

MSc In Computer Systems Management

Botho University

Research Project

Names: Laone Kwelagobe

Student ID: Sgb1202636

Title: Network Downtime in Government Department – An Investigation of this common Phenomenon with suggestion of best practices and best technologies

Acknowledgement

I would like to pass special thanks to the Botho University management for a great opportunity given to me to the opportunity to study in their highly reputable university. I then would like to thank my tutor for his patience, guidance and undoubted support when I was working on compiling this project.

I would like to thank my family most importantly my husband who has been so supportive and always encouraged me. I thank you Lord Jesus for you are the one who carried me throughout.

Abstract

Network downtime is the period in which a computer system is unavailable or system fails to provide/perform its primary functions. System reliability and/or availability are very Key as an unavailable system is a failing system. It is very common in Botswana for government clients to forfeit being serviced because the government department system is down.

The primary aim of this project was to investigate the causes of system/network downtimes in Botswana government department. Three government departments were targeted along with three system stakeholders who the researcher distinguished them as a technical User, a user and a client.

The study showed the concerning results that justifies that system downtimes in government department is very frequent and also it can take some time before downtime is resolved. Common causes of downtime in government departments were identified and with the help of literature the researcher recommended how the causes can be mitigated.

Contents

Acknowledgement	2
Abstract	3
Table of Figures	6
Table of Tables.....	6
Chapter ONE Introduction.....	7
1.1 Introduction	7
1.2 Background of the Study.....	8
1.4 Definitions	12
1.5 Research Scope	13
1.6 Dissertation Outlining	14
Chapter TWO Research Definition.....	16
2.1 The Practical Problem	16
2.2 Existing Relevant Knowledge	17
2.3 Aims & Objectives	23
Chapter THREE Methodology	25
3.1 Research Methods Chosen	25
3.2 Justification	30
3.3 Research Procedures	38
3.4 Ethical Considerations.....	40
Chapter FOUR Analysis and Interpretation.....	42
3.2 Results	42
3.2 Summary of data Collection.....	43
4.3 Results Interpretation	62
4.4 Recommendations	64
Chapter FIVE Conclusion.....	67
5.1 Further work	68
5.2 Research Implications	68
References	69
Appendices.....	72
Appendix 1 Extended Abstract	72

Appendix 2: Technical Questionnaire 76

Appendix 3 - User Questionnaire 81

Appendix 4 – Client/Customer Questionnaire 82

Appendix 5 - Gant Chart Sample 84

Table of Figures

Figure 4.2.1: Technical User Question 1 results	45
Figure 4.2.2: Technical User Question 2 results	45
Figure 4.2.3: Technical User Question 3 results	47
Figure 4.2.4: Technical User Question 4 results	48
Figure 4.2.5: Technical User Question 5 results	48
Figure 4.2.6: Technical User Question 6 results	49
Figure 4.2.7: Technical User Question 7 results	50
Figure 4.2.8: Technical User Question 8 results	51
Figure 4.2.9: Technical User Question 9 results	52
Figure 4.2.10: Technical User Question 10 results	52
Figure 4.2.11: User Question 1 results.....	53
Figure 4.2.12: User Question 2 results.....	54
Figure 4.2.13: User Question 3 results.....	55
Figure 4.2.14: User Question 4 results.....	56
Figure 4.2.15: Client/Customer Question 1 results.....	57
Figure 4.2.16: Client/Customer Question 2 results.....	58
Figure 4.2.17: Client/Customer Question 3 results.....	59
Figure 4.2.18: Client/Customer Question 4 results.....	60
Figure 4.2.19: Client/Customer Question 5 results.....	61

Table of Tables

Table 4.2.1: Shared Questionnaire Result Summary	43
Table 4.2.2: Shared Interviews Result Summary.....	44
Table 4.2.3: Technical User Question 2 results	46
Table 4.2.4: Technical User Question 3 results	47
Table 4.2.5: Technical User Question 6 results	49
Table 4.2.6: Technical User Question 8 results	51
Table 4.2.7: Technical User Question 10 results	53
Table 4.2.8: User Question 1 results	54
Table 4.2.9: User Question 2 results	54
Table 4.2.10: User Question 3 results	55
Table 4.2.11: User Question 3 results	56
Table 4.2.12: Client/Customer Question 1 results	57
Table 4.2.13: Client/Customer Question 2 results	58
Table 4.2.14: Client/Customer Question 3 results	59
Table 4.2.15: Client/Customer Question 4 results	60
Table 4.2.16: Client/Customer Question 5 results	61

Chapter ONE Introduction

1.1 Introduction

Botswana has been one of the fastest growing economies in the whole world as it shifted from being one of the poorest countries in the world into the ranks of upper-middle income countries ever since it got independence in the year 1966. (The World Bank portal (Oct 17, 2016)).

The country has been passive in taking advantage of areas that can better its economy. One factor that the government has to make use of is the Information Communications Technology (ICT), expanding the use of computers and the interconnected world. All is done with the aim to bring competence and efficiency in the services offered by the government. The President of Botswana confirmed that for competent and efficient service delivery from the public service the government has embarked on the computerization and incorporation of processes through the e-Government program and thus have seen government departments being fully equipped with Local Area Networks being active, He said this in the state of the Nation Address on the 13th November 2009.

Even though all these good measures have been put into place there is a common factor that is experienced in almost all government departments which is the frequent fault in the Local Area Networks, as a result the public service has very low ratings on services and productivity. And these phrases have become so normal to the government departments “there is no network” or “system is down”. This norm will therefore be referred to as the “Network is Down Syndrome”.

The aim of the study is to have concrete proposal on what can be put into place to decrease/transact with this common network downtime issues and to recommend any new technologies and/or strategies to be use/practiced to reduce or stop system downtime in government departments.

1.2 Background of the Study

Botswana as a country has developed rapidly therefore there was need for efficiency and effectiveness in service provision and thus a rapid increase in the use of computers or rapid growth of computer networks (Local Area Networks). A rapidly growing network requires careful planning and/or design, with hardware used catering for possibilities of growth.

An increase in the deployment of computer network system also exposes the networks to an increase in threats (Catherine Paquet (2013)). Therefore the network (Local Area Network) security becomes exposed and/or vulnerable because of its growth and because of the internet connection (World Wide Web). Therefore there is without a doubt a vital need for increased security. Government departments will possibly require security such as authentications, authorizations, surveillance and identifications in order to protect the integrity, availability, accountability and authenticity of computer hardware, data or general network equipment.

A poorly planned or designed and/or unsecure network leads to frequent system downtimes. Network downtime impacts negatively on business and administration as it “kills” the primary objective of the use of computer systems and/or networks, which is to bring about efficiency. Network downtime also brings forth lack of trust as elements of lack of security care shown by system failure and therefore leading to users not trusting the system.

As a result of the government system/network failures (“Network is down syndrome”), the government clients now lack trust in the government system(s), especially those that has their sensitive information stored in such systems. In December 2004 the Botswana government launched a national ICT Policy known as Maitlamo, Botswana’s National ICT Policy and has been improved ever since its inception. This was an effort to show commitment to developing a National ICT Policy that will build upon e-government initiatives and assist in achieving Vision 2016/2032. In keeping with Vision 2016, it was envisioned that the National ICT Policy will position Botswana for sustained growth in the digital age by serving as a key catalyst in achieving social, economic, political and cultural transformation within the country. Unfortunately a little was achieved as the network/computer system problem persisted, leading

to the common phenomenon in Botswana of system failures (Maitlamo, Botswana's National ICT Policy (2011-2016)).

The problem at hand is that Botswana government departments are commonly known for the failure of their Local Area Networks (LANs). This is therefore referred to as a "Network is down syndrome" because it is very common to be informed that the system is down in government departments in the country, leading to clients not at all being serviced or experience delayed services because of network downtime.

There are many factors that may lead to a network downtime. Hardware failure is the number one reason for network failure (Vinod Mohan (2007)). Below are some common causes of system downtime:

- Faults or errors in network devices
- Configuration updates in devices
- Mismanaging of devices and/or operational human errors
- Link failure due to network congestion and/or fiber cable cuts
- Electricity cuts
- Server and/or hardware failure
- Security attacks such as denial of service (DoS)
- Failed software and firmware upgrade and/or patches
- Incompatibility (firmware and hardware device)
- Lack/No technical Skills

The project will therefore try to identify the common factors that may lead to system downtimes (in Botswana) mainly focusing on government department(s) and endeavor come up with possible solution to ameliorate the situation.

1.3 Justification of Research

The purpose of this project is to look closely at the possible cause(s) of the network downtimes in government departments. The project will look closely into the current state of the government Local Area Networks as an effort to try and identify security issues that may be leading to the network down time (System is Down Syndrome). This will be done by identifying one or more government departments that the researcher will closely work with to try and understanding the possible causes.

According to the Botswana National e-Government strategy (2011-2016) Botswana government aimed at moving all its appropriate services online with the aim of drastically improving the convenience, quality and efficiency of public sector service delivery. But common network downtime has negatively affected this strategy which mainly came about because of many challenges of service delivery as indicated by the 2009 customer satisfaction survey which revealed a fairly low level of customer satisfaction of 27 %. According to the survey private sector appear to be more appreciative of the public service than government departments. Now with the anticipation that the service satisfaction level will markedly increase through the introduction of the service oriented and client-centric national e-Government program, the common phenomenon of “System is Down” is hindering all these good intentions/planning carried by the Botswana Government.

Furthermore, the government’s 2016 draft budget proposes an allocation of P174 million (approximately USD 15.6 million) for ICT development as part of the Ministry of Transport and Communications’ development budget which is the ministry driving the ICT development program/e-government (Ministry of Finance and Development Planning, 2016). The investment provided an important opportunity to improve the system/network performance in government and shows the determination by the Botswana government in driving the ICT development strategy (e-government).

Therefore a closer look on the common causes of system down times in government ministries and/or departments is critical for the success of the deployment of e-Government.

On the other hand, an American business, released a report that revealed and analyzed the financial impact of infrastructure vulnerability because of network downtime (Emerson Network

Power (2015)). Although this project will be focusing on government departments(s) not cooperate business, the network downtime brings the same kind of financial consequences across industries. The Emerson Network Power findings estimated network downtime financial costs as:

- Cost of network downtime across industries is estimated to cost a business \$5,600 per minute.
- A roughly 90 minute downtime results at an estimated average cost of \$505,500.
- A total network outage, with a recovery time of 2 and a half hour, average costs are projected at about \$680,000.
- A partial network downtime, averaged at an hour in length, costs an estimated average of \$258,000

Although this study was based in the United States of America, it still clearly shows that system downtime doesn't only affect services it costs business thousands if not millions of dollars. This is NO different to the government of Botswana as it means every time there is a system outage, Thousands of Botswana Pula (Local Currency) are Lost. Therefore, it is necessary to investigate at the possible causes of this downtime and suggest ways that can improve the issue and make the network more trustworthy or more secure.

1.4 Definitions

The following are the common terms/wordings that are used in the project and their definitions as per the researcher perspective.

Term	Definition
DIT - Department of Information Technology	Department of Information Technology is a department that facilitates and/or administers all of the information and communication technology services in all of Botswana government public sectors.
DRTS - Department of Roads Transport and Safety	Department of Roads Transport and Safety is a department under the Ministry of Transport and Communications in Botswana.
Government Departments	In this research the mainly refer to the DIT, DRTS & MLHA
LAN – Local Area Network	A computer network linking devices with a single government department building and it is with a one kilometer radius.
MLHA - Ministry of Labor & Home Affairs.	Botswana government ministry that is responsible for providing social and economical services development services in Botswana. The Ministry has departments such as the Immigration and Citizenship, Civil and Registration, Labor and Security, Gender and the Department of Occupational Health and Safety
Network	Connection of computers and other devices to share resources such as internet, printers, routers etc.
Network Down Time	The periods in which the government system is unavailable
Network is Down Syndrome	A description adopted by the researcher to describe the System is down term.
System is Down	Commonly used to inform government clients/customers that they cannot be assisted because of system/network issues.

1.5 Research Scope

The project focus is on the network downtimes commonly experienced by the government of Botswana departments. The research will be targeting at least three government departments and one of the three should be the Department of Information Technology which is a department that facilitates and/or administers all of the information and communication technology services in all of Botswana government public sectors and therefore would understand the government downtime issues better as there are more technical people there than any other government department or ministry.

The research will target technical and none technical user as well as government clients/customer to identify the common causes of system/network downtime in government departments. The literature shall also contribute in identifying causes of downtime, but most importantly it shall assist the research in recommending what can be done to mitigate the government system/network downtimes.

1.6 Dissertation Outlining

The dissertation has a document cover that clearly states the researchers' details and the research title, followed by an acknowledgement where the researcher passed his sincere gratitude towards those who have contributed to the success of the project. The document also has five chapters that clearly delineate the researchers' work in a way that makes it easy for readers to follow the work. The following are the chapters:

Chapter ONE: In this chapter there is the research introduction followed by the background study. In these two sections the researcher explained the research problem and its context. This was achieved by description of what the problem/issue with appropriately supported assertions and/or citations.

This chapter has the justification of research section which basically outlines why the research did this particular research and how the government of Botswana could benefit for conducting such a research. The research chapter continued with the terms definition, scope and dissertation outline as an effort to make the research clearer and concise to the reader.

Chapter TWO: The chapter has the practical problem section which is a section where the researcher has clearly outlined in detail what the problem really is and what is it that the project wants to achieve/address. This section is then followed by the Existing relevant knowledge section which primarily focuses on literature relevant to the project. Enough evidence is obtained from this section justifying that this research is relevant and it is of high quality and mainly is informed by the secondary research.

The project aims, objectives, tasks and deliverables are the last section of the chapter and they clearly describe the purpose of this study.

Chapter THREE: The section has the chosen research methods and techniques which are clearly explained with concise awareness of alternative methods shown by the researcher. The research clearly indicated how the chosen methods will produce data required and thus successfully achieving research aims. The chapter then has the justification section which primarily provides convincing reasons why the research chose the methods. The research

procedures and ethical issues are the last sections of the chapter and they generally show that the methods used have been applied as per the recognized good practice. With Ethical issues being identified along with methods that addresses them described.

Chapter FOUR: Analysis and interpretations is the forth chapter that comprises of data collection and presentation sections. This section the researcher presented made use of appropriate summaries, table, charts and appendices to clearly and effectively present data. Data analysis is the section where the researcher used statistical and/or graphical techniques to analyze data and results. The researcher then interpreted the results in the last section of this chapter.

Chapter FIVE: In this chapter the researcher started by drawing a conclusion by summarizing the study and by a brief discussion on implications of the conclusions. The researcher then did the further work section as well as the Implications sections.

Chapter SIX: The researcher worked on the extended abstract, summarizing key dissertation issues.

Chapter TWO Research Definition

2.1 The Practical Problem

Despite the availability of information and communication technologies (ICT's) infrastructure in most government departments in Botswana, there is evidence of a lack of exploitation of the technology as network failures are still common. There are several factors that hinder exploitation of information technology in Botswana. With the massive investments that Botswana government has made towards ICT, it should now be getting some rewards. Lack of ICT infrastructure is often cited as a problem limiting ICT success/use in developing countries. Botswana's situation shows that infrastructure does not necessarily leads to high levels of use mainly because of poor management issuers (Mogotlhwane, 2013).

The Botswana government has heavily invested in providing a relevant information and communication technology infrastructure in all government departments in the last ten years (Nkwe, 2012). According to Mogotlhwane there has been a perception that productivity in most of government departments is not up to the expected standard. Such perception have mainly come from looking at the quality of service offered and since the government is the largest employer in the country and such perceptions brings a huge negativity to governments investment in ICT. Therefore it is evident that there is a serious lack of exploitation of the availed technology infrastructure (Mogotlhwane, 2013).

The Botswana government has taken a number of initiatives to address lack of productivity in the civil service, such as Work Improvement Teams, setting up the Botswana National Productivity Centre, implementing a performance-based reward system and developing good information and communication technology infrastructure in government departments. Some of these intervention measures yielded expected results (Selepeng, 2006). However, efficient and/or effective productivity problems still persist to date, despite relatively good information and communication technology infrastructure (Annual Report, 2016). The availability of these facilities demonstrates as observed by Maitlamo that Botswana is already an active participant in the global information society (Maitlamo 2013). The common network downtime problems

however are the key factor that appears to hinder the government departments' successful ICT story.

2.2 Existing Relevant Knowledge

System downtime may be unavoidable, but measures can be taken to reduce the chances of their occurrence and help in operation restoration sooner as well as mitigating their impact on an organization. A critical review of existing literature is thus key as an effort to try put up a solid case that will be useful to Botswana government departments in the future.

The government of Botswana adopted an outsourcing system for its services and product acquisitions that are needed by the government and such services include system/network development, systems/network maintenance, etc. This was an attempt to encourage the growth of private sector as well as making the whole process transparent. However outsourcing of Information Technology services has its own limitations and the biggest problem being failure to manage the whole process thus leading to frequency in network downtimes (Chad, Graham, Donald, 2007). It has been shown in the past that most government department in developing countries employs practices that can engender poor network management due to lack of audit of the impact of the network infrastructure (Bhathagar 2010).

There are many computerized information systems deployed in the Botswana government departments such as the National Registration System (Omang), Livestock Identification System (LIS), Vehicle registration system etc. These systems relay on the Local Area networks of their respective government departments for their success. One of the early information technology systems in the Botswana government is the National Registration System implemented 1998. The national registration system has been a subject of investigation by the Auditor General Office, the Botswana government spending watchdog because of the frequency of its downtimes (Namogang 2015). The livestock identification system was progressively implemented in 2001 and it was bought from an Australian company known not stated by government. It is used to store information about cattle, which are a source of beef sold to the European Union. The livestock identification system implemented to adhere to strict quality control requirements by

the EU. However, the system is also not functioning as required as there are problems of system/network maintenance (T. Mogotlhwane, 2013).

As per a white paper by Juniper Networks (May 2008), system/network downtimes are primarily caused by human error and with the increasingly organizations do not tolerance network downtime at all. This is easy to understand when the average cost of an impaired network was estimated at \$3 million per day, with 10 percent giving an estimate of more than \$10 million in damages and lost revenue per day. The paper sates the Human Factors/ Errors as the leading factor to network downtimes stating that configuration changes cause such outages. Unplanned events such as Hardware and Software are regarded as the second factor that may cause a downtime and Planned Maintenance as the list as it includes Hardware and Software upgrades.

According to a report by Chevin, a British network management company, a poll conducted over six weeks by staff at its UK customer support centre found that simple human error and lack of proper planning can lead to basic faults. They argue that these are the two root causes of LAN downtime and inefficiencies. (ComputerWeekly.com (2016)). It can also be argued this may be a great major contributor towards the “System is Down Syndrome”. The following are some of the most common factors that can lead to a network downtime:

- **Misconfigured routers:** devices installed and/or configured incorrectly at the very beginning or network implementation can bring serious consequences to network and contribute to downtimes.
- **Ethernet cards fault:** it can take time to detect a fault in an Ethernet card especially poor quality cards. Such faults may lead to network downtimes as time passes
- **Broadcast storms:** legacy applications can cause this on legacy servers. Under normal circumstances these should have been taken out of commission
- **Unnecessary/unwanted protocols:** Having had peripherals installed along with extra protocols can bring suffer to a network when these protocols are left on the network when they are no longer in regular use
- **Poor switch allocation:** Too may devices allocated to through one overloaded switch has high chance of causing LAN bottlenecks and these may contribute negatively to a network

- **Server overloading:** Poor file server maintenance can causing slow spots on the network and such slow spots can harm a network
- **Devices faults:** Network devices with fundamental faults can be difficult to detect initially and thus of serious repercussions to the network in the near future
- **Rogue equipment:** these are connections that are unauthorized by illegitimate or inappropriate devices to the network.
- **Power outage:** Networks devices require electricity to run. Power outages can bring harm to such devices and thus affecting the network.

According to Maertn Perlin (2012), In September 2010, Virgin Blue's airline's check-in and online booking systems went down. Virgin Blue suffered a hardware failure, on September 26, and subsequent outage of the airline's internet booking, reservations, check-in and boarding systems. The outage severely interrupted the Virgin Blue business for a period of 11 days, affecting around 50,000 passengers and 400 flights, and was restored to normal on October 6.

Customers of Virgin Blue were thus subjected to major inconvenience, during an outage that lasted up to 11 days. The outage produced a lot of negative press coverage, as well costing the company millions of U.S Dollars in profits. This clearly shows negative perception/reputation that can come along with a system failure towards customers.

Reputable studies have concluded that as much as 75% of downtime is the result of some sort of human error (Robert McFarlane (2016)). Therefore this raises the question, what could be the cause of such human errors? In commenting on the report, MacFarlane indicated that it is often understood to be due to lack of training, but even the highly trained personnel still do make mistakes when working in a rush and/or working while being distracted or taking a shortcut due to impossible deadlines etc. The solution to this as the author saw it was that it all probably leans toward lack of planning. The author also indicated that the argument that many things can lead to human mistakes, simply because they are illogical in their layout, poorly labeled (if labeled at all) and generally tend to facilitate human error. This implies an insight that most can take for granted but end up being the root cause of system downtime.

White paper contends focusing on address the common server failures and human errors that cause 73% of downtime, organizations must adopt a business continuity strategy that prevents

downtime and protects against data loss (Stratus Technology (2014)). Simply put, if a “recovery” is necessary, that implies damage has already been incurred. Prevention is a sensible way to avoid costly damages in the first place. The following is how stratus elaborated the two terms;

- **Business Continuity:** Disaster deterrence that enables an organization to uphold business operations during a crisis.
- **Disaster Recovery:** The process of reinstating infrastructure purpose following a crisis (above all needed in the absence or crash of a BC plan).

Emphasis is that prevention is better than cure as preventions diminish downtime possibilities.

During a network downtime, **unrecoverable partial failures** are a combination of network protocols and network hardware problems that don't cause a complete failure. Network hardware and protocols usually work as expected in the case of complete failure, such as a line card outage, power loss to one half of a redundant pair, etc. (Bigelow, Goolsbe (2016)). The authors continued to stress that, where things go really wrong is when components continue to partially work while in the process of failing. While this most often happens with network hardware, similarly at time it can be seen with partial failures in electrical switch gear and uninterruptable power supply equipment causing downtime, such as the loss of a single phase in a three-phase distribution system. When comparing, to **pilot error** it was stated that this can almost always be traced back to either a lack of a comprehensive checklist for a particular procedure, or some deviating from an existing one.

The authors continued stating that there are tangible and intangible costs of downtime which are expensive. But beyond the financial implications, it is mentioned that there is also a loss of credibility and trust, as when a system goes down, both of these erode rapidly and take much longer to rebuild. The authors then closed by mentioning that the best way to mitigate system downtime is communication. Stating that an organization should have a communication strategy and use it and also customers are to be trained to expect it on a particular channel. Making sure that there is an out-of-band backup is vital. He explained that an organization that communicates well is more likely to put its credibility and trust intact.

The first step in mitigating any downtime is planning. That is if an outage arises and there is no plan for it, it can engender some harmful extended results (Kleyman (2015)). Being well trained

and/or organized for an emergency creates a more stable environment when the need for a disaster recovery solution arises. Planning, testing and actual execution of a disaster recovery plan will help any environment to be ready for emergencies. That is the more redundant and prepared an environment is, the better it can handle an emergency outage. According to Kleyman, a stable environment creates a stable workflow for both staff and data. The author continued stating that although It's almost impossible to plan for everything, being as ready as possible will help reduce the amount of things that can go wrong. That is when an outage occurs, it provides for an environment to resolve the situation as quickly as possible. Another point by the author is that given the opportunity, documentation of all activities and events should be carried out, by noting the point of failure. That is component(s) or equipment affected, what necessitates repair, how it should be auctioned and the final result. This documentation then requires embedding into an existing disaster recovery plan.

Purchasing of cheap equipment can ultimately be less cost effective in the long run due to reliability issues (Kleyman(2015)). The author continues, advising that it is critical to review all aspects of total ownership cost before committing to financial outlay. For instance spending to invest on more expensive but reliable power supply and power distribution units help protect hardware in case of a power surge. Many organizations will face database, software, and hardware downtime in spite of their progress in infrastructure strength. This therefore has made system downtimes somehow acceptable, almost as expected aspects of enterprise life (Gutman, Perlin (2012)).

On the 16th of May 2017, the Botswana government was forced to shut down all of its service as a computer virus by the name WannaCry that by then was sad to have hit over 150 countries became a serious threat to the country. A statement by the Ministry of Transport and communication informed members of the public about the virus, indicating that the government is taking necessary precautionary steps to secure all of its systems whose integrity could have been adversely affected. Such a step of an intentional network downtime meant that certain service offered to the public through government offices were not available for the period. Such service included but not limited to immigration and passport control services, court records management system (Tebele, 2017).

According to Africa Times, Botswana was one of the Five African nations listed among the Top 10 global ransomware vulnerable countries in a November 2016 report by Checkpoint Software Technologies and Botswana was in first place (Africa Business, 2016).

2.3 Aims & Objectives

Aims: The aim of this project is to investigate the problems of Government network services system downtime from a Botswana perspective.

The focus is on factors to be considered when securing a Local Area Network (LAN) of a government department(s) in order to see that digital information assets are protected through confidentiality, integrity and assured availability both within and between government departments, thus seeking any solutions that may be applied.

Objectives:

The Objectives, Tasks and Deliverables are listed below:

Objective 1: Identify common causes of system downtime in government.

Task: Critical review of existing relevant literature.

Deliverable: A cross referenced list of common cases and their severity ratings.

Objective 2: To investigate methods of mitigating downtime outages.

Task: Distributed question to relevant network stakeholders.

Deliverable: Best practice guide to amelioration of disruptive services.

Objective 3: To identify customer perception of service downtime.

Task: Distributed questionnaire to relevant network users.

Deliverable: Relevant data of customer perceptions.

Objective 4: Analysis of primary and secondary data.

Task: Correlation of system downtime with mitigation and customer perceptions.

Deliverable: A tabulated set of common predictable effects and reactions.

Objective 5: To formulate a set of recommendations.

Task: Triangulation of results with published research.

Deliverable: A set of best practice recommendation covering the following:

- Recommendations on ways to build redundancy into the network in anticipation of breakdowns.
- Standardizing hardware and software to keep maintenance costs in check.
- Disaster recovery plan to be in place in case of network downtime.
- Ways to allow or have room for future growth.

Chapter THREE Methodology

3.1 Research Methods Chosen

The Hybrid Method shall be the research method to be used to collect data, as it is a methodology that comprises more than one research methods and these research methods complementing each other. The hybrid method encompasses both the quantitative and qualitative techniques.

The quantitative technique applies mainly when quantifiable data is collected and evaluated. That is, quantitative techniques/method focuses on investigating on something that can be measured and/or observed. The technique addresses such questions as “how often?”, “how many” or “how much?” (Mujinga,2012). The qualitative technique however emphasizes on expressive facts collection other than quantities. That is, it focuses on collecting comprehensive information of individual behavior as well as the details administering that particular behavior.

Use of more than one method and/or technique can be vitally important provided either method complements the other. That is, the benefit is that one method/technique brings out extra proof on the other method and assist in responding to challenges that probably could have never been able to be addressed by a single method (Creswel et al 2011).

A rigorous survey will be done at all stages of the project but most importantly during the data gathering stage that is when a more comprehensive survey will come to play.

The Survey: A rigorous survey shall be carried out, focusing at the network administrators/support of several government departments, normal system users and general clients as an effort to collect relevant information. The following 2 methods shall be used as an effort to try and have convenient options which can reach out to the interviewees on their availability. Both methods will be considered so that they may balance each other, where one is limited:

Questionnaire: A series of carefully designed questions shall be written. These questions will be closed questions with answers ranked according to numerical scale. This method shall be used as it allows minimal contact with the participants, multiple contact avenues and participants can

answer readily recorded inform questions and that can be readily analyze using standard techniques.

Both Online (soft copied) and hard copied (Paper based) questionnaire shall be used. The online questions will be targeting those who have access to computer and/or those who have access to Google questionnaire tool as the Google survey tool will be used. The paper based or hard copied questionnaires will be targeting those who do not have access to computer and/or do not have Google email accounts.

Interview: This is an oral fact finding method, where the researcher will be asking question and the participants responding by answering. This is a standard method as it may be done with less/no contact as a telephone may be used. Same form of questionnaire shall be used to guide the interviewer but an interactive session will be guide the interview as at times the interviewee raised critical points that prove vital to the project. In order to conduct successful interview the researcher will be focusing on the two types of interviews which includes: The Structured Interview and The Unstructured Interview.

The Structured Interview: These can be implemented either face-to-face or via telephone using a standard set of carefully formulated questions to obtain data. Similar questions shall be given to different participants or interviewees of more or less the same expertise or those that are similarly affected and the data later rigorously analyzed. Standardized question shall be either open-ended or closed-ended. A structure interview may be interpreted as a standardized interview or a researcher-administrated survey which is a quantitative research method commonly employed in a survey research with the aim to ensure that each interview is presented with exactly the same questions in the same order. Candidates are asked the same questions, evaluated using a common rating scale and interviewers are in agreement on acceptable answers (U.S. Office of Personal Management 2008).

The Unstructured Interview: This is effectively done in a face-to-face format in some kind of story sharing and candidates are later asked questions. In this method a standard rating scale is not required and interviewers do not need to agree on acceptable answers or predetermined answers. In this method the interviewer/researcher has to provide a conducive environment that will see the interviewee being guardedly allowed to dominate the interview. Although such an interview is not as effective and reliable as the structure, the researcher may benefit by sourcing

some key areas that may have been overlooked but key to the research (U.S. Office of Personal Management 2008).

Survey strategy: As an effort to try and ascertain that these methods become successful, follow up will be carried out through telephone, email or any media which the person identified for interviewing is comfortable with. Telephone follow ups will be the core means of backup. That is in case any interviewee fails to complete the emailed questionnaire, and oral telephone interview conversation will be carried out.

As part of the strategy, core or relevant candidates whose input will be identified as vital to this project will be visited by the researcher in person. Appointments will be made and the researcher will go and do a face to face interview. As already stated identified people or those regarded as core by the researcher will be visited as the researcher believes an interactive oral interview can be beneficial as it can identify some key area that may be overlooked.

Online Google Docs survey will be used. Emails will be the primary tool used to communicate to all targeted people to be surveyed. The emails will be clearly stipulating the reasons/objectives of the research.

Another form of delivering questioners to those identified will be sending people to hand deliver the questioners where relevant. The questionnaires are to be completed and given back to those that have been requested to deliver them. An email requesting for an appointment for such meetings will be sent followed by telephone calls in case the targeted person does not respond to the email.

Hand in deliveries will be used as a last resort as it comes with a monetary cost. Those who are to deliver these questionnaires will require to be paid for their services. Therefore this will be budgeted for.

Identifying and recruitment of different stakeholders that are affected by the system will be done. They are categorized as:

Technical Users: These are the people who work in the network system directly or in the backend. They may include System administrator and network technicians. These are the people who have the technical knowledge of how a network operates and they may be working directly

or indirectly in a government network. These people should not necessarily be currently employed by the government, they should have somehow have worked on the government network. It may be as outsourced support or as government employed network/computer administrators. The Department of Information Technology (DIT) management will be contacted to try and make interview arrangement with government network administrator and also learn of who are the key outsourced companies that assist with administering the government networks in different departments if any.

Users: These are normal government employees who use the network daily as they service the government clients. They normally are not technical and therefore no nothing/less about network technical issues. Appointments should be done with the government HR or managers of different departments to make request to conduct such survey.

Clients/Customers: These are the people that are serviced and they only come to service and are not directly in contact with the systems but are affected by any system failure as they are delayed to be serviced. These will be targeted randomly as in Botswana everyone uses government services.

Data Analysis

The survey data analysis will be automated when using the Google. As there may be a chance that some data may be manually collected this might need manual analysis as well. Therefore after completed questioners are collected and/or received from the relevant targeted people the data collected will have to be transferred from the questionnaires into spreadsheet software for analysis. That is a simple grid in the spreadsheet software with a designed coding system will be used to collect all data provided in by questionnaires. Data will be entered on to the grid to calculate the proportion of respondents answering each and every category of each question.

The Formula will be to calculate average and standard deviations for the questions ranked. To further some more, the relationships in the data will be explored. For example, between challenges perceived obvious or regular network issue and complex issues. As an effort to try and come up with more accurate analysis the responses may be pooled to number related questions. That is answers must conform to a consistent numerical code and therefore the score will be summed up over the question. This will be another form that according to Munn and

Drever (1999) and Burns (2000) is regarded more accurate analysis than computing an average score. That is both methods will be considered in this research.

Questionnaire Design

There shall be 3 questionnaire designed and they shall be the Technical questionnaire, the Users questionnaire and the Client questionnaire. The research has opted for such, as the three do not interact with the system in the same way and are differently affected by system downtime.

3.2 Justification

As an effort to try and identify the common causes of the system downtimes in the government departments a survey was conducted in at list five government departments targeting at list 20 people. More than 50 technically sound people who are working or have worked for government departments either as employees of the government or working for companies contracted to the government are identified or were given a technical questionnaire. That is Relevant questionnaire focusing on relevant user are drafted focusing on how the user interacts with the system. Therefore these are the three types of questionnaires:

The Technical Questionnaire: This can be described as the core questionnaire since it was targeting the technical people such as the network administrators, helpdesk technicians. The questionnaire is focusing on soliciting technical issues that lead to network down time. These are normally ICT skilled professionals who work with the backend. Their questionnaire will be mostly technical. The questionnaire shall be aiming do address Objective 1 and objective 2.

Question 1: Please choose your relevant education level:

Education levels are listed for the candidate to choose from. This question shall help in determining whether the education/skill levels is one of the factors that leads to network downtimes in government departments. This could be due to poor skill sets in supporting or building systems/networks. The options listed with check box format will be as follows:

- Certificate level
- Diploma level
- Degree level
- Masters level
- Cisco Certifications
- Microsoft Certification
- Oracle Certification
- Others _____

Question 2: Please specify the government department you working under?

Since at least three government departments will be surveyed, the question shall identify which department the participant is from to help in observing is the problem is across different departments or is in just a single department. A participant will choose from the following:

- DIT
- DRTS
- Ministry of Labour

Question 3: How often do you normally experience system/network downtimes in the department(s) you working for?

The question looks at identifying the how often the downtimes are normally experienced in government departments. This will help the research know or identify the severity of the downtimes. The following answers were given with radio buttons to choose from.

- Daily
- Weekly
- Monthly
- Quarterly (3 Months)
- Yearly

Question 4: What are the common factors that lead to network downtimes in your department?

This looked at identifying the core causes of system downtimes. Common causes are listed for participants to choose from with an option of adding any other cause. The following are the listed common cause with check boxes to enable participants to choose more:

- Power Outage
- Rogue Equipments
- Device Faults
- Misconfigured Router
- Broadcast Storms

- Server Overloading
- Poor Switch Allocation
- Unnecessary Protocols

Question 5: What are the common attacks experienced in your network?

The question will assist the researcher in knowing/understanding how secure the network is and thus relate if such attacks are the reason for downtimes or not. The following are the possible choices for the participants to choose from:

- DNS problems
- Poor or bad cabling
- Slow application performance
- Printing problems
- Duplex mismatch
- Dead drop
- IP addressing issues
- Excessive network collisions
- Software problems
- Others _____

Question 6: Is your network secured with an antivirus?

This will assist the researcher in knowing if indeed the government networks are secured with basic security mechanisms. The following are the options to select from:

- Yes
- No
- May be

Questions 7: What are the measures put in place to secure the government networks?

The question shall assist the researcher in knowing if the security measures put in place to secure government systems/networks. The options for the participants to select from are as follows:

- Firewalls
- SSH Keys
- VPNs and Private Networks
- Public Key Infrastructure and SSL/TLS Encryption
- Service Auditing
- File Auditing and Intrusion Detections Systems
- Isolated Execution Environments
- Others _____

Question 8: How often are you and/or your team trained on network security technologies?

This shall help the researcher in identifying the competence of the technical user in the modern network security technologies. The following are options:

- Regularly
- Sometimes
- Never

Question 9: What is the longest time you have experienced system downtime in your department?

This shall assist the researcher in understand the severity of the network downtimes. The following are the options the participants should choose from:

- 1 hour or less
- 4 hours or less
- 8 hours or less
- 24 hours or less
- 48 hours or less
- More than 48 hours

Question 10: What is your average turnaround time in resolving system/network downtime by your department?

This shall assist the researcher in understanding if longer system downtimes are caused mainly by poor technical skills or poor planning. The following are the options for participants to choose from:

- Within 30 minutes
- Within 1 hours
- Within 8 hours
- Within 24 hours
- Within 48 hours
- Others _____

The User Questionnaire: These are those who use the system or interact with the system through an interface (User Interface) to extract information that benefits clients. The questionnaires are less or not technical but mostly will try revealing their technical knowledge on basic technical issues. Objective 1 shall also be address through the feedback from these questionnaires.

Question 1: How often do you normally experience system/network downtimes in the department(s) you working for?

The question looks at identifying the how often the downtimes are normally experienced in government departments. This will help the research know or identify the severity of the downtimes. The following answers were given with radio buttons to choose from.

- Daily
- Weekly
- Monthly
- Quarterly (3 Months)
- Yearly

Question 2: What are the primary causes of the system/network downtimes in your department?

The user's perspective on what primarily causes system/network downtime is critical for the research as relevant suggestions can be put forth by the researcher. The following are the options listed:

- Technical Issues
- None Technical issues

Question 3: What is the longest time you have experienced system downtime in your department?

This shall assist the researcher in understand the severity of the network downtimes. The following are the options the participants should choose from:

- 1 hour or less
- 4 hours or less
- 8 hours or less
- 24 hours or less
- 48 hours or less
- More than 48 hours

Question 4: What is your average turnaround time in resolving system/network downtime by your department?

This shall assist the researcher in understanding if longer system downtimes are caused mainly by poor technical skills or poor planning. The following are the options for participants to choose from:

- Within 30 minutes
- Within 1 hours
- Within 8 hours
- Within 24 hours
- Within 48 hours
- Others _____

The Client Questionnaire: The less important but necessary questionnaire which its primary objective is to try and identify the perception of the clients towards the system downtime and as clients perspective will assist in solidifying the necessity to act towards improving/reducing the downtimes. Objective 3 shall be fulfilled by feedback from this questionnaire.

Question 1: How often do you normally experience system/network downtimes in the department(s) you working for?

The question looks at identifying the how often the downtimes are normally experienced in government departments. This will help the research know or identify the severity of the downtimes. The following answers were given with radio buttons to choose from.

- Daily
- Weekly
- Monthly
- Quarterly (3 Months)
- Yearly

Question 2: What are the primary causes of the system/network downtimes in your department?

The user's perspective on what primarily causes system/network downtime is critical for the research as relevant suggestions can be put forth by the researcher. The following are the options listed:

- Technical Issues
- None Technical issues

Question 3: What is the longest time you have experienced system downtime in your department?

This shall assist the researcher in understand the severity of the network downtimes. The following are the options the participants should choose from:

- 1 hour or less
- 4 hours or less

- 8 hours or less
- 24 hours or less
- 48 hours or less
- More than 48 hours

Question 4: What is your average turnaround time in resolving system/network downtime by your department?

This shall assist the researcher in understanding if longer system downtimes are caused mainly by poor technical skills or poor planning. The following are the options for participants to choose from:

- Within 30 minutes
- Within 1 hours
- Within 8 hours
- Within 24 hours
- Within 48 hours
- Others _____

Question 5: Which of the following service type would you prefer the government departments to adopt?

This is to try and understand the level of satisfaction or desertification by clients with regards to computerized services as network downtimes are the key hindrance to effective services. The following are the options:

- Manual
- Computer based
- Both

3.3 Research Procedures

Questionnaire Design

Both the open and closed ended questions were open for use in designing questions used for the three users although the closed ended questions dominated. In designing the questions the research was aware of the scale questionnaires which are used for choosing statements from strongly disagreeing to strongly agreeing. The research simplified the scale to 1 to 5 as a way of simplifying choices although according to Buttle (2006), the 7 point likert scale is the most reliable as there are more point scale that helps avoid being too neutral.

Data collection Validations

The Google Docs questionnaire was used as the primary method to collect data. This was chosen as an effort to bring reliability and validity on results as the Google Docs does data analysis automatically. Moreover a pilot study was carried out to ascertain or legitimize data as this helped the researcher identify the relevance of the questionnaire. This was carried out by sharing the relevant questionnaires with 4 Technical Users, 10 Users and 10 Clients/Customers. The pilot study helped the research to reduce the number of questions and the use of simple concise language.

Data Collection and Analysis

A Google Docs questionnaire was the ultimate choice of data collection and analysis as the researcher could not afford other means. Means such as hardcopy questionnaires meant that the researcher had to embark on visitations to targeted participants and/or hiring of research field assistants and all these would be at a price thus choosing Google Docs questionnaire. Other means such as the survey monkey were strongly considered as well but the cost issue refrain the researcher from embarking on the use of the survey.

Therefore the when using the Google Docs survey the researcher sourced emails of targeted participants and fortunately the government of Botswana emails are Google compatible as the participants could be able to access Google Docs through their emails. All of the government employees which mostly comprised of the Technical User and the users were sent designed

Google Docs questionnaires. The researcher selected 100 of his email contacts who he was sure have used the identified government departments services as clients/customers. By choosing those who are already in the researches contact list this brought forth a higher probability of response rate. The results received were automatically analyzed by the Google Docs. The research did consider the use of other software such as Microsoft Excel, Statistical Package for Social Science (SPSS) but the analysis done by the Google was sufficient. This is because the Google Docs provided accurate analysis immediately and thus saved time as some responses came very late.

Sample Size Techniques

The research population is represented by four sources, namely the Technical User, the ordinary user, the client and relevant literature. For both the Technical Users and Ordinary user, the questionnaire survey was done on the following government departments; The Department of Information Technology (DIT), the Department of Roads Transport and Safety (DRTS) and the Ministry of Labor and Home Affairs (MLHA). A total of 50 Technical Users and 50 ordinary users were targeted from all the three government departments.

When targeting government clients, the participants were chosen by chance, meaning that every person who is a Motswana and has used government services could have been picked and at least 100 users were to be interviewed.

The two sampling techniques used are the probability sampling and none probability sampling (Zikmund, 2003). The researcher opted for none probability sampling technique's convenience sampling which makes use of available participants thus affordable and quick. The probability sampling means that every targeted populations element should be equality chosen and assumptions made to generalize such choice.

Although the overall sample study for the research is 200 participants and that 3 government departments were picked, the researchers' confidence is entirely this is at a balance. Balanced sample is regarded as the best criterion for evaluating adequacy of sampling (Pattern, 2004). Through this study the research is confident that more than 90% of the research is accurate.

Privacy

Confidentiality of participants' feedback is very vital as some questions feedback in the questionnaire may bring conflict between Technical users and user and/or clients/customers and government. That is when different users who are affected differently by the system are questioned with the same way there may be different answer.

It is therefore vital for the researcher to clearly explain the importance of such feedback with proper analysis of the feedback. The researcher shall see that the no individual participants' feedback is quoted but rather a collective feedback.

3.4 Ethical Considerations

The researcher is aware of the moral principles which guide a research activity. Therefore the researcher has not and will not disclose any information to public without the participants' consent.

The researcher abides to the highest level of professionalism by:

- Treating those affected or associated with research with high level of respect.
- Clearly stipulating and explaining the Informed consent in questioners.
- Give those that were participating during interview to review the findings as well.
- Keep personal information if any highly confidential.
- Ensuring that everyone's' work used during the research is acknowledged.
- Adhere to ethical standards laid by professional bodies.

Lastly the researcher diligently abides by the Data protection as per the advice for T802 student as a way to complying with the Data Protection Act.

Risk Assessments

There are no direct risks identified in carrying out this project but the indirect risks. The indirect risk is that the researcher required field research assistants in carrying out some questionnaire follow ups. This is considered a risk as they are a third party knows participants information.

Therefore the researcher carefully selected assists with high ethic courtesy.

Chapter FOUR Analysis and Interpretation

3.2 Results

Data was collected from three stakeholders that directly/indirectly work with government system/network. These stakeholders/participants include the Technical User, the User and the Customer/Client.

Technical User: The participant has computing/networking technical skills and has worked with the government network for some time. This includes the Network Administrator, System Analyst, Computer Technicians, Help desk Technicians as well as companies that support the government system/network.

The User: These are government employees who use the system or network on daily basis to assist the government clients. These are receptionists, help desk people, general officers, managers etc.

The Customer/Client: These are the people who are being serviced, they include the citizens, and any other person who requires assistance from government department and they get it through the use of computer system.

The results which from two research techniques stated in the previous chapter are now revealed in this chapter. The collected data is influenced by the objectives and answers the research questions.

3.2 Summary of data Collection

Data collection was carried out by the use of questionnaires and Interviews. The questionnaire was the primary data collection tool, therefore it was sent to almost all of the participants. A Google Docs questionnaire was developed and shared with all the targeted participants. The interview was a secondary tool used to compliment the questionnaires. That is, participants who could not be reached were followed up with a questionnaire and these were mostly participant targeted. These were key participants who the researcher felt that their input was critical to the success of this project and thus followed. This was done because an interview supports questionnaires in that it can be more elaborative. The researcher and the research filed assistants conducted these follow ups with a hardcopy.

Shared Questionnaire Result Summary

#	PARTICIPANT	SHARED	RECEIVED	%RESPONSE
1	Technical User	50	27	54%
2	User	50	32	64%
3	Clients/Customers	100	48	48%
4	TOTAL	200	107	54%

Table 4.2.1: Shared Questionnaire Result Summary

A Google Docs Questionnaire was shared to a total of 200 participants that comprised of Technical user, use and customer. Only 53.5 percent of the shared questionnaires were received back making only 107 participants. The above table clearly indicates in detail how the participants targeted responded. In general over 50 percent of participants responded and this was a positive feedback as the researcher wanted a 50percent response rate from each of the participants groups targeted. The only group of participants that the response rate was below 50 percent was the client/customers. Although the research hoped for at least 50 percent, the 48 percent response rate is acceptable as the researcher sees the client/customer input in this research as less critical as compared to that of the technical users and users.

The researcher observed the following as challenges that may lead poor response:

- Technical Users are mostly found in the Department of Information Technology (DIT) and their duty is to support other government departments as well thus they are rarely available to work complete questionnaire or access their emails.
- Users were not all aware of the questionnaire as some feedback that the researcher received was that they did not know how to access the questionnaire.
- The clients/customers' primary challenge was that they rarely access their email addresses. Other the observation is that they could not identify the link to guide them to the questionnaire.

Shared Interviews Result Summary

#	PARTICIPANT	TARGETED	CONTACTED	%RESPONSE
1	Technical User	10	8	80%
2	User	0	0	0%
3	Clients/Customers	0	0	0%
4	TOTAL	10	8	80%

Table 4.2.2: Shared Interviews Result Summary

As the interviews were carried out whenever necessary, 8 participants were interviewed. The 10 targeted participants were mostly experienced technical users across the departments but only managed to interview 8. The research managed to interview 6 highly experienced technical users from Department of Information Technology (DIT), 1 from Department of Roads Transport Services (DRTS) and 1 from the Ministry of Labour and Home Affairs.

Technical User Summary

Questions:

1. Please choose your relevant education level

27 responses

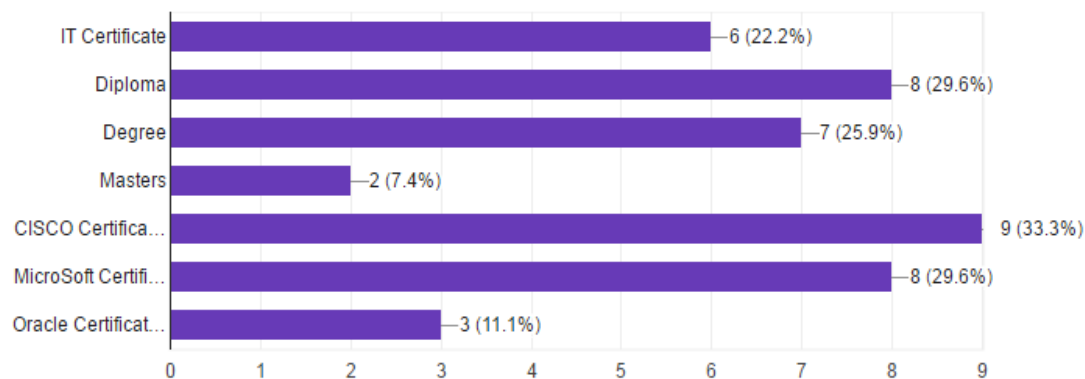


Figure 4.2.1: Technical User Question 1 results

This question was to investigate the skill level or competency of the government technical team. The table above does show that indeed there are various technical competencies within government departments.

2. Please specify the government department you work under

27 responses

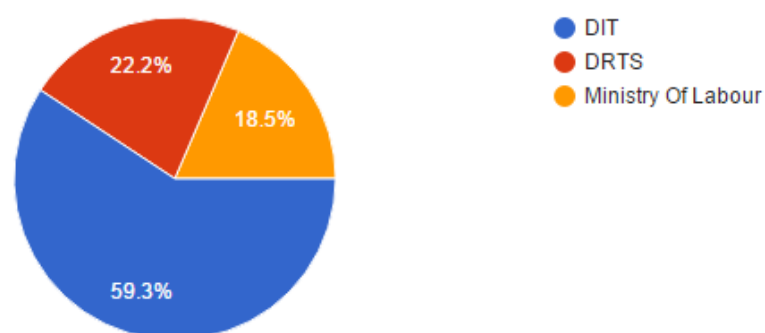


Figure 4.2.2: Technical User Question 2 results

The above Figure (Figure 4.2.2) shows that out of the 27 respondents 59% was from the DIT, 22% from DRTS 19% from Ministry of Labor and Home Affairs. Table 4.2.3 further explains this.

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	DIT	16	53%
2	DSTS	6	60%
3	Ministry of Labor	5	50%
4	TOTAL	27	54%

Table 4.2.3: Technical User Question 2 results

The above table (Table 4.2.3) shows that 50 technical users were targeted but only 27 responded. That is 30 DIT, 10 DSTS and 10 Ministry of Labor responded. In overall only 54% of targeted technical users responded.

3. How often do you experience network/system downtime?

26 responses

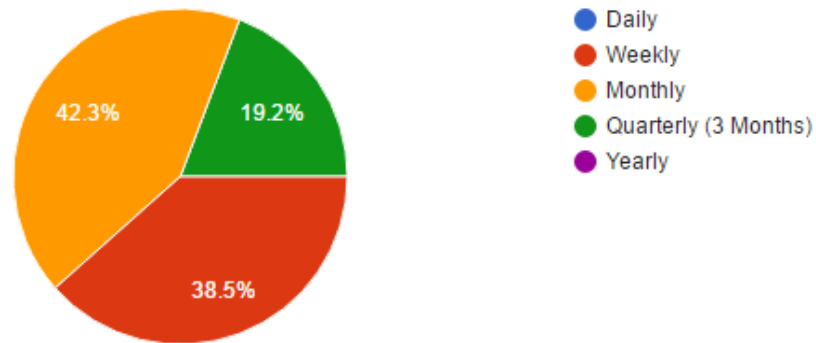


Figure 4.2.3: Technical User Question 3 results

There were 26 responses on only 3 of the possible 5 choices/answers. Although this figure shows that network downtimes are experienced mostly monthly, there is a clear strong perception that network downtimes do occur weekly.

#	POSSIBLE ANSWERS	RESPONSE	%RESPONSE
1	Daily	0	0%
2	Weekly	10	39%
3	Monthly	11	42%
4	Quarterly (3 Months)	5	19%
5	Yearly	0	0%
6	TOTAL	26	52%

Table 4.2.4: Technical User Question 3 results

The above (Table 4.2.4) table clearly shows the technical team system downtime frequency. None of the technical team has is of a view that downtimes do occur neither daily nor yearly. Their perception is that downtimes occur on monthly/weekly.

4. What are the common factors that lead to a network downtime in your department?

27 responses

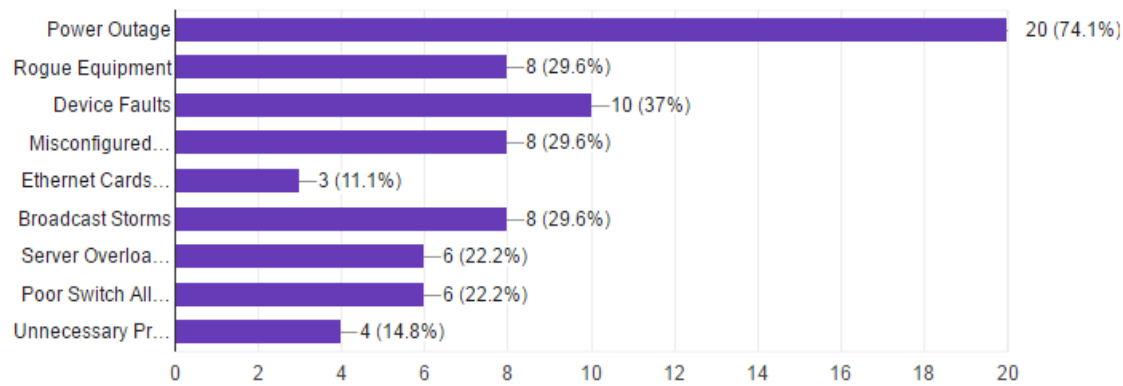


Figure 4.2.4: Technical User Question 4 results

The table above shows that power outage contributes more towards network downtimes.

5. What are the common attacks on your network?

27 responses

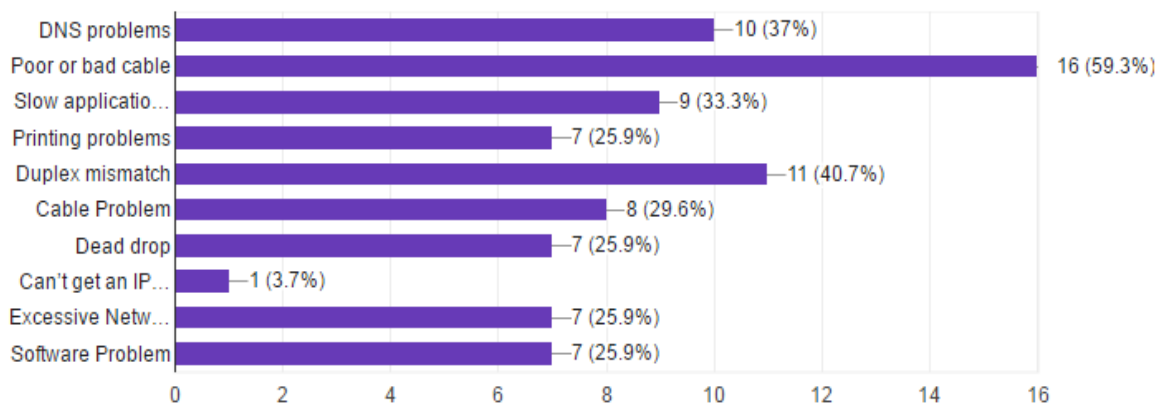


Figure 4.2.5: Technical User Question 5 results

6. Is your network secured with an antivirus?

26 responses

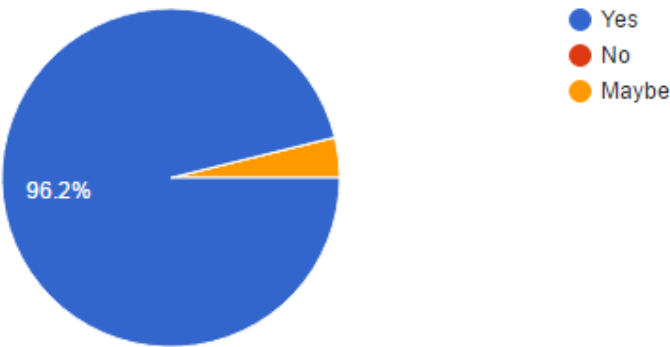


Figure 4.2.6: Technical User Question 6 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	Yes	25	96%
2	No	0	0%
3	Maybe	1	4%
6	TOTAL	26	52%

Table 4.2.5: Technical User Question 6 results

7. What measures has been put in place to secure your network?

27 responses

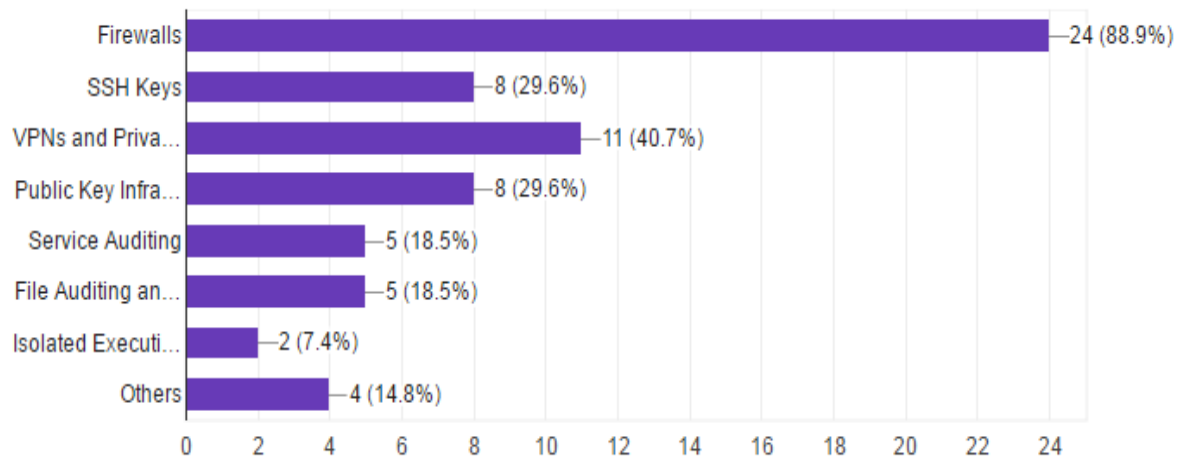


Figure 4.2.7: Technical User Question 7 results

8. How often are you and/or your team trained on network security technologies?

26 responses

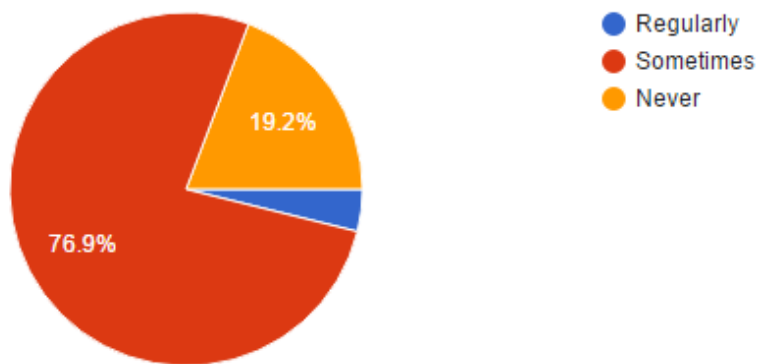


Figure 4.2.8: Technical User Question 8 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	Regularly	1	4%
2	Sometimes	20	77%
3	Never	5	19%
6	TOTAL	26	52%

Table 4.2.6: Technical User Question 8 results

9. What is the longest time you experienced system downtime in your department?

27 responses

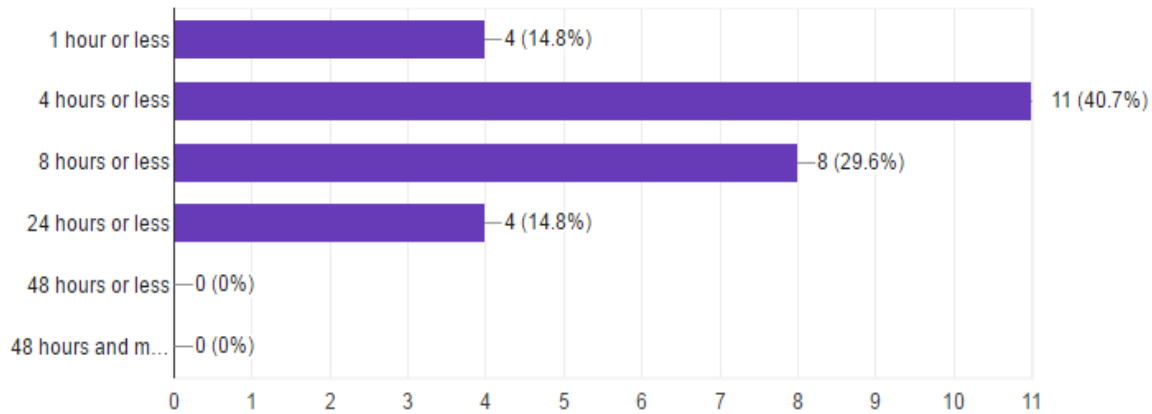


Figure 4.2.9: Technical User Question 9 results

10. On average what is the turnaround time for resolving network failure in your department?

27 responses

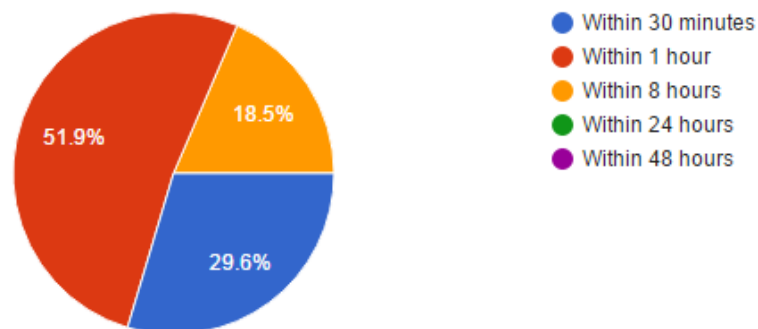


Figure 4.2.10: Technical User Question 10 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	Within 30 minutes	8	30%
2	Within 1 hour	14	52%
3	Within 8 hours	5	18%
4	Within 24 hours	0	0
5	Within 48 hours	0	0
6	TOTAL	27	54%

Table 4.2.7: Technical User Question 10 results

User Summary

Questions:

1. How often do you experience system/network downtime in your department?

32 responses

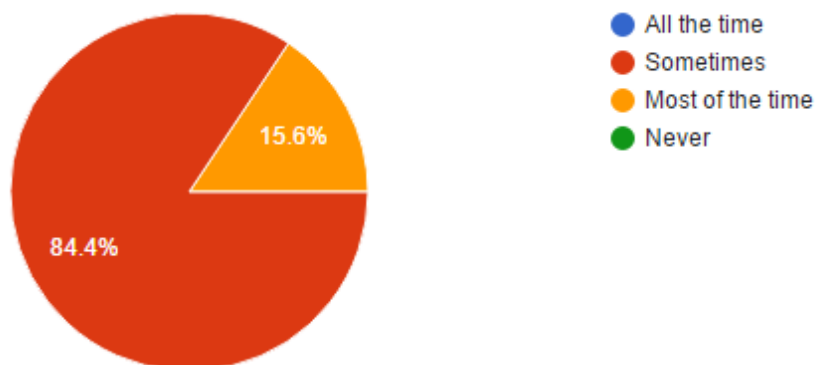


Figure 4.2.11: User Question 1 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	All the time	0	0%
2	Sometimes	27	84%
3	Most of the times	5	16%
4	Never	0	0
5	TOTAL	32	54%

Table 4.2.8: User Question 1 results

2. What are the primary causes of network/system downtime?

31 responses

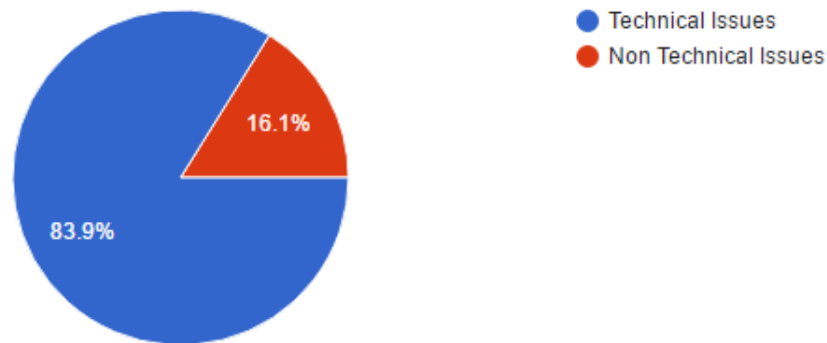


Figure 4.2.12: User Question 2 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	All the time	0	0%
2	Sometimes	27	84%
3	Most of the times	5	16%
4	Never	0	0
5	TOTAL	32	54%

Table 4.2.9: User Question 2 results

3. What is the longest time you experienced system downtime in your department?

32 responses

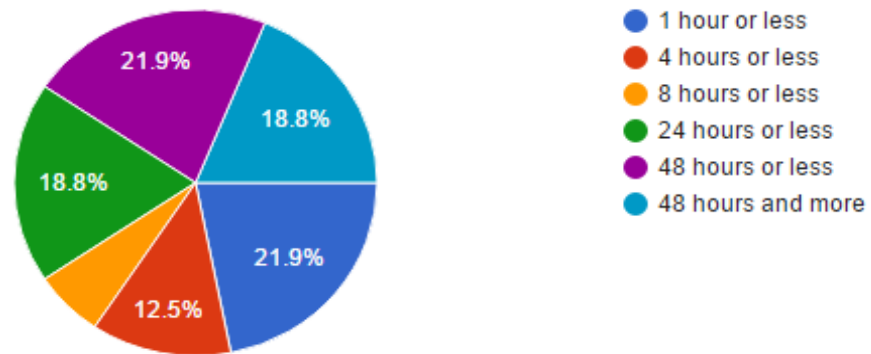


Figure 4.2.13: User Question 3 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	1 hour or less	7	22%
2	4 hours or less	4	13%
3	8 hours or less	2	5%
4	24 hours or less	6	19%
5	48 hours or less	7	22%
6	48 hours and more	6	19%
7	TOTAL	32	54%

Table 4.2.10: User Question 3 results

4. On average what is the turnaround time for resolving network failure in your department?

32 responses

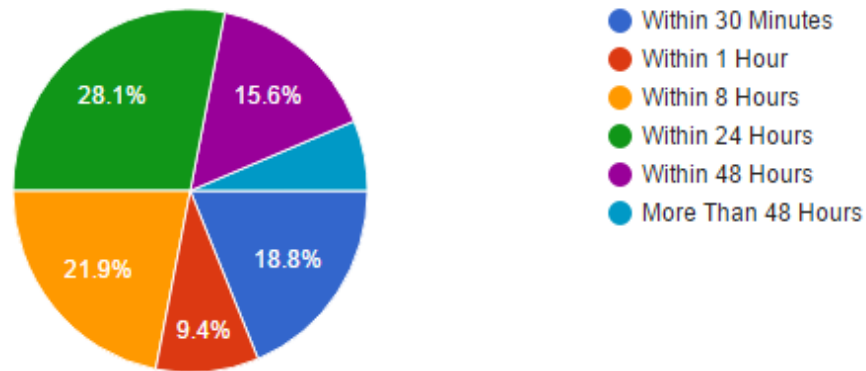


Figure 4.2.14: User Question 4 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	Within 30 Minutes	6	19%
2	Within 1 Hour	3	9%
3	Within 8 Hours	7	22%
4	Within 24 Hours	9	28%
5	Within 48 Hours	5	16%
6	More than 48 Hours	2	6%
7	TOTAL	32	54%

Table 4.2.11: User Question 3 results

Customer Summary

Questions:

1. How often do you experience system/network downtime when visiting government departments?

48 responses

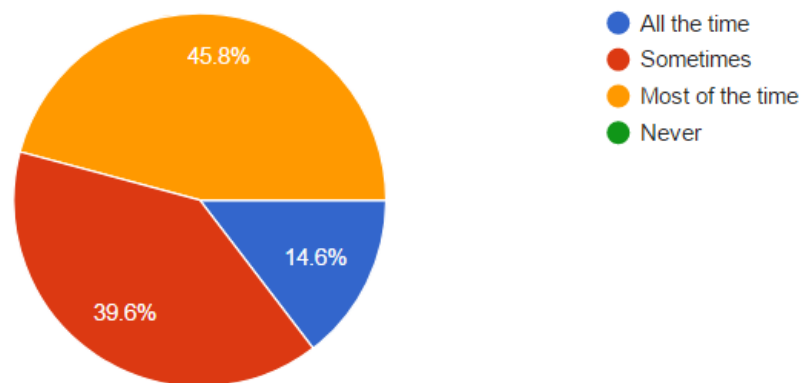


Figure 4.2.15: Client/Customer Question 1 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	All the time	7	15%
2	Sometime	19	37%
3	Most of the time	22	46%
4	Never	0	0%
7	TOTAL	48	96%

Table 4.2.12: Client/Customer Question 1 results

2. What are the primary causes of network/system downtime?

48 responses

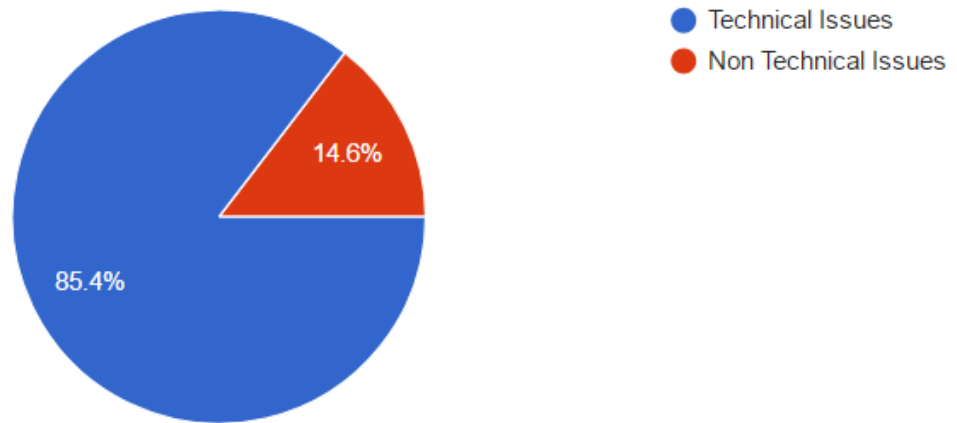


Figure 4.2.16: Client/Customer Question 2 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	Technical Issues	41	85%
2	None Technical Issues	7	15%
7	TOTAL	47	96%

Table 4.2.13: Client/Customer Question 2 results

3. What is the longest time you experienced system downtime in the government department?

48 responses

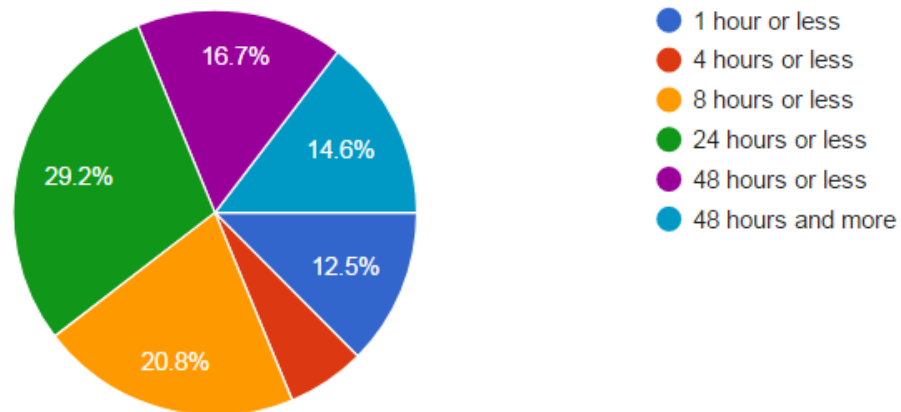


Figure 4.2.17: Client/Customer Question 3 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	1 Hour or less	6	12%
2	4 Hours or less	3	6%
3	8 Hours or less	10	21%
4	24 Hours or less	14	29%
5	48 Hours or less	8	17%
6	48 Hours or more	7	15%
7	Never	0	0%
8	TOTAL	48	96%

Table 4.2.14: Client/Customer Question 3 results

4. On average what is the turnaround time for resolving network failure in the government department?

48 responses

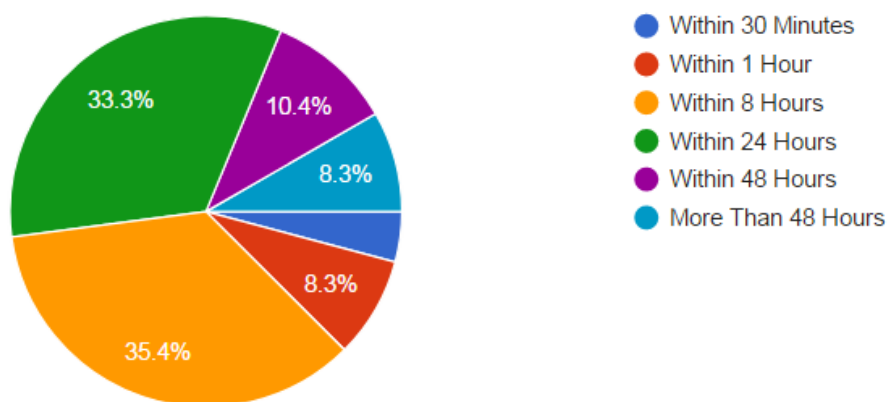


Figure 4.2.18: Client/Customer Question 4 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	Within 30 minutes	2	4%
2	Within 1 Hour	4	8%
3	Within 8 Hours	18	37%
4	Within 24 Hours	16	33%
5	Within 48 Hours	5	10%
6	More than 48 Hours	4	8%
7	TOTAL	48	96%

Table 4.2.15: Client/Customer Question 4 results

5. According to you which of the following services would you prefer government to adopt?

48 responses

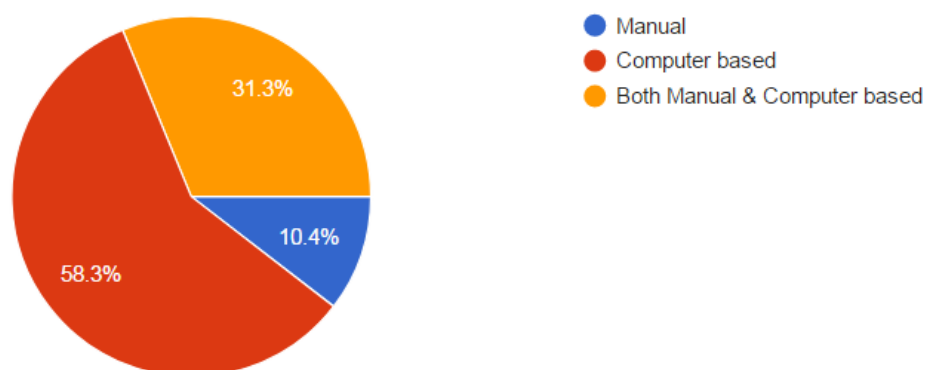


Figure 4.2.19: Client/Customer Question 5 results

#	POSSIBLE ANSWERS	RESPONSES	%RESPONSE
1	Within 30 minutes	2	4%
2	Within 1 Hour	4	8%
3	Within 8 Hours	18	37%
4	Within 24 Hours	16	33%
5	Within 48 Hours	5	10%
6	More than 48 Hours	4	8%
7	TOTAL	48	96%

Table 4.2.16: Client/Customer Question 5 results

4.3 Results Interpretation

The feedback from both the technical and none technical users clearly shows that Botswana government departments do experience system downtimes frequently. That 84% of the users indicated that they sometimes experience system/network downtimes which can take over two days to resolve (48 hours). The customers reiterated this as 77% of the customer agreed to have experienced system downtime with a turnaround time of over 8 hours. These results confirmed the researcher suspicions and thus justify the importance of this study.

Objective: Identify common causes of system downtime in government.

The results from the questionnaire have successfully satisfied this objective. After the researcher critical reviewed existing relevant literature he listed common issues that may lead to system downtimes. The research question was therefore influenced by the literature.

Power Outages is regarded as the major factor that causes system downtimes in government departments as 74% of technical participants indicated this. None technical users do share the same sentiments although they also strongly stated that 85% of the time technical issues are the ones that causes downtimes. Other common causes include poor/bad cabling, device faults, DNS problems, poorly configured routers and many more.

It is expected that most if not all of these causes be dealt with as the feedback clearly shows that the team is well educated as more 30% of the team are diploma holders and more than 30% do hold professional certifications such as Cisco certificate. But the research clearly shows that team is rarely trained as over 75% of participants indicated that they are sometimes trained. This may be the problem core as the team may be lacking in terms of new security technologies.

Objective: To investigate methods of mitigating downtime outages.

The following are the approaches that government departments can take to mitigating downtime outages looking at the results:

- The government should adopt using an off-site systems hosting facility as an alternate data center. This should be able to be brought online in case of an emergency on government network.
- Every critical device/equipment should have a spare readily available for use.

- Making of scheduled backups and storing them outside of the department should be done at all times. The backups should not be kept in the same location but in a different safe location that will not be affected by the same disasters as the department network copy.
- Technical documentation should be maintained at all time to facilitate recovery as no disaster recovery plan would be complete without documents explaining how to get it done. This helps when severe disaster happen to the network causing the technical team to be inflicted with the drama of a traumatic disaster thus limited personnel. This will thus help as there will be detailed steps to follow.
- Regular testing should be done. This helps confirm that indeed the government department disaster recovery plan does work. That is even the best disaster recovery plan only are effective when tested regularly you will never know equipment does work, how long it takes to restore backup data to a system, or whether there is enough personnel to make the process flow smoothly.

Objective: To identify customer perception of service downtime.

Customers strongly believe that technical issues are the core cause of system/network downtime. This is shown by the 85% who agreed to this during survey and on 15% believed none technical issues are the cause.

The customer feedback shows that it takes at list 16 hours for a network downtime issue to be resolved. Majority indicated that the longest time they were affected by a system downtime was 24hours and the shortest 4 hours.

Regardless of poor feedback by the customers towards how their experiences to downtimes, they still believe that computerized system are effective as 58% agreed with this. A good 31% believe that a combination of both computer base systems and manual should be adopted by the government. Unfortunately 11% indicated their preference of manual system over computer based system.

4.4 Recommendations

The following are recommendations made by the researcher to address objective 5:

Objective: To formulate a set of recommendations:

Recommendation 1: Dealing with Power Outages:

Power outages can be described as a short-term or long-term loss of electric power. To protect computer systems against power outages it is strongly recommended that the government department uses the following devices:

Uninterruptible power supply – UPS: The use of a UPS in a computer network environment provides a constant flow of electricity in case of a primary power supply becoming unavailable for a short period of time. Devices such as computers, routers and switches should each have a UPS. This device works well with an automated back-up generator explained in the following paragraph.

Back-up Generator: This is an automated electrical system that operates as a back-up, generating electricity within seconds of a utility outage. Normally an automatic transfer switch will sense the power loss thus commanding the generator to immediately start by transferring the electrical load to the standby back-up generator which will immediately begin to supply power to the circuits. The back-up generator will continue supplying power until utility power returns. When power returns the automatic transfer switch will then transfer the electrical load back to the utility and thus signaling the standby generator to shut off. It will then return to standby mode where it awaits the next outage.

Surge protector: A device designed to protect electrical devices such as computers, switch and routers from voltage spikes. A surge protector limits the voltage supplied to the electric device by blocking and/or shorting to ground any unwanted voltages that exceeds a safe threshold.

A combination of a UPS, back-up generator and surge protectors is highly recommended to be implemented in each and every government department to deal with the power outage issues.

Recommendation 2: Dealing with Rogue Equipment

It is strongly recommended that proper planning of detecting rogue equipment in government departments be done. It should be noted that when planning for such, it is important that a holistic approach taken as technology alone will not completely address the problem, thus requires a combination of both procedural and technical controls. This is why following of the IEC 27002 standards for help and guidance is very critical. Therefore the following recommendations are derived from the standards:

Physical Security

Barriers should be places around the government departments' networks to restrict who can physically connect to the network infrastructure. This can be achieved by controlling access to cabling and connection points in the network. Physical security measures should be taken seriously by the government by incorporating the every department facilities and including special cabling conduits, locked work areas and equipment rooms. Such measures can be overlooked and a failure in physical security can bring about the same effect level as any other type of security breach that may result in unauthorized network access (solarwinds, 2016).

Implementation of security controls at the network layer as the network layer is a representation of the next logical area of vulnerability and point of incursion. To defend the government network at this level, the following should be done:

- **Identifying of authorized devices**

This will help create device profiles and help in determining which devices are authorized. The use of a centralized port monitoring tool as a device tracker that is able to locate other devices anywhere on your network like switches should be adopted. By tracking such devices it will be easy for them to be profiled and documented. The following are the devices to track and document:

- Every switch and wireless access point nodes in government network
- Every node in the network, profiled by user identification, contact information, physical location, performance summary and capacity metrics.
- All device endpoint inventory connecting the node device should be kept

- **Building of network access controls**

Use of Whitelists should be adopted to help identify and verify which devices are authorized to use the network and to construct access controls. That is only whitelisted devices should be connected to the network and those not whitelisted should not. This should be used with a compatible port monitoring tool and the following will be achieved:

- Detection of potential rogue devices and thus can prevent them from accessing the network
 - Ability to withdraw network access to systems that do not conform to the government security policies
 - Easy removal and/or quarantining of infected systems in the network
- **Monitoring of network connected devices**

This is basically performance, capacity (switch port capacity included) and compliance monitoring.

- Monitoring compliance is achieved by refining of whitelists and ensures that controls are effective in the network.
- Monitoring performance means detecting faults and errors that may affect performance as well as signal malicious activity.
- Monitoring capacity is proactively avoiding performance degradation and problems that may occur as users try to augment the network with unauthorized hardware, software, or configuration change (solarwinds, 2016).

Recommendation 3: Dealing with Device faults

Regular training and/or idea sharing by technical team with departments and between departments is highly recommended. Sessions where technical teams sits regularly for a few hours and share their experiences and how they dealt with problems whenever they came across them.

Documenting of device faults and how they were resolved can be encouraged as well. This culture will empower the team and whenever a fault that occurred in the past occurs again it will be efficiently and effectively resolved.

Chapter FIVE Conclusion

After the investigation the conclusion is that government system security is at a satisfactory level as the findings do show that there network is encrypted; access controls are used as well as authentication mechanism. These controls show that measures were indeed put in place from the initial stages to see data confidentiality being achieved. Therefore there is less likelihood of unauthorized access to information in government departments. Data integrity may be venerable mainly because of the DIT set up.

The research has identified that DIT is the core technical department and supports almost all of the government departments. Therefore data integrity may be jeopardized as the system administrators' supports more than one department interchangeably. That is controls over administrators is minimal and also since they work in different departments they may be prone to making mistakes. Therefore it is strongly recommended that each government department should have its own system administrator.

Objective: Identify common causes of system downtime in government.

Common causes were identified and the researcher has realized that the government departments' primary causes of downtime are power outages, poor cabling and poor management as there are less trainings done to equip system/network supporting team with new technologies.

Objective: To investigate methods of mitigating downtime outages.

The following should be carried out as ways to reduce network downtimes:

- Empowering technical team with new skill set that will keep them updates and confident to maintain system/network. Taking some basic steps and implementation of best practices can help government department technical team protect government network, Dolisy (2014). Regular review of router configurations and/or software codes and vigilant system/network monitoring is critical.

Objective: To identify customer perception of service downtime.

Customers are not happy with government service and therefore more needs to be done in making sure that they are provided with reliable service.

5.1 Further work

More research may be carried out in the future, targeting more government departments. That is a research targeting more than three government departments and probably targeting only technical users and clients.

Another research can be done focusing on the cost fact of system downtimes. That is how much it costs the government of Botswana whenever there is system/network downtime.

5.2 Research Implications

The results of this research will be beneficial to other government departments as the problem of network downtimes go across the government ministries. Other African governments or developing countries will also benefit as the researcher observed that there is little research this area. Therefore other scholar will benefit in the long ran as well especially those that are in Botswana as a few papers are available in Botswana.

References

1. Africa Times (2017), Global 'ransomware' attack a reminder to vulnerable African firms, <http://africatimes.com/2017/05/13/global-ransomware-attack-a-reminder-to-vulnerable-african-firms/> Accessed 28/05/2017
2. Africa Business (2017), The battle against ransomware, Africa Business Magazine, <http://africanbusinessmagazine.com/sectors/technology/the-battle-against-ransomware/> Accessed 28/05/17
3. An Algosec Whitepaper (2016), Firewall Management, 5 Challenges every company must address, <https://www.algosec.com/wp-content/uploads/2016/03/Firewall-Management-5-Challenges-Every-Company-Must-Address-WEB.pdf>, Accessed: 20/01/2017
4. Avishai Wool (August 2010), Internet Security, Trends in Firewall Configuration Errors, Measuring the Hotel in Swiss Chess, Accessed: 22/01/2017
5. Bhathagar, S. (2000) "Social implications of information and communication technology in developing countries: lessons from Asian success stories". The Electronic Journal on Information Systems in Developing Countries. 1(4), p.1-9. Accessed: 25/01/2017
6. Botswana National E-Government Strategy (2011-2016), The Republic Of Botswana, Accessed: August 26th 2016, <https://www.eng.tau.ac.il/~yash/05440153.pdf>, Accessed: 20/01/2017
7. Buttle, F., (2006), Relationship marketing . In: Buttle,F(Ed.),Relationship Marketing Theory and Practices. London: Paul Chapman Publishing ltd, pp. 1-16, Accessed 22/03/2017
8. Chad, L., Graham, P., & Donald, M. (2007)"Issues and recommendations in evaluating and managing the benefits of public sector IS/IT outsourcing". Information Technology & People. 20(2), p.191- 183. Accessed: 22/17/2017
9. Dudovsky ,J (2015), Ethical Considerations, Research Methodology methodology.net/research-methodology/ethical-considerations/ , Accessed: 16/11/2016

10. Emerson Network Power Report, Understanding the Cost of Data Center Downtime: Understanding the Cost of Data Center Downtime: An Analysis of the Financial Impact of Infrastructure Vulnerability, Accessed: 28/09/2016
11. Implementing Cisco IOS Network Security (IINS 640-554) (November 30th 2012), Foundation Learning Guide, 2nd Edition, Catherine Paquet, Accessed: 30/10/2016
12. Laura Castle (2008), Use the Guidance and Tools of your Software and Service Providers to Prevent, Anticipate, and Mitigate System Downtime, <http://www.lauracastle.com/portfolio/qedmktg.pdf>, 06/06/2017
13. Maetin Perlin (2012), Downtime, Outages and Failure – Understanding their true Cost, Evoven Blog, Accessed: 31/10/2016
14. Maine, L. (Annual report 2003/2004). 2005. Gaborone, Botswana: The Ombudsman Mosireletsi Public Protector, Accessed: 22/07/2017
15. Maitlamo, Botswana's National ICT Policy, A Legislative Framework & Change Report, December 2004, http://www.researchictafrica.net/countries/botswana/MAITLAMO_Botswana_National_ICT_Policy.pdf, Accessed: 26/08/2016
16. Martin Perlin (Sep 2012), Downtime, Outages and Failures - Understanding Their True Costs, Blog, <http://www.evoven.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html>, Accessed: 28/09/2016
17. Mpho Tebele (2017), Botswana Hit By a Worldwide Cyber Attack, The Southern Times, <https://southernafrican.news/2017/05/16/botswana-hit-by-worldwide-cyber-attack/> Accessed 21/05/2017
18. Namogang, P. E.(2015) The computerisation of the national registration (Omang) system (No. No. 3, 2014). 2015. Gaborone, Botswana: Office of the Auditor General. Accessed: 22/01/2017
19. Nugi Nkwe (2012), E-Government: Challenges and Opportunities in Botswana, International Journal of Humanities and Social Science, Department of Accounting and Finance, University of Botswana, Gaborone, Accessed: 25/04/2017
20. Rouse Margaret's article (2013), titled Network Evolution, An OSI (Open Systems Interconnection), Accessed: 28/09/2016

21. Salah Alabady (2008), What's Behind Network Downtime? Sunnyvale, California, Juniper Networks, White Paper, Accessed: 28/09/2016
22. Selepeng, M. L. "The performance management system as an instrument to enable government ministries and departments to conscientiously work towards optimum delivery of service to the nation" 2002. Retrieved 12th July 2006, from <http://www.gov.bw>, Accessed: 22/01/2017
23. Slone John (1999), Local Area Network (6th Edition), Accessed September 28th 2016
24. Solarwinds (2016), White Paper, Detecting and Preventing Rogue Devices, http://web.swcdn.net/creative/pdf/Whitepapers/UDT_WP_Detect_Prevent_Rogue_Devices.pdf, Accessed: 05/06/2017
25. Stephen J. Bigelow (2016), The causes and costs of data center system downtime: Advisory Board Q&A, Accessed: 28/09/2016
26. Stratus Technologies (2014), Focus on Business Continuity Instead of Disaster Recovery, White Paper, Accessed: 30/10/2016
27. Thapisa, A. P. N., & Jain, P.. (200)"Bio-factor analysis of library productivity". Library Management. 21(1/2), 86-93. Accessed: 22/01/2017
28. The Government Gazette, (November 13th 2009), State of the Nation Address, His Excellency the President of The Republic of Botswana, Lieutenant General, Dr. Sir Seretse Khama, Ian Khama, Accessed: 26/08/2016
29. The World Bank (Oct 17, 2016)– Working for a World Free of Poverty, Countries / Botswana. <http://www.worldbank.org/en/country/botswana/overview>, Accessed: 28/10/2016
30. T. Mogotlhwane, F. Khosrowshahi, J. Underwood (2013), IT Challenges in Developing Countries: Botswana's Perspective, International Journal of Computer and Information Technology (ISSN: 2279 – 0764), Volume 02, <http://www.ijcit.com/archives/volume2/issue6/Paper020608.pdf>, Accessed: 25/01/2017
31. U.S. Office of Personnel Management (Sept 2008), Theodore Roosevelt Building 1900 E Street, NW Washington, DC 20415-0001. Accessed January 27th 2017
32. UNDP (2005). "Botswana human development report 2005", 2005 Gaborone, Botswana: UNDP. Accessed: 22/01/2017

33. Vinod Mohan (2007), Top reasons for network downtime, Geek Speak Blog, Accessed: 31/10/2016

34. Zikmund. W, (2003), Business research methods. 7th edition. Ohio: South west college publishing, Accessed 38/04/2017

Appendices

Appendix 1 Extended Abstract

System Downtime a common phenomenon in Botswana – An investigation on the possible causes and possible solutions

Background

Botswana has been one of the fastest growing economies in the world as it moved into the ranks of upper-middle income countries from being one of the poorest countries in the world since its independence in 1966. (The World Bank portal (Oct 17, 2016)).

The country has always been proactive in exploiting areas that can better its economy. One area that the government has been exploiting is the Information Communications Technology area, taking advantage the use of computers and/or the interconnected world. In recent years government has heavily invested in building government network in different departments as an effort to improve its service delivery. Unfortunately the periods in which government systems fails to provide or perform their intended service are very frequent. The periods in which a system is unavailable or cannot perform its primary function is referred to as a system downtime period. This could be due to various reasons and these reasons could be hardware or software related.

Aim and Objectives

Aim: The aim of this project is to investigate the problems of Government network services system downtime from a Botswana perspective.

Objectives

- Identify common causes of system downtime in government.
- The goal of this project is to have solid recommendations on what can be put into place to reduce/deal with this common network downtime issues.

Research Methods

The hybrid method encompasses both the quantitative and qualitative techniques.

The quantitative technique applies mainly when quantifiable data is collected and evaluated. That is, quantitative techniques/method focuses on investigating on something that can be measured and/or observed. The technique addresses such questions as “how often?”, “how many” or “how much?” (Mujinga,2012). The qualitative technique however emphasizes on expressive facts collection other than quantities. That is, it focuses on collecting comprehensive information of individual behavior as well as the details administering that particular behavior.

Use of more than one method and/or technique can be vitally important provided either method complements the other. That is, the benefit is that one method/technique brings out extra proof on the other method and assist in responding to challenges that probably could have never been able to be addressed by a single method (Creswel et al 2011).

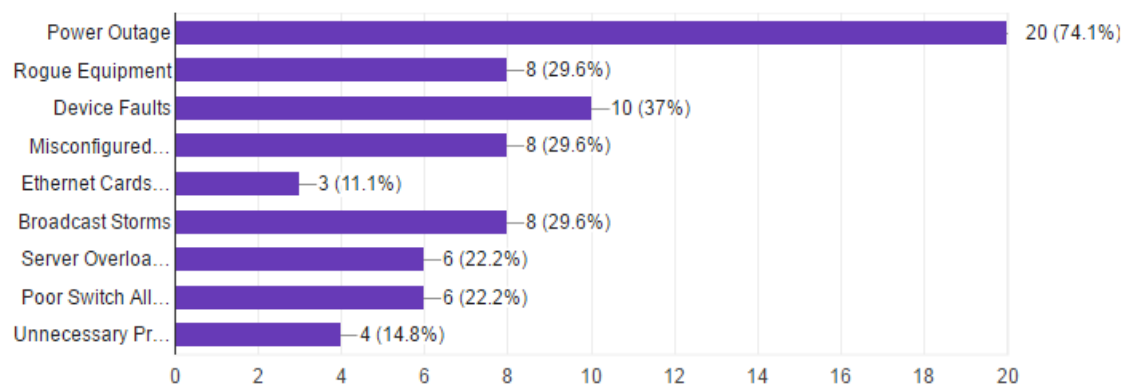
A rigorous survey will be done at all stages of the project but most importantly during the data gathering stage that is when a more comprehensive survey will come to play.

Results

Data collection was carried out by the use of questionnaires and Interviews. The questionnaire was the primary data collection tool, therefore it was sent to almost all of the participants. A Google Docs questionnaire was developed and shared with all the targeted participants. The interview was a secondary tool used to compliment the questionnaires. That is, participants who could not be reached were followed up with a questionnaire and these were mostly participant targeted. These were key participants who the researcher felt that their input was critical to the success of this project and thus followed.

4. What are the common factors that lead to a network downtime in your department?

27 responses



Conclusion

Common causes were identified and the researcher has realized that the government departments' primary causes of downtime are power outages, poor cabling and poor management as there are less trainings done to equip system/network supporting team with new technologies.

References

1. An Algosec Whitepaper (2016), Firewall Management, 5 Challenges every company must address, <https://www.algosec.com/wp-content/uploads/2016/03/Firewall-Management-5-Challenges-Every-Company-Must-Address-WEB.pdf>, Accessed: 20/01/2017
2. Avishai Wool (August 2010), Internet Security, Trends in Firewall Configuration Errors, Measuring the Hotel in Swiss Chess, Accessed: 22/01/2017
3. Bhathagar, S. (2000) "Social implications of information and communication technology in developing countries: lessons from Asian success stories". The Electronic Journal on Information Systems in Developing Countries. 1(4), p.1-9. Accessed: 25/01/2017
4. Botswana National E-Government Strategy (2011-2016), The Republic Of Botswana, Accessed: August 26th 2016, <https://www.eng.tau.ac.il/~yash/05440153.pdf>, Accessed: 20/01/2017
5. Buttle, F., (2006), Relationship marketing . In: Buttle,F(Ed.),Relationship Marketing Theory and Practices. London: Paul Chapman Publishing ltd, pp. 1-16, Accessed 22/03/2017

Appendix 2: Technical Questionnaire

A kind request from Mr Resego K Kwelagobe to you, to assist him by completing the following questionnaire. The questionnaire is set to assist the research on his MSc thesis aimed at investigating the problem of government computer network services system downtime. Please be assured that the information you provide will be kept confidential. Your name will not appear in any thesis or report resulting from this study.

1. Please choose your relevant education level

- ☐ IT Certificate
- ☐ Diploma
- ☐ Degree
- ☐ Masters
- ☐ CISCO Certifications
- ☐ MicroSoft Certification
- ☐ Oracle Certification

2. Please specify the government department you work under

- ☐ DIT
- ☐ DRTS
- ☐ Ministry Of Labour

3. How often do you experience network/system downtime?

- ☐ Daily
- ☐ Weekly
- ☐ Monthly
- ☐ Quarterly (3 Months)
- ☐ Yearly

4. What are the common factors that lead to a network downtime in your department?

- ☐ Power Outage
- ☐ Rogue Equipment
- ☐ Device Faults
- ☐ Misconfigured Router
- ☐ Ethernet Cards Faults
- ☐ Broadcast Storms
- ☐ Server Overloading
- ☐ Poor Switch Allocation
- ☐ Unnecessary Protocols

5. What are the common attacks on your network?

- ☐ DNS problems
- ☐ Poor or bad cable
- ☐ Slow application performance
- ☐ Printing problems
- ☐ Duplex mismatch
- ☐ Cable Problem
- ☐ Dead drop
- ☐ Can't get an IP address
- ☐ Excessive Network Collisions
- ☐ Software Problem

6. Is your network secured with an antivirus?

- ☐ Yes
- ☐ No
- ☐ Maybe

7. What measures has been put in place to secure your network?

- ☐ Firewalls
- ☐ SSH Keys
- ☐ VPNs and Private Networking
- ☐ Public Key Infrastructure and SSL/TLS Encryption
- ☐ Service Auditing
- ☐ File Auditing and Intrusion Detection Systems
- ☐ Isolated Execution Environments
- ☐ Others

8. How often are you and/or your team trained on network security technologies?

- ☐ Regularly
- ☐ Sometimes
- ☐ Never

9. What is the longest time you experienced system downtime in your department?

- ☐ 1 hour or less
- ☐ 4 hours or less
- ☐ 8 hours or less
- ☐ 24 hours or less
- ☐ 48 hours or less
- ☐ 48 hours and more

10. On average what is the turnaround time for resolving network failure in your department?

- ☐ Within 30 minutes
- ☐ Within 1 hour
- ☐ Within 8 hours
- ☐ Within 24 hours
- ☐ Within 48 hours

Appendix 3 - User Questionnaire

1. How often do you experience system/network downtime in your department?

- ☐ All the time
- ☐ Sometimes
- ☐ Most of the time
- ☐ Never

2. What are the primary causes of network/system downtime?

- ☐ Technical Issues
- ☐ Non Technical Issues

3. What is the longest time you experienced system downtime in your department?

- ☐ 1 hour or less
- ☐ 4 hours or less
- ☐ 8 hours or less
- ☐ 24 hours or less
- ☐ 48 hours or less
- ☐ 48 hours and more

4. On average what is the turnaround time for resolving network failure in your department?

- ☐ Within 30 Minutes
- ☐ Within 1 Hour
- ☐ Within 8 Hours
- ☐ Within 24 Hours
- ☐ Within 48 Hours
- ☐ More Than 48 Hours

Appendix 4 – Client/Customer Questionnaire

1. How often do you experience system/network downtime when visiting government departments?

- ☐ All the time
- ☐ Sometimes
- ☐ Most of the time
- ☐ Never

2. What are the primary causes of network/system downtime?

- ☐ Technical Issues
- ☐ Non Technical Issues

3. What is the longest time you experienced system downtime in the government department?

- ☐ 1 hour or less
- ☐ 4 hours or less
- ☐ 8 hours or less
- ☐ 24 hours or less
- ☐ 48 hours or less
- ☐ 48 hours and more

4. On average what is the turnaround time for resolving network failure in the government department?

- ☐ Within 30 Minutes
- ☐ Within 1 Hour
- ☐ Within 8 Hours
- ☐ Within 24 Hours
- ☐ Within 48 Hours
- ☐ More Than 48 Hours

5. According to you which of the following services would you prefer government to adopt?

- ☐ Manual
- ☐ Computer based
- ☐ Both Manual & Computer based

Appendix 5 – Gant Chart Sample

