be used in the enterprise?

First, are the vulnerability points that the system has, at which point of the network the program or website will be implemented. As an example it can be implemented with a public IP directly or bring a password or with an own DNS or another DNS, all this have a security factor. The position where it will be implemented, the vulnerabilities it has and how modular it is this to properly identify the possible problems that can occur. Open Source software are very modular, this means that adding security to it, in case it doesn’t have any, can be done easily by searching on the internet and add a security plug-in or any add-on that adhere SSL.

2. For you, what is the importance of company data assets?

For me as a network engineer data is not that important. As an example, I am focused more on that the data gets to its destination. For example, for me what is important is that all enterprise programs that use the database connects correctly to it, that the reader doesn’t time out, if someone asks for a query that it respond fast, data for my job is not that important, but for the maintenance department they are, this because they do backup and all that sort of things. But I focus more on the transport of the data and its availability instead of its maintenance itself.

3. In your words, what must be done to diminish malware?

The malware exist because there are interesting things, secrets that everybody has, that people who develop malware wants to know. For example, bank data. There also exist teams of malicious programmers who make their profits from the competition that exists between businesses and the desire to know what is the competition doing right now, even having objectives as malicious as to damaging their computer or network.
4. What do you think is the difference between spyware and virus?

Viruses are generally made to multiply themselves, spread themselves between different machines to its payload and re-replicate. Spyware doesn’t function like viruses, since spyware are only grieving to gather information and send them to its developer, meanwhile viruses normally have a damaging payload and keep replicating themselves. All spyware are virus but not every virus is a spyware. Spyware objectives are primarily to collect some information and send them as possible, and spyware are viruses because they replicate and everything that lives only to replicate is a virus.

5. What practices you consider that you can do, to help secure the enterprise data assets?

This question refers broadly to hardware security and software security, because for protection it is important for you to assure the security of the hardware equipments, this means the servers, hard drives, network cables, and as well it is important to ensure the security of the software used, this means that the use of it in the servers won’t compromise the Enterprise data. In order to assure security standards the enterprise must use secure software, this software must have a good data encryption that is very difficult to break. These programs should be certified by the company that develop or sells them. Especially, if the company uses Open Source software they need to assure that it comes from a recognized community, so that you can assure that malware developers aren’t inserting malicious codes to the software. Software from a community that provides good documentation and makes updates in case of vulnerability is discovered. When speaking about user level, that the users that have access to the data be responsible and cares to keep the data confidential. Also at the software level, that the user has a secure access, protected by a strong password, using a system such as Active Directory, Open LDAP, so that users could be authenticated to use the data, but the IT administrator knows who is using what data, and when is using it. At the network level, the use of LAN and VPN is recommended.

At hardware level, I recommend to use hard disks redundancy (or RAID) and as well as server redundancy in other locations, so in case of server failure or that something happens to the branch location then the data will still be stored on the other site’s server, this means that the data will not be lost. Other good practices are, to have a password changing policy that changes user’s passwords periodically, to have defined maintenance policies, with this I refer to backup and periodically planned software updates.
6. In your opinion, what is the importance of maintenance in network security?

Well, mainly, before maintenance, monitoring the network goes first, to have knowledge about the network’s health. After this, comes maintenance, which is very important, because they are the ones that let you do a full check of the enterprise network, for example, and then make appropriate changes to the network so that it remains active, by fixing all the errors that appear in a prudent time. The importance of doing maintenance has to do with the time of use of the equipment, for example, backups are done weekly, monthly physical prove of the network cables, verify each two weeks the software on each computer, and like I said above to revise the servers for inactive users, their passwords and its logins. Many policies can be implemented in order to give different types of maintenance.

7. What do you think about social engineering? Is it an issue for the network security?

Well, social engineering is very dangerous, because people psychology is difficult to know, since each person is different from the others, it doesn’t exist a standard of people, even though there are people alike, but it doesn’t exist a homogeneous type of people. You cannot tell when a person can give information easily even though they can be educated, it still isn’t certain that it couldn’t give away information to someone by mistake, innocently. It is a problem because many people may be aware of what a network has, for example if I use ports that are different from the default ones, for security purposes, from outside we have a firewall so that not everyone could access what is inside, for example, for the SSH port I use a different port, there are people that use them from their homes, and a friend or an acquaintance’s in a moment of distraction gets to use the computer and opens the Putty program that keeps the port configuration, and gets to access the server.

That’s why your closest friend could be your worst enemy, because you have confidence in him, but it’s important to have some distance because you don’t know if maybe someone offers him some money for getting information of the company, everybody has their price.

8. Do you consider that to have a disaster recovery plan is important for the enterprise? If yes, why?

Yes, because disasters make enterprises lose a lot of time and vital information to the company. Not only that, but also loss of money. But here we are talking about disaster recovery, because even if you have a backup the company still loses money. Now more money is lost if the company does not have a backup. It is always important to have a disaster plan, but it depends on the site where the company is located, and to plan what to do in case a disaster takes place. For example, our company is established in a tropical island where hurricanes, seaquakes and earthquakes happen frequently. There are other places that are subject to volcanoes,
tornadoes, and forest fires. I believe that all companies should have a disaster recovery plan; at least they must take it into consideration and especially for servers that are critical for the business to keep working, and it should be focused on minimizing costs in the event of a disaster. I also think that making a disaster plan is easy because there are facilities for data, since data can be uploaded to websites, data web house, it's easy and inexpensive.

9. When speaking about passwords, what is your strategy for maintaining it secure?

In this company we use randomly generated passwords that changes each 5 minutes, this is done with a key that we use them for each labor that needs authentication, I consider that this is the best way to maintain a safe password, because we don’t have to remember the passwords and also we don’t need to change them since they are changed automatically on the authentication key and the system, so in conclusion to access anyplace in the enterprise you need an access key, but to login on a computer we also use them. I consider being a good strategy to use different passwords for each server, and to use the key I mentioned above to generate random passwords each X minutes.

10. Do you believe that a company needs to apply network security policies? If so, why?

Yes, because networks are vulnerable and on the networks rest the traffic or the movement of data from one site to another between users and servers, between servers and servers and is very important that the traffic always gets to its destination with minimum corruption, is important that the data is always there so the enterprise could access it easily when they need. Policies are especially set up to monitor the users, for example that they don’t decide password but we give them a secure one, use of certification, that for them the connection via VPN to the enterprise is only available in work hours. We don’t have in our company a defined policy for IT managers, but if one is fired what we do is to temporarily disable his account and since passwords are randomly generated each 10 minutes, it changes automatically and that’s why they are difficult to determine for everyone that doesn’t have the password generator.
6.1.3- Interview number three:

1. What facts you consider to be important when deciding that a program or website is trusted enough to be used in the enterprise?

The first thing to have under consideration are the needs that the enterprise have, because is useless to have a program with some functionalities that won’t be used, and that could be used to harm the enterprise, since it won’t be revised for the possible vulnerabilities that the program could generate then the program becomes a risk for the security of the network. When you have a program developed exactly for the company needs, it is good to review the level of security on which it manages data, this means how much it protects the data, how much it manipulates it, if it creates backups, or if it encrypts the data.

2. For you, what is the importance of company data assets?

For most businesses it is vital, in the case of the company I work for, if a data leakage happens, the competition could know what we will do in terms of the launch of services, how we process certain things or save money in another, this means that in our business it is very important data security. In summary I consider it the most valuable thing a company could have. That would make the soft drink companies if their secret formulas are known or search engines business (the Internet) if their search algorithm gets public.

3. In your words, what must be done to diminish malware?

Malware is very hard to control, because they are small applications, techniques are developed to identify the patterns or behavior of these, but it is not something that eliminates all of them, I believe that the best we can do is to educate the user, so they would not be navigating on websites that are not supposed to navigate. Education gives the employee a wider knowledge, at least to identify when a friend is sending him a virus and to avoid getting the pc infected for it.

4. What do you think is the difference between spyware and virus?

Well, the difference between these two is that spyware usually gather information of the host, meanwhile the virus could change the operative system registry in order to cause damage and replicates itself, I mean the term virus is somewhat a wider term, we could say that a spyware is a virus that gathers data of its host.
5. What practices you consider that you can do, to help secure the enterprise data assets?

The first practice is to educate the user, it is the most important because is useless to have the best antivirus of the world if the user is constantly doing activities that are harmful to the network.

To monitor network activities from time to time, to detect possible worm infections.

To have an antivirus as a preventive measure, not as the most important one, because there exist an amount of time between the development of a virus and the development of the counterpart of the virus, add to this also the time that the actualization of the antivirus gets installed in the equipment that has the virus, this results in a period of vulnerability to the network.

6. In your opinion, what is the importance of maintenance in network security?

It’s quite important, because in maintenance firmware updates are included, to revise the network lines, you have a free socket and suddenly there is someone connected, that Cisco developed a new firmware that needs to be installed as soon as possible because it was a solution for a vulnerability they found. So maintenance is part of the evolution of systems, but if you don’t do them, then you won’t have the benefits of the new improvements to security and ease of use that updates give. So in conclusion it is a vital part, if there is no maintenance there will never be improvements in the network system.

7. What do you think about social engineering? Is it an issue for the network security?

Yes, it is problematic, because it allows foreign people to gather confidential Enterprise information, an example could be that in the Enterprise where I work, a friend of mine takes my ID card and dresses himself with the company uniform and sneak in the datacenter, no one would say anything since a lot of people enters the place frequently, since there are so many contractors and consultants, he could sit on a PC and say that he is a contractor, and grab the information he wants and then leave. Or he could say that he works on floor X and that he needs the information Y to finish his job with the datacenter, this is very dangerous and it’s all done tricking people. One of the first hackers that existed, to maintain himself as the best hacker around, what he did was that he befriended with all the technicians that were working on certain technology that was going to come out in certain date, then this way he learned about the technical details that the technology possessed before it could come out, then when the technology came out to the market he was aware of all its vulnerabilities, as well as its benefits and much other things.
8. Do you consider that to have a disaster recovery plan is important for the enterprise? If yes, why? If no, why?

Yes, absolutely, because of the well known Murphy law that says “If something can go wrong it will go wrong”, we are humans; this means that we aren’t perfect, failure will always occur. The solution is always to foresee what could happen, see the possible consequence that each action will generate. An example is the backup, people tend to think of the importance of the backup exactly when a problem has occurred, but when there isn’t any problem they tend to believe that backup is a worthless occupied disk space.

9. When speaking about passwords, what is your strategy for maintaining it secure?

I believe that is good to have a strong password regime that forces the user to change passwords every month, a regime that does not permit users to use the first 5 previous used passwords, with the intention that the user will have to vary his everyday routine, making the network safer.

10. Do you believe that a company needs to apply network security policies? If so, why?

Yes definitely, there’s something curious happening today and that is that technology is becoming a well know knowledge, even on YouTube is possible to find tutorials on how to hack systems. It is very important, it’s the same as long time ago (as an example) that people could live in a house with no fences, the thieves did not enter, but then they realized that they could enter the house and that valuable things are inside the house that can be robbed, so they started robbing and the people started creating fences and ways to avoid thieves, the same happens with computer networks. You don’t have to be a guru for hacking systems, because of the information revolution that is taking place in today’s scene.
6.1.4- Interview number four:

1. What facts you consider to be important when deciding that a program or website is trusted enough to be used in the enterprise?

The first thing to have in consideration is that the application follows globally recognized standards, and that it is certified by a recognized enterprise. Avoid piracy at all costs, as these programs don’t receive maintenance nor customer service and the most important reason to avoid their use is that they are illegal. The use of licensed programs it's the most convenient solution for an enterprise, and when we are talking of the database of a company which is something that cost money to the enterprise if it loses it. Many people that doesn’t know much of technology sees spending money on security and licensed programs as an expense, but it is actually an investment, a database, a program and a website all certified and licensed is an investment to help assure a secure network and secure data.

2. For you, what is the importance of company data assets?

They are very important, as the company information is essential for the business, as is something that cannot be corrupted. It's not like an employee who is actually here today but I can get fired tomorrow, is really an important part of the company, and is like the core of the company. The reason for the data to exist is that the company has: taxes to pay to the state, sales record, accounts to collect, and other things that the enterprise must have on hand when it needs to pay all its expenses, and, as everything in business, the faster the better, and this is what data does, it accelerated the business, which means more money, if we compare how fast everything was made when everything was done in paper, it would be easier to notice the importance of the data, also it had less options to maintain active copies and not forgetting the physical amount of space that the papers occupy.

So as a summary, data is very important as important as the papers that were and are still used in some company as their primary means of maintaining their accounting.

3. In your words, what must be done to diminish malware?

Use anti-malware software licenses, and always maintain them updated. In cases that I have known the manager of the company, with the goal of reducing malware in the network, what has done is to completely remove the internet access of all the company computers, and only his computer has internet, which I believe that does not solve the malware problem because the employees still bring in their USB sticks, with malware from their respective houses, these are replicated in the entire network and the infection is spread to all the machines, in addition to not being connected to the internet these machines do not receive the necessary updates to keep itself free of the threats could affect the company, and it doesn’t use legal operative systems, which is
a fatal combination, still the company functions but with a lot of headaches because of their not reliable network.

4. What do you think is the difference between spyware and virus?

The difference between the two, I consider the spyware as something less harmful than a virus, but I know they have their malice, I see them as negative for the computers. So virus is a program that can harm the data, can allow intruders to hack the enterprise database, and can use enterprise system resources for the benefit of its developer. But about spyware I currently don’t have a specific definition of what exactly is, but I do know that it is a type of virus.

5. What practices you consider that you can do, to help secure the enterprise data assets?

Make backups outside of the company via the Internet, and physical backups, either on hard drives, CD’s, but it’s a very good practice to have the network functioning, for doing backup via the web. To have a contingency plan, and restrict user access to places and applications that they don’t need to use in their daily labor.

6. In your opinion, what is the importance of maintenance in network security?

It is extremely important, since it’s how systems evolve, and it’s like what I say frequently, that what’s obsolete is obsolete and it must be changed as soon as possible, since I believe that the best brand is what is new. To do regularly maintenance to the database of the enterprise keeps it safe from possible data corruption. I believe that maintenance of hardware and software is essential to keep a healthy network.

Well as a summary, wherever there is a software update the IT department should do it as fast as possible, if this is done correctly, giving it proper maintenance, the network is less prone to have a malicious attack or a system failure, if everything is in order and actualized to the latest version.

7. What do you think about social engineering? Is it an issue for the network security?

Well in my opinion, the good part of social engineering is that it helps advertising, in this times sellers don’t have to go directly to the client’s location to deliver a price estimate, nor can sending it by fax, since often go wrong, if they, by social engineering, could get the email of a possible client, then they are encouraged to do so since the laws in our country doesn’t penalize it, this is why email has changed totally the way that things are done in this topic, I believe that is excellent.

As everything in life a bad part exist, the bad part is that there are many people who can get information from your enterprise using social engineering, these information could be the new product that the company is developing, the name of your company servers to try to hack it or to get some information from the secretary or a seller that could lead to critical finance
information. When there is no proper security malicious people could get information that can be critical for the enterprise.

8. Do you consider that to have a disaster recovery plan is important for the enterprise? If yes, why? If no, why?

As I said before, it is important to have a plan B, especially when we speak of a company which is entirely dependent on the data it manages. It's always good to have a contingency plan. An example of a contingency plan is to have redundancy, to have redundancy of all the critical equipment of our network, and have an external backup that activates itself in case of an emergency so production is maintained and almost never halted.

9. When speaking about passwords, what is your strategy for maintaining it secure?

I recommend avoiding the use of birthdates or personal names, birthdays of a relative, anniversary date, family names, and names of things the user likes. I think that to have a secure password, it is good to think about the things that are less related to oneself, this should help to make possible password breakers clueless when trying to guess a password, and also this oblige them to try to use try and error programs to guess it. As part of the strategy we have policies that make users aware of the rules about passwords security and every other rule. Every user receives training before they even start to use our network equipment, with the objective of creating better users that will cause fewer problems to the network. We believe that people that have formal education is better at everything. In our case, that is, the IT team, we receive trainings or conferences every six months which keeps us actualized and prepared for everything that could happen.

10. Do you believe that a company needs to apply network security policies? If so, why?

Yes, because network security policies allow us to keep a tight control of the network, they also help to reduce the problems that occur in it. A well-enforced policy helps to protect data from threats that pose the modern world and the internet. An example of a network security policy could be to ban the use of the USB port on all user computers; other policy is to not allow the entry of foreign computers to the enterprise network.
6.1.5- Interview number five:

1. What facts you consider to be important when deciding that a program or website is trusted enough to be used in the enterprise?

The first factor that I take under consideration is that the application must meet the market standards, this includes that it must be certified by a company that ensures the quality of the program, and that gives to it proper maintenance so that the risks potential risks are reduced. I consider that a program that will be implemented in our company must be licensed by a big company, because this gives us IT less headaches when we have to solve any problem that appears.

In the case that this company decides to have the program developed internally, quality assurance must be done to the program in order to assure that the program doesn’t harm the enterprise interests and integrity, with this I mean directly that it doesn’t harm it’s data or its intention to make some or all the data confidential. This could include also checking the methods that the program uses to access the data, if it’s going to permit the data to be accessed via web, and if this is true that it has a proper security protocol that ensures the confidentiality of the data. It is no mystery to know that there are always people who wish to pay to know information about the strategy that your business use to do certain things, this happen mainly in competing companies, which pay spies to get internal information from its competing companies, they do this as a strategy to keep their competitors close. I personally believe that in order to develop the program internally, a Quality Assurance department or a software maintenance department should be created, or in case that the enterprise would not like to create a whole department for it at least to create a team of 2 or 3 QA that ensures the quality of the program, part of its goal would also be to check if there is malicious code in the program in addition to verify that there are no errors in the program.

It’s also good from time to time to hire a team of contractors to verify the systems with the goal of discovering problems that internal team failed to reveal, thus improving the security of these systems, of course this team of contractors must come from a company recognized internationally. All this said is of course taking into consideration that the management provide the money to do it, because most of the times enterprises in our country lack of security measures because of two main reasons, the first is that the company financial administrators consider the money spent in security measures as a waste of money, the second is that they don’t have the enough money to do it, this is the case of mid size companies, so because of these two reasons there are many breaches in their systems.
2. For you, what is the importance of company data assets?

*It is very important for the company because the data stores the files used every day, and this data includes customer information, employee’s information, information of the project that the company possesses, payments, debts and other economic data that a business manages. We could say that the data handled by the company is its life. They are essential for any company, and a business that loses its data is a company that basically has to start from scratch. Many times the administration of corporations in this country gives little importance to company data. They are more engaged in the production of money, and tend to abandon the maintenance of data, with this I mention they do not hire professional staff who can indicate what is best to keep their data assets, and therefore employ cheap technician that only know how to repair computers and that doesn’t necessarily now how to prevent network problems. Then a disaster occurs this could be a virus that corrupt the data, or that damages their hard disk, a fire burns the main server, then they are left without anything and after this happens is when they think of improving the business data security. As a last opinion to your question is that in our country there are many flaws in data security only large companies really secure their data.*

3. In your words, what must be done to diminish malware?

*I think that having a good antivirus installed, a good antispyware should diminish malware correctly. Not only to have an antivirus but several antivirus because there are some that find different types of files, to have 2 or 3 specific antivirus will do to diminish malware. To reduce malware in business is as convenient to use antivirus like NOD32, Panda, but it is better to use traditional antivirus or licenses such as Symantec and McAfee, because these companies have years working with malware and this truly demonstrates that they have much experience in dealing with malware. It is also advisable to maintain the antivirus programs updated, which also is good practice to reduce the malware, because what would be the objective of having antivirus installed on all computers if the IT department doesn’t maintain it actualized.*

4. What do you think is the difference between spyware and virus?

*Viruses are more malicious programs than the spyware. Spyware are little programs that send you to an address and that it keeps record of your cookies. They don’t do as much damage as viruses, since viruses are programs that tend to damage any archive or intend to harm the data. Viruses tend to infect computers that use Microsoft’s OS and programs, trying to damage the OS to make you lose information, and corrupt critical OS files, the *.exe files are the ones that get infected with more frequency.*
5. What practices you consider that you can do, to help secure the enterprise data assets?

Update the antivirus, actualize the operative system, do a daily antivirus check to all the PC’s. Also perform daily backup or at least in a regular period. Monitor frequently the network security. Verify that only the permitted server ports are open with a firewall like Microsoft ISA server which not only blocks hacks attempts but also controls user access, reducing this way the possibilities of an outside attack and to ensure that no attempts have been made to enter the server by internal staff.

6. In your opinion, what is the importance of maintenance in network security?

It is very important for the reason that I stated before that the programs always lack of something, or have a vulnerability that must be fixed, or the developers discovered a better way of doing something. Therefore the IT team must keep updating and checking to see if there are new updates and if they find them to install them, because the new version could fix some vulnerability that the last version had that would compromise your company. Evaluate, if you get more security or better benefits with a new software upgrade, then it would be reasonable to change all the software to the new upgraded version. I think it is very important to perform maintenance on the computer. If the company does not give maintenance to the network, it can become damaged and if you do not know where the damage is, information is lost, then if you do not give proper maintenance to the network, even if the company has a backup, in case a disaster occurs it will not be possible to recover. Data can be so important that the company cannot afford to lose them, as it may lose millions of pesos, lose the credibility of their clients, and you can also lose the ISO 9001 certification if the company owns it. For what I think is very important.

7. What do you think about social engineering? Is it an issue for the network security?

Currently I don’t know about the term.

8. Do you consider that to have a disaster recovery plan is important for the enterprise? If yes, why? If no, why?

It's important, because if a disaster happens the data can be recovered. Thus this way the IT team is prepared for a disaster. To be aware of the possible problems that a disaster could bring, increases the possibility to possibly recover from the disaster, with a minimum of loses.
9. When speaking about passwords, what is your strategy for maintaining it secure?

Really what we do is that each user has his password to access the company’s program. Not every user has all access privileges, this means that some programs are accessible but other aren’t. But talking about strategies on how to create passwords, it is important to use the standards known in the market, either the use a long password, so it is more difficult to decipher or the use of certain codes to identify the service that the user is accessing. I believe that it isn’t a good practice to use the same password on different web pages or in different programs. To solve this problem I recommend the use of different passwords for each program and to help remind each password I create them a little similar but with some distinction. You can use the technique of framing, something that identify the program you’re using, for example, if you’re going to use a Gmail ending in g. Another strategy is to change it periodically. Banks that use internet banking also use this strategy.

10. Do you believe that a company needs to apply network security policies? If so, why?

Of course, because in these policies is where you define the network security of the company. An example of a network policy is that one I said before about changing the password from time to time. They are important because they permit the administration to control the users and thus reduce the risks of possible damage to the system and the enterprise network. A major network policy is to educate all staff who uses it, so they would subsequently know how to use the systems that the company provides and so they know what they should and shouldn’t do, and to improve job performance.

6.1.6 - Interview number six:

1. What facts you consider to be important when deciding that a program or website is trusted enough to be used in the enterprise?

The first is to make the site a reliable source, at least that it uses SSL, if the website uses forms, at least it should use a secure code for data collection, certificate verification is the first thing to do, is always important to verify the technology that is being used, because that way you know what vulnerabilities it has, since there are technologies that have a bigger number of vulnerabilities than others. As a developer is necessary to review the code, check if it validates the fields, what kind of validation it has, if it really validates correctly, if it avoids SQL Injection, field validation at value level, security ranges from simple things like these up to security certificates, which are currently the most powerful security tools, adding reliable authentication tools is desirable, which is not simply entering a username and password to the database, but other parameters and other conditions like temporary passwords, and such things that also applied in the company. An important thing to mention is the use of plug-ins and ads that the website have, which can be very delicate because there are companies that may want to restrict the use of Active X, which is not very reliable for a domain, because there are certain vulnerabilities that are attached directly with the implementations of these ads and plug-ins, and
most common browsers such as Internet Explorer, Firefox, and others, are vulnerable by themselves, then there is the business that has to define, according to its parameters, which plug-ins and ads that will be accepted and implemented and which websites, because if the website isn’t verified as secure for the company then it’s not added.

2. For you, what is the importance of company data assets?

Data assets are the company, this means that the information handled by the company or the entire enterprise is sustained on the management of data, for example I could say that in education institutions the registry in PUCMM manages the data with enough security at the staff level, but what would this level of security mean if a student of the institution could change his academic grades record, on the website of the Institution. This is why I say that the data is the company. In addition to this, for example, a student gets to modify some information within the Institution website, it is understood that the website is the responsibility of the Institution, then, once this happens, it immediately has a direct impact on the confidence that the general public have of the institution, so if there is no mechanism that immediately detects such change or modification, then what would be the reputation of the Institution. The data is the core of the company, something as simple as a denial of service or access to the data makes it impossible for the entire enterprise to work, which means that the data in the business world today is the most important asset, a denial of access to the data or undesired modification of the entity’s data or alteration of it could imply that the firm could get out of the service.

3. In your words, what must be done to diminish malware?

Well I think the biggest problem of malware is not the program’s source code as such, but more the awareness of users to run malefic applications that they receive in their email, applications that they have in their memory sticks. The IT manager could restrict all access to the machine, but still the users keep downloading a bunch of nonsense, or trusting everyone, they share any information through the network. The most effective way of controlling malware is to make people aware of the danger, because you could have the best and latest antivirus and firewall impeding the unauthorized change of data, but at the time of opening some program the antivirus asks the user "This file can be harmful to your computer are you sure you want to open it?" and the user not even read it and click yes, then all the technology used to avoid the possible malware did not protect anything, then I understand that the problem of malware is more a thing of user awareness than anything else. I believe that over 60% of malware infections are executed by the user, whether consciously or unconsciously, but 60% showing that it’s really the majority.
4. What do you think is the difference between spyware and virus?

A spyware or a virus, the virus is basically anything that can reproduce by itself, spyware already has a different purpose, spyware is intended to open a hole to extract information, the virus objective could be to bother, just a banner printed on the screen that can spread itself, a program that has the property of reproducing itself alone and independently is a virus whether is harmful or not, spyware goes beyond, and tries to infringe the privacy of the user machine and gather information.

5. What practices you consider that you can do, to help secure the enterprise data assets?

First, starting with the Operating System, to help protect the data assets it has to have all the current patches, most vulnerabilities occur due to the lack of a patch that is already available a long time, and if you do not have a policy of operating system update then we have a breach. After the operating system we have programs like office that use macros, this everyone knows, is no secret that the use of macro can create a lot of things that can affect the security of the enterprise data systems, all this must be controlled, these vulnerabilities must be patched properly not only the operating system but also its applications. Subsequent to this would be the use of mechanisms like antivirus, for example on each client, on each server to verify the characteristics for everyone and, depending on the stringency that the company we are working for, to block or not or any use or not of the USB interface, prohibiting software that run automatically like the autorun.exe program, those are things that are easy to make and are at first-hand, things that are used every day, like the everyday update of the antivirus system. A well structured policy design and that the user get to know the policies and respect them, often in many companies a table of policies that no one knows and that no one is there to enforce and compel or persuade people that they must comply with it. Then there are rules of proper use of computer, mail, internet, it must be known by the user. I personally am very insistent with the common user, because this one is the one that executes the problems. Inside the company we have the use of firewalls. Like all IT know, most attacks come from inside the company which means that not much come from the outside, one covering the outer perimeter, but the inside network is not covered, and for that there are many mechanisms for permission control, IDS, all such technologies, expensive although, the importance that the company's information has will justify the payment for it, if they consider their data as important they will pay the price, if not they won’t.
6. In your opinion, what is the importance of maintenance in network security?

Maintenance is very important since maintenance is monitoring the health of the network, on a daily scale the IT’s check that the server is downloading updates, this if you have configured policies that download updates but don’t install them, it is part of the maintenance to check and really install or permit the installation of updates. Mostly in Operating Systems like Windows a restart is required for an update of the OS, Windows OS will require it greater proportion but in other operating systems like Linux, when there is an update, the updated service must be restarted, indicating that at least the service will be down for a small period of time. Then, maintenance is to verify not only to revise the physical part, but also to verify the logic part, as well as the updates of the antivirus, the list that the IDS have, to check that they are being updated, check that the repository are downloading the lists repeatedly, to review, something that not everyone does as part of maintenance, to revise the backup since often the IT is entrusted and never restore a backup, so he never knows if it works or not, then part of maintenance is to take a tape backup or hard disk, restore information from backup and check if it works well in a test environment, verify that the redundant digital lines, if for the business is critical to have redundancy of lines, is part of the maintenance to review the health of these digital lines, if indeed they are giving the contracted bandwidth, according to the requirements of the company, which is constantly changing, after 5 years that passed after contracting the service the company grew so much that the bandwidth of the line is very small and when you use these lines falls short of your bandwidth, so again, it is part of the maintenance to check if things are working and check if they change.

7. What do you think about social engineering? Is it an issue for the network security?

It is a problem for everyone even in our own home, the amount of information that is given unconsciously to a person using social engineering is almost impossible, well not totally impossible, because if one, with the proper conscience, wouldn’t give sensitive information, but if one is always thinking on it paranoia could be reached. There are people who are experts in this subject and they could get any information, if they want to do it, maybe not directly but indirectly with someone who already has it, if one is not properly trained. How to combat social engineering? It is better that if a person that is not supposed to know something to stay without knowing it. That is how the enterprise helps to avoid that the secretary ends giving very sensitive information, including server names. Then, also, no one can blame the secretary, perhaps because of their academic level or the level of importance she gives to the server name or something as simple as that, she is not aware of this, then a person of some awareness of this can gather sensitive information and she believes that it is not creating a problem, she may be told not to give information to others but it is something that is not important for her, then how to counter this, the first form is that it is better that if a person that is not supposed to know something to stay without knowing it, then after that we are going to make her aware of this by mentioning, for example, these things should not be said, you should always call a person from the technical staff of the company to run anything on the computer, that you cannot do, no matter the level of confidence that you have to the person that is asking you or stressing you. Also that is very common is people that finds memory sticks from anywhere and then they go and install them on any network computer and a virus hits the network. As for phishing this is also a world apart, in this case what one prefer is to block this type of user to access this site.
8. Do you consider that to have a disaster recovery plan is important for the enterprise? If yes, why? If no, why?

Yes, because the enterprise is not only being exposed to vulnerability in the security level but also the fact that in the case of a disaster no one protects you. In a country like ours that is localized in the tropics, which is at the mercy of incidents in either the form of hurricanes, earthquakes or tsunamis, a backup plan or contingency plan would be ideal, the company that doesn’t have it would have a serious fault, so serious that simply not having it makes the company very vulnerable at the time of the incident and is little they can do after the accident happens if you are not prepared for this, the company could simply go out of the business, of course, this if it is important its presence, nevertheless, in the market. If the company doesn’t have a contingency plan, the company exited the market and this can cause the collapse of the whole business. In case of a company that is based on the use of information, such as an academic Institute, if you lose all your academic records, the academic institution is broke, as simple as that, because this information defines which students are studying and those who have had previously studied, whether they are on paper everything can be lost. How important is a disaster plan, I understand that is the most important in addition to protect what's working and what is working as backup.

9. When speaking about passwords, what is your strategy for maintaining it secure?

It depends, password policies depend on the work environment, depend on the company, not the same rules apply for a banking enterprise security password policy, that what would require a manufacturing industry, it is not the same and it makes no sense to have the same requirement. Effective use of password, users must know that the password is personal, not to be transferred, which should not be under any circumstances given or written and left it at an accessible site. Meanwhile the level of complexity and password expiration time depends on the company, since it can go right from changing passwords monthly or less than a month, or are changed every 3 months, which is the most common. Then the complexity can also be changed according to the level of information handled. Speaking about the permissions that are granted to users, a person who uses a PC and use an application that intends to access critical server information, that a program block the access to the sensitive equipment of the company, because we already have security mechanisms to make this impossible, so if you can have passwords is easier since there are already other ways to counter any attempt to do harm. Now in the case of a network administrator or any other area, then more complicated requirements are given because of the responsibility that this user has and its capacity to handle sensitive data.
10. Do you believe that a company needs to apply network security policies? If so, why?

Of course, simply because this way you have control over the physical access to the hardware, or as a result, it is possible to filter the entrance to the area where the datacenter is, this means that only the indicated staff could enter, and with policies IT administrators can control what, the staff that can enter the data center, can and cannot do, but through the network a rogue employee can do much more damage, then if you don’t have an effective mechanism to counterattack any threat, and, as we know, most of these threats are transmitted through the network, and most of the vulnerabilities are run from a person who is within the company, using the resources of the enterprise network, if there isn’t any policy that helps protect the business data against these threats, then the company should leave the business. So if it does not exist, within the company, a minimum of security in the network, then the business could have massive losses. Also access policies, most people have a flat structure, there isn’t any division and everyone can connect to computers that pose high and lower risks without any problems, then in those cases, where there is no protocol filtering things are worse. The initial principal mechanism should at least have a different hierarchical division between clients and servers after that and the firewall, IDS, on clients and servers and that’s all.

Go back to the results section.
7.0- Appendix B:

7.1- Quantitative data collection

7.1.1- Network administration best practices:

What do you understand by access privilege hierarchy?

d) That common user must have less privilege than IT users.
e) That always there should be someone that has all the privileges, which supervises the access of every user.
f) That a type of privilege pyramid exists, on which only a few have maximum privileges, but also these don’t have totalitarian privileges.

How much do you agree with this expression: “It is considered a good practice to have a universal password to access network equipment”?

d) I agree, because if everyone of the department of IT knows the password it will help to work more efficiently when they find a problem.
e) I disagree, because it could be discovered very easily because all network since use the same password.
f) It depends, because if the password is unique and universal but it is changed every certain amount of time, then it sounds as a combination of security and efficiency.

How much do you agree with this expression: “The value of the data is proportional to the size of the company”?

d) I disagree; because the data has the same value whether is a grand enterprise or a small company.
e) I agree; it’s not the same to manage the data of a small company than the data of an enterprise, because the last one handles more critical data.
f) It depends on the business of the company, because there are businesses that support loss of information, meanwhile others do not.

How much do you agree with this expression: “Most common networking problems come from misconfigured network equipment”?

e) It depends, because it is not possible to determine what provokes more problems, if misconfigured network equipments, non trained users, or bad network administration.
f) I agree, because the network equipments get misconfigured frequently, and this is a constant problem.
g) I disagree, because the most common reason of network problems comes from non trained users.
h) I disagree, because the most common cause of network problems comes from a bad network administration, including not applying network policies.
How much do you agree with this expression: “It is considered a good practice the proactive maintenance of the network”?

d) I agree, because by giving proactive maintenance it is possible to foresee and solve problems before they happen.

e) I disagree, because I consider that the proactive maintenance is a waste of time, I prefer to solve the problems when they appear, because it is cheaper and efficient.

f) It depends, because it is possible to do a proactive view to solve future problems and a reactive view to solve problems that happens by surprise.

What do you understand for Disaster Recovery Plan?

e) To only make backups of all the information of the enterprise.

f) To create a list of instructions that depicts all possible forms that the enterprise could survive a disaster.

g) To install redundancy on all servers, and connections of the enterprise.

h) To not think on what is the worst that could happen, before it happens, apply it on a plan and execute it when necessary.

Do you consider important the existence of policies that control the activities of the IT administrator?

a) Yes, because it is considered a good practice that the company could control in a pyramid like form the access and modification of the important data of the business.

b) No, I believe that the IT Admin must have all privileges in order for him to solve all network problems without having any obstacles.

c) I consider that it depends on the business, because there are businesses that could operate independently from the network, so network policies applied to IT become less important.

Could you differentiate which of the options aren’t network policies?

e) Check if the backup was correctly done.

f) Give training to each new user about how to use the equipment that they’ll use.

g) Don’t give information of the company computer systems to people that doesn’t belong to the Business.

h) Work with honesty and commitment.
7.1.2- Vulnerability and attacks:

How much do you agree with this expression: “Cross-site scripting attack happens with more frequency on websites that manages money”? 

d) I agree, because this type of attack it’s focused on website vulnerabilities, and it happens with more frequency on websites that permits the user to manage credit cards and bank accounts.

e) I disagree, because this attack doesn’t occur with much frequency on those websites, because they have enough security.

f) It depends, because it is not necessarily used to obtain money, the attacker may have many different objective, since the principal objective is to trick the website user and to obtain any information that it is inserted on it.

What it is known as a Denial of Service Attack or DoS?

d) It is a group of computers that combine themselves to send virus and spam.

e) It is an OS made by Microsoft.

f) It is known as DoS to an attack made by one or more computers to a specific target computer, with the objective of squandering all its resources, so it wouldn’t keep delivering its service.

How much do you agree with this expression: “It is possible to completely eliminate all malware existent in the network with a good antivirus”?

d) I agree, because by having an antivirus that is from a recognized brand, that has a proper support, and that the IT administrators maintain them with the latest update installed it is possible to eliminate all malware threats that could affect the network.

e) I disagree, because for diminishing malware in the enterprise a quantity of measures must be taken, these measures includes a good antivirus, network software maintenance and the implementation of network security policies.

f) I disagree, because malware is very difficult to eliminate, there is always a virus in the servers, there is always a curious user that breaks the rules without one noticing it.

Select the options that don’t have any relationship with the definition of phishing:

f) It is a technique for gathering information from the computer.

g) Apply redundancy in all connections and network terminals.

h) A branch of social engineering

i) A type of vulnerability that permits a malicious attacker to inject a script, provided by his own domain, to a website that is open to the public.

j) It is called phishing to e-mails sent with the objective of obtaining critical information by tricking, scamming or exploiting a vulnerability of the system.
Select the possible reasons why malware enters to the data network of the business:

f) Outdated Antivirus and Operative Systems.
g) Good network policies.
h) Banning the users to install any software on the network.
i) No control over the user’s removable devices.
j) Bad implementation of network security policies.

Why are common people generally tricked by phishing?

d) Because users don’t know it exists.
e) Because scammers use very effective methods to trick the victim.
f) Because the user doesn’t know that is a scam.

Do you consider a Distributed Denial of Service attack or DDoS a risk for the networks of Dominican Republic? Why?

d) Yes, because technology is no longer a mystery and anyone can pay hackers to do a DDoS attack to a certain company server, with the objective of removing it from the market.
e) No, it is not a risk for our country because we have never seen an attack like these on our country, and I consider that here there aren’t hackers with the enough level of knowledge to create an attack of such magnitude.
f) It depends on the business that the company has, and how necessary is its online presence, because is possible that they don’t need any presence on the web.

Go back to the results section.
8.0- References:


[9] W. Robert Collins (a), Keith W. Miller (b), Bethany J. Spielman (c), Phillip Wherry (d). 1994. “How good is good enough?: an ethical analysis of software construction and use”, (a) College of William and Mary, Williamsburg, VA, (b) Sangamon State Univ., Springfield, IL, (c) Southern Illinois Univ. of Medicine, Springfield, IL, and (d) MITRE Corp., McLean, VA.


[12] www.surveymonkey.com