✓

University of KwaZulu-Natal

What is the Impact of the Cyber Crime Act on The Business community in Mauritius?

2004

(Nasserkhan Jamalkhan)

What is the Impact of the Cyber Crime Act on The Business Community in Mauritius?

2004

by

(Nasserkhan Jamalkhan)

(14 January 2005)

Submitted in partial fulfilment for the degree of MBA Information Management & E-commerce, University of KwaZulu-Natal, Durban. Student no. 201511966.

Declaration

I declare that "What is the impact of the Cyber Crime Act on the business community in Mauritius" is my own work and that all the sources I have used or quoted have been indicated and acknowledged by means of complete references.

Signature:

Name: Nasserkhan Jamalkhan

Acknowledgements

The growing number of threats for the past 20 years in the ICT sector has created the enthusiasm to come out with this research on the "Impact of the Cyber crime Act on the Business community".

This research would not have been made possible without the precious collaboration and support of the team which has been with me during the last four months.

First and foremost, I would like to convey my sincere appreciation to Mr Craig Blewett, my Supervisor for his guidance and professionalism regarding the presentation of this work, as well as the supporting staff of the Graduate School of Business at the University of KwaZulu-Natal, Durban.

A special thanks to the executive members and legal advisers of the American Chamber of Commerce, Mauritius (AMCHAM) and the staff of Babic Group for their help and contribution for having recovered a maximum of survey forms and questionnaires duly completed.

My sincere thanks go to the members of the Police Force, IT Policy Units and the Police Press Office for their kind support and appreciation regarding this research. My earnest thanks equally go to the senior officers of the Prime Minister's office who cooperated with this survey despite a short delay.

My profound gratitude goes to members of my family and close relatives who understood the preciousness of this work to me. Their sacrifice has indeed contributed to the driving force of this resounding success.

Finally, I am grateful to all those who contributed directly or indirectly towards the success of this research and understood its importance for a betterment of the Cyber Community in Mauritius.

Abstract

At this early age of the internet, the e-business environment is almost like a lawless territory. Fast movers are making fortunes whereas rebels can act with impunity and move on before the legal process can catch up.

The fast expansion of cyber crimes in the world has been the motivation to perform this research on its impact on the business community in Mauritius after the devastating effects in developing countries. Organisations that are not keeping pace with these realities are becoming vulnerable to cyber criminals or hackers.

An analysis of the situation in the world from the literature review has provided a better understanding of the most common crimes that are causing trouble to the businesses and obstacles to the advancement of e-commerce. Compared to earlier technological changes, the internet has shown a rapid proliferation. Organisations have to be ready to face this challenge or they may face the dangers of being attacked or even prosecuted for not having secured their system properly.

While securing the internet remains a major challenge for every country, businesses have to cope with limited protection until an international law become in force to control this wild territory. The reports available on the Crime trend show that there has been a steady increase in Computer related crimes in the world.

The research is conducted on a sample of IT literate participants. Interviews and focus group discussion have also contributed in the accuracy of the findings.

The results and findings demonstrate that there is room for improvement but there is a lack of awareness on the Cyber crime act.

Hopefully, this research will help to shed light on the major concerns of the business community.

Table of Contents

List of Figures

List of Tables

1. Introduction

The fast expansion of the Internet usage has resulted in a major jump in the number of cyber crimes worldwide. With the sustained development of the Information Communication and Technology in Mauritius, the Computer Misuse and Cybercrime Act (ACT) was passed in 2003 to protect the cyber communities. This research intends to investigate the impact of this new regulation on the business community in Mauritius.

Mauritius is an island situated 890 km to the east of Madagascar, some 2,000 km off the south-east coast of Africa. The population of Mauritius is around 1.2 million. The Economy relies mainly on Agriculture, Textile Industries, Tourism and the Information, Communication & Technology (ICT) sectors. The government's priority is to make the ICT sector, one of the main pillars of the economy in the coming years.

The internet influences the development of e-business and, in particular, e-commerce. According to the Forrester Research, e-commerce transactions will exceed $6.8 trillion by the end of 2004 (http://www.glreach.com/eng/ed/art/2004.ecommerce.php3), that is a growth of nearly 10 times over the last four years. These transactions are conducted between companies and business institutes, as well as between firms and average clients.

Unfortunately doing business and working on the internet is no longer that safe. The number of computer hackers has increased over the years. This situation has created a number of debates as to whether it is safe to use internet services and e-mail for client communications. Clearly, this is an area with some privilege/confidentiality concerns, as well as a number of ethical considerations with the gradual increase in internet users. The ethical concerns coupled with a legal field that is just starting to take shape with the Internet basics will not mix well when things like electronic commerce are just around the corner.

The rationale for this research is to understand the Cyber crime trend and make the necessary recommendations to the concerned authorities.

The objective of this research is to measure the impact of the ACT on the business communities and evaluate its awareness in general. In the ICT sector, the law is amended and updated regularly to protect internet users and intellectual property rights from new type of threats. We will find out whether Mauritius is following the general trend in the world.

The impact of the Cybercrime Act on the business community in Mauritius will be addressed by the following research questions:-

- How much at risk is the Mauritius business community?
- Is there a proper structure to deal with this kind of crime?
- What is the general feeling of the cyber community about this law?
- What are the proactive roles of business organisations to prevent and control the cyber crimes in Mauritius?

The chapter that follows is a review of the literature on computer related crimes in the world. It provides an overview on the subject being studied. The business community in Mauritius should be concerned about the growing number of threats in the world despite the Cyber Crime Act. They should be aware about how much additional protection they still require in this fast changing environment. A few cases of damages caused by cybercrimes are being referred.

Then we have the research methodology chapter which addresses the research questions. It includes the research design, construction of the questionnaires and collection of data.

Chapter 4 examines the Findings and offers Discussion on the data collected and analysed. These data are presented as charts and tables for a better understanding.

Finally we have the Conclusion chapter with a section on the recommendations and contribution of this research.

2. Literature Review

The literature review will tell us more on the general situation of cybercrimes in the world. Where applicable, some quotes and references will be added to clarify the relationship between this research and previous work conducted on this topic. After reading this chapter, you should be able to have a broader view about the cyber crime dimensions and why this research is distinctive in its way.

2.1 Definition

The Oxford Reference Online(http://www.oxfordreference.com/views) defines cybercrime as crime committed over the Internet. Some people refer cybercrime as "computer crime." The Encyclopaedia Britannica defines computer crime as any crime that is committed by means of special knowledge or expert use of computer technology. In some countries the Computer Misuse is know as Cybercrime or Computer crime.

Computer crime could reasonably include a wide variety of criminal offences, activities, or issues. The scope of the definition becomes even larger with the frequent companion or substitute term "computer-related crime."

The word "hacker" should also be defined here, as it will be used extensively in this study - hackers are basically people who break into and tamper with computer information systems. The word "cracker" carries a similar meaning, and "cracking" means to decipher a code, password or encrypted message.

The need to make the cyber communities become aware of the dangers lying ahead has become more than necessary.

Now we will be looking at how the major crimes are being handled in the world.

2.2 Types of Cyber crime

While most computers are nowadays linked to the World Wide Web (www), some hackers for different reasons have found a way to express their feelings, anger or message to the world at the cheapest known cost. These hackers can cause damages to the content of the computer or the system completely. Thus, the need for laws against cybercriminals became obvious. The most popular case is the school dropout from the Philippines who wrote the "1LOVEYOU" virus (http://bossding2002.free.fr/ilu.htm). He was not prosecuted by the Philippines Government because at that time, the country did not have laws relating to virus creators.

The internet is almost like a lawless territory. Fast movers are making fortunes whereas rebels can act with impunity and move on before the legal process can catch up.

The most common form of Cyber crimes can be perpetuated in the following ways:-
a) Viruses and worms (http://www.bainet.com/main.php?mode=displaysection&i_d=6&PHPSESSID=) are getting more insidious nowadays – take for instance, the Swen worm,(http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SWEN.A) which cleverly disguises itself as an e-mail message from Microsoft with a patch attached.
Malicious codes like worms, viruses and Trojan horses. These exploit security vulnerabilities of a system and they tend to alter or destroy data. The damage they cost is worth millions of dollars to companies as well as government agencies. Worms are different from viruses because they are able to spread themselves with no user interaction. They may send emails using addresses from a user's database. A virus can attack systems in many ways: by erasing files, corrupting databases and destroying hard disk drives.
The Santee worm first appeared on 20 December 2004 and within 24 hours had successfully hit more than 40,000 websites.
(http://news.bbc.co.uk/1/hi/technology/4117711.stm)

b) Hacking
Hacked systems can be used for information gathering, information alteration, and sabotage. Vulnerabilities exist in almost every network. Hackers sometime crack into

systems to brag about their abilities to penetrate into systems, but others do it for illegal gain or other malicious purposes. Today, hacking is simpler than ever – hackers can now go to websites and download protocols, programs and scripts to use against their victims. More information on this topic is available on http://archives.cnn.com/2001/TECH/internet/11/19/hack.history.idg/.

Compared to hackers, crackers perform a similar job but ask for a fee to do it. The most common job of crackers today is the removal of mobile phone lock for a particular service provider.

c) Cyberterrorism

This is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets. More information on this kind of crime can be available on Cyber- Terrorism by Adam Savino at http://www.cybercrimes.net/Terrorism/ct.html.

d) Industrial espionage

This is where corporations spy on other companies and with network systems, this can be an easy task. Companies can retrieve sensitive information rarely leaving behind any evidence. Cyber-espionage can also be applied to nations that spy on other countries' sensitive information. According to the 2003 Emerging Internet Security Survey, more than one in three firms across Europe has reported that their computing environments have been infected with spyware. A report by Websense Inc is available on http://www.net-security.org/press.php?id=1614.

e) Spoofing of IP addresses

This is where a false IP address is used to impersonate an authorised user. Citibank experienced that huge numbers of its customers desktop PCs are passing on e-mails for conmen trying to steal confidential details.

Analysis by mail security firm Ciphertrust (http://news.bbc.co.uk/go/em/fr/-/1/hi/technology/3762264.stm) reveals that the hijacked computers are unwitting accomplices for almost all so-called phishing attacks. Its research shows that the hijacked

PCs are organised into five separate networks of zombie computers that send out the fraudulent e-mails.

f) Copyright piracy

This is the unlawful reproduction and distribution of copyright protected material and software piracy. Most countries in the world today have their own copyright act to fight this fraud. This is also known as the Intellectual Property Rights.

g) Cyber Attacks on financial systems

This includes electronic banking and payment systems frauds. Very recently, the federal police in Brazil said they have arrested more than 50 people for allegedly stealing $30m from Brazilians through internet fraud.

The group secured the money by sending e-mail attachments infected with a virus able to store details of people's internet bank accounts, police said.

Computer fraud experts said last month Brazil was now the global capital of hacking and internet fraud. (http://news.bbc.co.uk/go/em/fr/-/1/hi/world/americas/3761946.stm).

h) Cyber vandalism

Cyber Vandalism is the defacing of web information or pages. Very recently due to a poor regulation in Zambia, the picture of the president was replaced by a cartoon in one of the official website. No proper action could be taken since there was no suitable law to condemn the offender at that time.

i) Spim

It is similar in design to spam. But instead of attacking your inbox, it works through instant messaging (IM) services (http://news.bbc.co.uk/2/hi/technology/3581148.stm). It is thought that "spimmers" have developed the idea because of the attention-grabbing nature of IM, and the increasingly effective spam filters that specialist companies have developed.

j) Cyberstalking
(http://www.crimelibrary.com/criminology/cyberstalking)
The goal of a cyberstalker is control. Stalking and harassment over cyberspace is more easily practised than in real life. This is due to the anonymity of the internet. There are many cases where cyberstalking crosses over to physical stalking. Some examples of computer harassment are:

- Live chat obscenities and harassment;
- Unsolicited and threatening e-mail;
- Hostile postings about someone;
- Spreading vicious rumours about someone;
- Leaving abusive messages on a website's guest books.

Apart from the above types of Cyber Crimes, a list of most common cyber crimes and frauds happening everyday in the world is also available on http://www.net-intrusion.com/member/data/fraud_info.html.

Having understood the different types of cyber crimes affecting the world, we would now find out about the criminals.

2.3 Who are the Cyber Criminals?

In order to understand this question, it is important to know about the different facets in which cybercrimes may present themselves. Some people may argue that there is a difference between hackers who break into a website to deface its homepage and cases where the crime can occur even if there was no computer. However, the use of technology makes the commission of the crime faster and permits the processing of larger amounts of information. Examples would be credit card fraud, drug trafficking, criminal breach of trust, forgery, cheating, illegal betting or gambling, forgery of valuable documents (money, cheques, passports and identification cards) and money laundering.

Cybercriminals can use the internet for a myriad of other illegal purposes including drug dealings, hackers and burglary rings. For example a gangster can crack the hospital's computer system to alter the dosage of medication for the patient who is his target. Cybercriminals can range from teenagers who vandalise websites to terrorists who target a nation.

Out of the ten most frequent crimes that are reported, hackers occupy the main source of the problem.

2.3.1 Hackers – The problem for every publicly connected network.

For all organisations with publicly connected networks, independent hackers will always represent a serious threat, regardless of the nature of the organisation's business or its profile. The motive of independent hackers will vary considerably and may include financial gain, malicious damage (e.g., web site defacements, DoS attacks, release of viruses and worms) or a common favourite, the theft of network resources (e.g., bandwidth usage) for personal use.

The relentless barrage, and global nature, of malicious activity that occurs against networks 24 hours a day, means that network and system administrators have to be constantly up to date with the latest anti-virus signatures, software patches and aware of the nature and impact of ongoing changes to their network architecture and environment. Has a network user, for example, installed an unauthorised modem in order to gain faster access to the Internet and thereby bypassed the firewall, IDS and virus checkers? Did a user introduce an infected floppy disk on the internal network bypassing the gateway virus checking? One small transgression may result in a back door trojan being installed and provide with it, future undetected network access or result in other forms of serious network compromise.

It is not so much that independent hackers are necessarily highly skilled that makes the threat from them so serious – though some are – but rather, it is the combination of the sheer volume of attacks that are attempted on a daily basis; the rapidly changing nature of the attacks and vulnerabilities; and that many attack tools are sophisticated and powerful and provide low-skilled attackers with an easy to use interface.

Network and system administrators have the additional burden of getting network defence right all the time, whereas an attacker needs to find only one point of vulnerability to do damage.
(Adapted from Australian Computer Crime and Security Survey, by AusCERT, Deloitte Touche Tohmatsu and the NSW Police, 2002)
Hackers are really the problem for every publicly connected network.

2.3.2 Phishing

Referring to an article which was published on the BBC news website (http://news.bbc.co.uk/1/hi/technology/4072647.stm), cyber criminals step up the pace in 2004. The So-called phishing attacks that try to trick people into handing over confidential details have boomed in 2004. This article also reported that the number of phishing e-mail messages stopped by security firm MessageLabs has risen more than tenfold in less than 12 months.

In 2004 it detected more than 18 million phishing e-mail messages.

In its end-of-year report, MessageLabs said that phishing had become the top security threat and most popular form of attack among cyber criminals.

Older attacks relied on users not spotting the fact that the site they were visiting was fake, but more recent phishing e-mails simply try to steal details as soon as a message is opened.

Other phishing scams try to recruit innocent people into acting as middlemen for laundering money or goods bought with stolen credit cards.

"E-mail security attacks remain unabated in their persistence and ferocity," said Mark Sunner, chief technology officer at MessageLabs.

"In just 12 months phishing has firmly established itself as a threat to any organisation or individual conducting business online," he said.

Mr Sunner said MessageLabs was starting to notice that some phishing attacks become very focused on one company or organisation.

"Already particular businesses are threatened and blackmailed, indicating a shift from the random, scattergun approach, to customised attacks designed to take advantage of the perceived weaknesses of some businesses," he said.

Although phishing attacks grew substantially throughout 2004, viruses and spam remain popular with cyber-criminals and vandals.

One of the biggest outbreaks took place in January when the MyDoom virus started circulating. To date the company has caught more than 60 million copies of the virus.

Also up this year was the amount of spam in circulation. In 2003 only 40% of messages were spam. But by the end of 2004, almost three-quarters of messages were junk.

This increase in Cyber crimes is also confirmed with the report of Mark Ward, Technology correspondent at the BBC News website. He pointed out that the count of the known viruses broke the 100,000 barrier and the number of new viruses grew by more than 50%. (http://news.bbc.co.uk/1/hi/technology/4105007.stm)

Also on the increase is the number of networks of remotely controlled computers, called bot nets, used by malicious hackers and conmen to carry out many new type of cyber crimes.

Despite the above quote, the National Police Force still remains the principal authority that can enforce the law.

2.3.3 Teenage kicks

One of the biggest changes of 2004 was the waning influence of the boy hackers keen to make a name by writing a fast-spreading virus, said Kevin Hogan, senior manager in Symantec's security response group.

Web portal Lycos Europe reported a 500% increase in the number of phishing e-mail messages it was catching.

The Anti-Phishing Working group reported that the number of phishing attacks against new targets was growing at a rate of 30% or more per month.

Those who fall victim to these attacks can find that their bank account has been cleaned out or that their good name has been ruined by somebody who stole their identity.

This change in the ranks of virus writers could mean the end of the mass-mailing virus which attempts to spread by tricking people into opening infected attachments on e-mail messages.

Mr Hogan said worm writers were more interested in recruiting PCs to take part in "bot nets" that can be used to send out spam or to mount attacks on websites.

In September Symantec released statistics which showed that the numbers of active "bot computers" rose from 2,000 to 30,000 per day.

These figures confirm that hackers, phishing attacks and teenage kicks are all following the same trend in the world.

2.3.4 Moving target (Virus threat to mobile phones).

The emergence of the first proper virus for mobile phones was also seen in 2004.

In the past, threats to smart phones have been largely theoretical because the viruses created to cripple phones existed only in the laboratory rather than the wild.

In June 2004, the Cabir virus was discovered that can hop from phone to phone using Bluetooth short-range radio technology.

Also released in 2004 was the Mosquito game for Symbian phones which surreptitiously sends messages to premium rate numbers, and in November the Skulls Trojan came to light which can cripple phones.

On the positive side, Finnish security firm F-Secure said that 2004 was the best-ever year for the capture, arrest and sentencing of virus writers and criminally-minded hackers.

In total, eight virus writers were arrested and some members of the so-called 29A virus writing group were sentenced.

One high-profile arrest was that of German teenager Sven Jaschen who confessed to be behind the Netsky and Sasser virus families.

Also shut down were the Carderplanet and Shadowcrew websites that were used to trade stolen credit card numbers

Even in the United States, it was noted that American law enforcement agencies, including the Justice Department, lacked the staff to investigate and prosecute cybercrimes like digital break-ins, data destruction and viruses. As a result of this, cybercriminals were breaking into or paralysing US-based websites with little fear of retribution, costing the private sector hundreds of millions of dollars. Interpol, the organisation set up to track fugitives and investigate international crime and of which most countries are affiliated members of, considered letting a Silicon Valley computer security company, AtomicTangerine, help it to protect businesses from hackers. This is after it acknowledged that international law enforcers were unable to combat computer crime effectively and also after acknowledging that governments found it difficult to coordinate cross-border efforts to combat this new phenomenon. Its secretary general at the time, Raymond Kendall stated that "... there's a limit to how you can transform police officers or detectives into technicians" (http://lists.insecure.org/lists/isn/2000/Jul/0056.html).

The moving target is a new dimension of threats that need to be watched carefully due to the enormous demand of mobile devices in the coming years.

Now we want to find out about the impact of these crimes on business in general.

2.4 The Cyber Crimes impact on business

Having considered the types of crimes and the people motivated in perpetuating these crimes, this section now addresses the impact of cyber crimes on businesses in other countries.

2.4.1 The NCSA

A survey commissioned by the National Cyber Security Alliance (NCSA) of the United States, (http://www.staysafeonline.info/index.html) found that 30% of people believed they had more chance of getting struck by lightning, being audited by the tax man or winning the lottery than they did of falling victim to a computer security problem. By contrast the chances of falling victim to a computer virus, phishing attack, malicious hack attempt or other cyber security dangers are currently running at 70%, according to statistics gathered for the E-Crime Watch Survey (http://www.csoonline.com/releases/ecrimewatch04.pdf).

According to Ken Watson, chairman of the NCSA, "Cyber-security should become second nature, just like brushing our teeth". (http://www.csoonline.com/releases/ecrimewatch04.pdf).

It is this apparent lethargy that is increasing the vulnerability of many individuals and businesses. Cahoot bank learned a lesson from the security breach which had been caused during a system upgrade 12 days before. A security loophole at internet bank Cahoot briefly allowed customers to access other people's accounts.
"I believe that we need to look closely at our processes because this has not been our greatest moment," stated Mr Sawyer, head of the bank. (http://news.bbc.co.uk/go/em/fr/-/1/hi/business/3984845.stm).

Efforts by US authorities to counter cyber-crime and terrorism have been criticised in an internal report.

"The resulting widespread disruption of essential services after a cyber attack could delay the notification of emergency services, damage our economy, and put public safety at risk," said the report. (http://news.bbc.co.uk/go/em/fr/-/1/hi/technology/3921515.stm).

The national legal systems have no uniform interpretation of e-commerce. For example, European countries have some restrictions. Contracts that require notary's certification and government bodies' registration or cover family and inheritance laws cannot be made through the Internet. Nevertheless, e-commerce embraces Internet relationships including e-sales and e-services (medical, juridical, banking, financial and others).

The approach to the Internet legal regulation has to be revised. Numerous works (mainly written by American scientists) on the Internet as a new info-social space having its own normative regulating system and requiring to work out a special conception of legal regulation have been abandoned. The practice has picked the way of involving the Internet into the national jurisdictions. In this connection, the assumption of other lawyers that there will be a jump in the development of international laws and intensification of their role in unifying national legislations has not proven to be correct. Such tendencies can be noticed in Europe because the European Council strives to create a uniform legal space including that of e-commerce and, as a result, to protect interests of e-commerce participants.

In Malaysia, the development of the Multimedia Super Corridor (MSC) (http://www.msc.com.my/cyberlaws/) and the creation of a pioneer legal and regulatory framework encompassing, amongst other things, the Communications and Multimedia Act, the Computer Crimes Act and the Digital Signatures Act is indicative that most governments are commitment towards the creation of a knowledge-based economy. With this unique corridor, Malaysia continues to attract leading ICT companies of the world to locate their industries in the MSC and undertake research, develop new products and technologies and export from this base.
An International Cybercourt of Justice was established in the MSC and the intelligent cities (Cyber cities) were linked to the global information highway

Thus, the Computer Crimes regulations must be seen not only as a law which regulates the behaviour of people who use and do business over the Internet, but it also must be seen as the Governments efforts to put in place soft infrastructure to nurture the knowledge-based economy.

At the same time, the authorities should be aware that technological innovation and the deviousness of human minds would mean that the law as well as enforcement must not only keep up with cyber criminals, but it must ensure that their officers are one step ahead of cyber criminals, ready to catch them if they perform their dirty deeds.

Prof Ho, Senior Minister of State for Law and Home Affairs of Singapore, stated 'The heavy reliance on IT today can become our Achilles' heel if we do not give enough emphasis to IT security, don't assume your system will not be affected just because it has never happened to you.' (http://straitstimes.asia1.com.sg).

Furthermore, the impact of cyber crimes is causing more and more damages every day. Unfortunately a lot of them are not always reported for obvious reasons like credibility and reputation of the company.

2.4.2 The IC3 Statistics

An interesting joint report from the FBI and the National White Collar Crime Center of the US (http://www.ifccfbi.gov/strategy/2003_IC3Report.pdf) known as the Internet Crime Complaint Center(IC3) shows the following complaints received during the year 2003 only:-

- IC3 websites received 124,509 complaint submissions. These filings were composed of fraudulent and non-fraudulent complaints primarily related to the Internet.

- IC3 referred 95,064 complaints to enforcement agencies on behalf of the filing individuals. These complaints were composed of many different fraud types such as auction fraud, non-delivery, and credit/debit card fraud, as well as non-fraudulent complaints, such as computer intrusions, spam/unsolicited e-mail, and child pornography. From the submissions, IC3 referred 63,316 complaints of fraud, the majority of which were committed over the Internet or similar online service. The total dollar loss from all referred cases of fraud was $125.6 million with a median dollar loss of $329 per complaint. Significant findings include:

• Internet auction fraud was still by far the most reported offence, comprising 61.0% of referred complaints. Non-delivered merchandise and/or payment accounted for 20.9% of complaints. Credit/debit card fraud made up 6.9% of complaints. Check Fraud, identity theft, business fraud, and investment fraud round out the top seven categories of complaints referred to law enforcement during the year (all at 1.0% or more).

• Among those individuals who reported a dollar loss, the highest median dollar losses were found among Nigerian letter fraud, identity theft, and check fraud complainants.

• Among perpetrators, nearly 79% were male and half resided in one of the following states: California, New York, Florida, Texas, Pennsylvania, and Illinois. The majority of reported perpetrators were from the United States. However, perpetrators also had a representation in Canada, Nigeria, Italy, Spain, and Romania.

• Among complainants, 70% were male, half were between the ages of 30 and 50 (39.4 average age) and over one-third resided in one of the four most populated states: California, Florida, Texas, and New York. While most were from the United States, IC3 received a number of complaints from Canada, Australia, Great Britain, Germany, and Japan.

• Males lost more money than females. This may be a function of both online purchasing differences by gender and the type of fraudulent schemes the individual were victimized by.

• Electronic mail (E-mail) and web pages were the two primary mechanisms by which the fraudulent contact took place. In all, 64.8% of complainants reported that they had e-mail contact with the perpetrator and 19.4% had contact through a web page.

During one of these typical attacks the cyber-thieves enter an organization's computer system, steal electronic copies of employee records, customer data, client data, patient data and other sensitive, confidential and secret information, defined as "protected information." The cyber-criminal's main objective is to acquire sufficient information to facilitate identity theft of all of the organization's employees; customers, clients; patients; suppliers; vendors; contactors; advisors; and others, and if available steal credit and debit card information and other valuable information.

Under American law a custodian of protected information in electronic format has an affirmative duty to provide adequate security against cyber-theft, cyber-manipulation, cyber-extortion and cyber-terror acts. Adequate security is commonly defined as that degree or level of security that a prudent custodian of sensitive, confidential or secret information would provide. The current trend is to define adequate as meeting or exceeding the requirements in the cyber-security of protected information as established by the Federal Information Security Management Act (FISMA) (See **Appendix I**). In fulfilling this duty and obligation, be aware that some courts have held a custodian of a party's protected information is potentially liable for all damages resulting from the unauthorized release of such information, even if the information is available from the public records. The obligation of providing adequate cyber-security of protected information is a specific duty which is owed by the custodian irrespective of whether the protected information could have been acquired from some other sources, such as the public records, and irrespective of the fact that the unauthorized release occurred thought the acts of a cyber-crime attack.

Responding to this new cyber-crime attack threat requires both a capital and resource commitment. The Federal Government in the National Strategy to Secure Cyberspace has addressed some of the concerns associated with the expense of responding to cyber-crime risks:

For individual companies and the national, Cyberspace vulnerabilities place more than transactions at risk; they jeopardize intellectual property, business operations, infrastructure services, and consumer trust.

Conversely, cyber security investments result in more than costly overhead expenditures. They produce a return on investment. Surveys repeatedly show that:

Although the likelihood of suffering a severe cyber-attack is difficult to estimate, the costs associated with a successful one [cyber-crime attack] are likely to be greater than the investment in a cyber security program to prevent it;
(Source: The National Strategy to Secure Cyberspace, Feb 2003.)

Organized crime syndicates are tending to focus their cyber-crime activities on the cyber-theft of individuals' identities, credit card numbers, debit card numbers, bank account numbers, and other valuable protected information from the databases of organizations. They are pursing the expansion of cyber-crime attacks on every organization's protected information because

1) electronic data is easy to steal, and

2) it is easy to transfer the stolen information into cash.

Because the custodian organization, that is your organization, has the legal responsibility to cyber-secure all protected information, including the individual victim's identity information, from any unauthorized release and, in fact, as part of the cyber-crime attack an unauthorized release occurred, unless there is a valid and legally effective defence the custodian organization is liable for millions loss suffered by its individuals and their third party creditors. The obligation of providing adequate cyber-security of protected information is a specific duty which is owed by the custodian organization, your organization, to the individual whose protected information your organization maintains. This obligation exists irrespective of whether the protected information could have been acquired from some other sources, such as the public records, and irrespective of the fact that the unauthorized release occurred thought the acts of a cyber-crime attack.

Failure to meet the "safe harbour" defence criteria means that the organization, plus potentially all of its officers, directors, and some members of senior management, may have to pay millions and millions of dollars to the damaged victims and their lawyers. Not a desirable option for most organizations.

(Source : United States General Accounting Office (GAO) Report to U. S. Congress, GAO-02-363, March 2002, Subject: IDENTITY THEFT.)

The section that follows will provide an overview of the prevalence of industrial crimes.

2.4.3 Prevalence of cyber espionage and sabotage

If foreign governments and corporate competitors choose to direct such activity towards their adversaries or competitors – and many do, they will have at their disposal, more sophisticated computer attack skills and resources than the average script kiddie. In the USA, theft of proprietary information was reported by 13% of respondents as a source of financial loss and was the largest source of financial loss (currently estimated to be over $US170 million) compared to all other categories. Clearly, for those who seek to obtain proprietary information, it can be a lucrative business. But if organisations fully understand and recognise the nature of the threat they face, they will be in a position to more effectively manage it by developing appropriate protection and mitigation strategies to minimise the overall risk to the organisation. (Adapted from the Australian Computer Crime and Security Survey, by AusCERT, Deloitte Touche Tohmatsu and the NSW Police, 2002)

If an attacker is sufficiently skilled and his goal is to steal information rather than destroy data or disrupt services, the attack may never be detected or if an attack is suspected, what is left of the forensic trail is likely to be insufficient to establish or prove a case, let alone identify the true source. With the odds in the skilled attacker's favour, it is likely that more attacks of this nature are occurring than many organisations realise. It is quite possible, therefore, that of the 20% of respondents that reported system penetration by an outsider, or of the 39% that reported unauthorised privileged access, a proportion of these attacks may have been motivated by the desire to obtain sensitive or proprietary information for personal, political or commercial gain.

However, determining the motive of an attack is often difficult to gauge on the basis of the forensic evidence left. For many cases of unauthorised privileged access or system penetration, without a full civil or criminal investigation, determining both the motive and the real impact of the attack may never be known. However, personal or financial gain is likely to be the motive for 24% of respondents who reported they experienced the electronic theft or breach of confidential or proprietary information and for the few who experienced wiretapping (1%) and telecommunications interception (1%).
(Adapted from the Australian Computer Crime and Security Survey, by AusCERT,
Deloitte Touche Tohmatsu and the NSW Police, 2002)

From the above reports, we notice that the methods and actions taken by the different authorities are important tools that can be examined and implemented with some viable solutions in Mauritius.

The section that follows provides an overview of the existing solutions in the world.

2.5 Existing Solutions

Having looked at the causes and damages caused to several organisations, this section considers what solutions have been implemented to deal with the problem so far.

2.5.1 Technical Solutions

Even though anti-virus solutions occupy the major protection of computer users, very few users feel concern about having a security system against hackers. Most of the time, the organization becomes aware after that the crime has been committed.

Microsoft said it would soon release a toolkit that strips machines of the irritating programs (http://news.bbc.co.uk/1/hi/technology/4104129.stm). Surveys show that almost every Windows PC is infested with spyware programs that do everything from bombard users with adverts to steal login data. Designed for PCs running Windows 2000

and XP, the utility will clean out spyware programs, constantly monitor what happens on a PC and will be regularly updated to catch the latest variants.
Before now many of Microsoft's other security boosting programs, such as the firewall in Windows XP, have been given away free.

A recent survey by Earthlink and Webroot found that 90% of PCs are infested with the surreptitious software and that, on average, each one is harbouring 28 separate spyware programs. (http://www.earthlink.net/spyaudit/press/)

Users wanting protection from spyware have turned to free programs such as Spybot and Ad-Aware. Spyware comes in many forms and at its most benign exploits lazy browsing habits to install itself and subject users to unwanted adverts.

Other forms hijack net browser settings to force people to view pages they would otherwise never visit. At its most malign, spyware watches everything that people do with their PC and steals login information and other personal data.

2.5.2 Legal Solution

Every organization has a unique business model, a unique staff, a unique management structure, a unique electronic processing infrastructure and many more unique elements and factors associated with its day-to-day operations. Given this fact, it is impossible to begin to address every specific risk and liability exposure which a specific organization may encounter as a result of a cyber-crime attack. Therefore, the following is presented as a general awareness educational discussion. Some of the topics and some of the examples may be directly applicable to your organization and others may not. Furthermore, many risks and liability exposures may exist which this short introduction does not mention.

The fundamental liability derived from cyber-crime based damage claims flows from the premise that every organization that utilizes protected electronic information in its operational activities is potentially liable for all damages that are suffered by each employee, customer, client, patient, contactor, vendor, supplier, associate, partner, agent, and all others who become a damaged-victim through the unauthorized release of their sensitive, confidential or secret information- protected information.

The fact that the unauthorized release was the result of a cyber-crime attack or other criminal act is irrelevant. The custodian organization plus all of its officers, directors and some members of senior management are potentially liable for all damages suffered by all of the damaged-victims.

Potential loss exposures can be significantly reduced with the use of a system like the Advanced Cyber-crime Attack Protection (ACAP, www.acapsecurity.com). An example of the ACAP System which provides an organization with two defence systems:

i) an advanced multi-layered and multi-functional cyber-security defence system and

ii) a cyber-crime attack liability defence system.

In general, there are at least three common cyber-crime attack situations which create the potential for large damage claim liability exposure. These attacks include: the "Direct Attack;" the "Indirect Attack;" and the "Unknown Target Attack." To begin to comprehend the seriousness and the scope of this potential liability the following explores three cyber-crime attack situations.

1) An Organization as the Direct Target:

The cyber-crime attack targeted your organization's computer system and the damaged-victim's protected information was stolen from your organization's computer systems and was fraudulently used by the cyber-criminals causing financial losses to the damaged-victim.

Liability:

Your organization and all of your organization's officers and directors are potentially directly liable for all losses to the damaged-victims because it was your negligence in not securing, or not properly managing the cyber-security of, the protected information, and allowing an unauthorized release of the damaged-victims' protected information which, ultimately resulted in financial losses to the damaged-victims.

Unless your organization, and the officers and directors, can establish with independently verifiable, creditable evidence that your organization was in compliance with the Cyber Crime act for the cyber-security of protected information and/or your organization has credible evidence that risk notices were provided to the potential damaged-victims, providing your organization with the assumption-of-the-risk defence, your organization, and all of the officers and directors, probably have no, or at best very little, effective legal defence against the damage claims alleged by the damaged-victims.

2) An Organization as an Indirect Target:

The cyber-crime attack targeted one of your organization's Client or Customer organization's (C-organization's) computer systems and their employees, clients, customers, patients, contactors, vendors, suppliers or other parties (potential victims) protected information was stolen from the C-organization's computer systems.

Liability:

Your organization and all of your organization's officers and directors are potentially directly liable for all financial losses to the damaged-victims because you were negligent in that you failed to warn C-organization of the potential risks of a cyber-crime attack and that C-organization had an obligation to comply with the Cyber Crime Act and to warm its employees, customers, clients, patients and others of their risk of potential loss from a cyber-crime attack and the related identity theft (liability for failure to warn).

The defence is based upon your organization establishing with independently verifiable, creditable evidence that prior to the cyber-crime attack on C-organization, in a timely manner that your organization notified the C-organization of the risk of a cyber-crime attack, and the possibility of financial damages to the potential victims of an attack upon C-organization and that the risk notice included some general guidance as to where the C-organization could obtain the products and services (such as the ACAP System) which are needed for the C-organization to obtain compliance with the acting laws and established standards for the cyber-security of protected information. The failure of your organization to be able to establish a diligent effort to at least notify the C-organization of the risk will in all likelihood limit your organization and the officers and directors, in the legal defence against the damage claim allegations alleged by the damaged-victims of the C-organization attack as against your organization, the officers and directors.

3) The Actual Targeted Party is Unknown:

The cyber-crime attack occurred and damages were inflicted but the actual targeted organization of the cyber-crime attack is unknown. It could have been your organization's computer system, or your C-organization's computer system or both your computer system and your C-organization's computer systems.

Liability:

Basically the legal liability rational discussed in both items 1) and 2) applies to this factual situation. Based upon those prior discussions your organization and all of your organization's officers and directors are contributing parties to the negligence that allow the unauthorized release of the damaged-victim's protected information and the resulting damages to the damaged-victim. As a contributing party your organization and your firm's officers and directors are potentially liable parties. (Source : http://www.acapsecurity.com/html/CYBER_SECURITY_REPORT.htm)

2.5.3 Preventive solutions

The following tips
(http://www.cybercellmumbai.com/General%20Tips/General%20tips.htm)
can help to avoid cyber crimes:-

a) For the Students

1) Do not give out identifying information such as name, home address, school name or telephone number in a chat room.

2) Do not send your photograph to any one on the Net without initially checking with the parent or guardian.

3) Do not respond to messages or bulletin board items that are obscene, belligerent or threatening.

4) Never arrange a face to face meeting without informing your parent or guardian.

5) Remember that people online may not be who they seem to be

b) For a Personal Computer

1) Use the latest version of a good anti-virus software package which allows updating from the Internet.

2) Use the latest version of the operating system, web browsers and e-mail programs.

3) Don't open e-mail attachments unless you know the source. Attachments, especially executables (those having .exe extension) can be dangerous.

4) Confirm the site you are doing business with. Secure yourself against "Web-Spoofing". Do not go to websites from email links.

5) Create passwords containing at least 8 digits. They should not be dictionary words. They should combine upper and lower case characters.

6) Use different passwords for different websites.

7) Send credit card information only to secure sites.

8) Use a security program that gives you control over "Cookies" that send information back to websites. Letting all cookies in without monitoring them could be risky.

c) For your Business

1) Stay informed and be in touch with security related news.

2) Watch traffic to your site. Put host-based intrusion detection devices on your web servers and monitor activities looking for any irregularities.

3) Put in a firewall and ensure that it has been correctly configured

4) Develop the web content off line.

5) Ensure that the web servers running your public web site are physically separate and individually protected from your internal corporate network.

6) Protect your databases. If your web site serves up dynamic content from database, consider putting that database behind a second interface on your firewall, with tighter access rules than the interface to your web server.

7) Back up your web site after every update.

2.6 Cybercrime Situation in Mauritius

Attention in now turned especially to the situation in Mauritius. This section provides an overview of the current cyber crime situation. A summary of the penalties from the Cyber crime ACT 2003 is also included for reference.

2.6.1 Current situation

In Mauritius, the IT Unit of the Police Force is responsible for the tracking of cybercrimes. According to the Commissioner of Police (Mauritius Crime Survey, 2004) white-colour crime, computer crime and financial crime in all their categories are constantly on the increase. He also stated that "the prevailing situation calls for a re-examination of the whole issue of public safety and requires us to expand the traditional concept of peace and security to include safety needs which now constitute the key components of all national security and crime prevention strategies".

2.6.2 The Regulation in Mauritius

The table which follows is a summary of the Mauritius Computer Misuse and Cybercrime Bill 2003(part II).

Table 1

Offences	Unauthorised/Illegal action	Max.Penalty
Unauthorised access to computer data	Knowingly accessing an unauthorized computer	5 Years and/or MRs50,000
Unauthorised disclosure of password	For Wrongful gain, unlawful purpose or prejudice	5 Years and MRs50,000
Unlawful possession of devices and data	Possession of an unlawful computer device or program/data to commit an offence	5 Years and MRs50,000
Unauthorised access to and interception of computer service	Including a function or data	10 Years and MRs100,000
	Computer System Operation impaired or data is suppressed/modified	20 Years and MRs200,000
Unauthorised modification of computer material	Modification of data	10 Years and MRs100,000
	Suppression, Modification or Reliability of a program or data held in a computer	20 Years and MRs200,000
Access with Intent to Commit offence	Convicted to secure access to a program or data	20 Years and MRs200,000
Damaging or denying access to computer system	Casing a degradation, failure or denial of access to the computer system	20 Years and MRs200,000
Electronic fraud	Fraudulently cause a loss or take advantage	20 Years and MRs200,000

For the international reader, the conversion rate of MRs into US$ is approximately MRs28.

The Computer Crimes Act also states that provisions are made to amend The Child Protection Act and the The Criminal Code (Supplementary) Act.

The above table offers an idea of the different penalties that cyber criminals will face if they commit an offence. However not much is known at the present on the number of crimes that have been committed in Mauritius. According to the Assistant Commissioner of Police, a few cases have been reported and are under investigations.

2.6.3 The Law enforcement

The Law enforcers face several challenges:

Firstly, there is the identification of the criminal – Internet investigations are equipment and labour-intensive. It is not that easy to identify cybercriminals.

This is because they operate in a virtual world and do not leave physical clues and paper trails behind, like the more traditional criminals do. Although they do leave their digital fingerprints now and then, enforcers need to move quickly before evidence fades away. Furthermore, with encryption, route relay and other types of technology and processes, they can make themselves almost undetectable by cyber-enforcers.

Besides legal differences, there are practical differences in terms of enforcement and co-ordination efforts between nations. There may not be enough trained personnel or sufficient equipment to detect and to bring cybercriminals to book.

Finally, technology is constantly evolving and the enforcers must keep up with changes.

The 1997 UN Manual on the Prevention and Control of Computer-Related Crime noted that 90% of economic crimes such as thefts of information and frauds were committed by the relevant company's employees. So laws and regulations must go together with the training of the staff.

The literature reviewed so far does not reveal much about the impact of the ACT and the number of crimes recorded at this point of time in Mauritius. It may be because the law is new and the major crimes have not been reported. In order to find out whether the local business has been or is at risk, the research questions in the section below will be tested.

2.7 The Research Question (Problem Statement)

There is no doubt that the impact and the extent of damages caused by Virus, Hackers and other cyber criminals stated above in this chapter has been very consequent on a global scale. These increase threats has driven the push to amend the law.
The Cyber crime act has been implemented in 2003 after a few months of debates regarding the security of computer users and the fast development of the ICT sector in Mauritius. Many countries and organisations including universities have faced the worst experience of cyber crimes. The down time and consequent loss resulting from these attacks can be very serious. Preventive actions need to be taken before this kind of disaster hit our local organisations. The threats of cyber crimes on the business organisation in Mauritius are real and need to be measured.

The research questions on this matter can be formulated as follows:-

- How much at risk is the Mauritius business community?
- Is there a proper structure to deal with this kind of crime?
- What is the general feeling of the cyber community about this law?
- What are the proactive roles of business organisations to prevent and control these crimes in Mauritius?

Answers to these questions will fill up the gap between the known part that is this literature review and the unknown part to be discovered in the next chapters.

2.8 Conclusion

After reviewing the available articles and reports regarding this matter, there are enough evidences that the Cyber crime problem will be one of the future concerns of the local authorities regarding the Safety and Security of the ICT users in general. However the business community represents the greater risk because of frauds and espionage.

The anonymity of the Internet also makes it an ideal channel and instrument for committing organized crime activities. The notion of a criminal underworld connotes a lack of transparency, where and who is doing what, is usually hidden from view. Secrecy is a key part of organized crime strategy and the Internet offers excellent opportunities for its maintenance. Actions can be hidden behind a veil of anonymity that can range from the use of ubiquitous cyber-cafes to sophisticated efforts to cover Internet routing.

The United States and other developed nations are already battling with these crimes and are seeking help and ventures with I.T professionals to enforce the law further. Specialized Forensic labs have started to offer their services. The methods used are very technological and requires continuous development to stay ahead of new flaws. Some countries are outsourcing these services but a delay in response may increase the damage of the crime. This shows that there must be a joint venture among all the stake holders like the Government, Businesses, I.T professionals, Telecommunication authorities and Legal services to create the necessary synergy for a fast and efficient action against Cyber crimes.

The methodology chapter which follows will provide the Instrumentation and Procedures to collect data for this research.

3. Research Methodology

A good Research methodology is very important to address the research questions and hypotheses. For that reason the Methodology section follows logically from the Statement of the problem. After a careful consideration of the research questions, a triangulated approach that is both partly qualitative and partly quantitative will be more appropriate.

A questionnaire became the most appropriate way to collect information while there was a need to confirm the real trend at the moment in Mauritius. In the latter case, an interview with the deputy commissioner of Police together with a workshop on the Intellectual Property Rights (IPR) have helped to understand the current status of the problem.

3.1 Plan of the study

This research is performed on a sample of IT Literate organisations in Mauritius in the ratio 40% Large, 30% Medium to large and 30% Small to Medium enterprises.

CIO, CTO and senior officers of major organizations will be targeted as well as those officers who together with the concerned authorities setup the necessary regulations. The sampling should be able to show how much concerned are the local organization regarding the threats which are facing them or may have faced them.

The questionnaire utilizes a cross sectional survey design (Appendix II) to assess IT professionals both in the private and public sectors. Interviews were carried out with the stake holders of the enforcement division of the police department. Focus group discussions or workshops have provided a better understanding of the actual situation. Secondary information is collected from government reports and surveys, and the internet.

3.2 Participants

The population selected for this study has been downloaded from the National Computer Board website (http://www.ncb.mu). They are companies that are already computerized and have at least an integrated network and a minimum of 5 staff. A short list of 100 participants, mostly from major organizations has been selected.

3.3 Measurement

The data collection questionnaire (Appendix II) was designed to receive information from the selected population. The questionnaire provides an easy and effective means of communication to the participants. In order to avoid legal issues, every precaution has been taken to obtain the informed consent of the participants. The participation was voluntary and anonymity was respected to those who wish so.

Legends are provided to help and guide the participants to answer in a fast and efficient way. The questionnaire's reliability and validity have been tested.

The questions were kept simple in a tabular format and most of them have a default possibility to be filled with an "X". Where the strength of the questions has to be measured, the first or left column will expect a low or poor answer and an "X" in the last right column with the strongest scenario. The lowest score is labelled "1" and the highest one is "5". Unless there is no answer for that particular question, it can be marked with an "X" in the corresponding N/A field.

3.4 Data Collection

A total 100 questionnaires were mailed and despatched in person. Two days after the questionnaires were sent to the participants, they were reminded by phone to return the completed questionnaire within 1 week. One week later, a follow-up survey was made to non-respondents and the latter were requested to do the necessary effort. A pick-up arrangement was also made so that the remaining questionnaires were returned as soon as possible.

A close follow up was made to ensure that the maximum number of completed questionnaire is collected. Where necessary a telephone number was offered for assistance.

Even if the population selected is a criterion sampling, a demographics section has been inserted to make sure that the participant fits a minimum criterion so that the results are not biased. He or she should be at least a computer literate person preferably at management level and has a proven experience in the IT field. An average internet usage and a proper network infrastructure within the organisation is an important requirement to be eligible for this survey.

The survey was conducted between the 15th November and 11th December 2004.

3.4.1 Questionnaire

The Questionnaire was divided into 3 sections:-

- Demographics
- Environment
- Computer Misuse and Cyber Crime Act Awareness

The Demographics envelops the Position of participant, the type of organization, his or her academic level, his management and computer experience, his gender, age and his means of access to internet.

The Environment includes a general knowledge of the internet security and the general environment regarding this matter. The Environment section is to help the participant to open up his mind regarding the flaws that may influence his working or business environment. His awareness about the internet security within his organization and the external factors that influence his organization was tested.

The last section of the questionnaire covers the main concern of this subject. The participants had to answer on related topics regarding Cyber crimes.

These include the Computer Misuse and Cyber Crime Act 2003 of Mauritius itself and knowledge about the flaws regarding his business as well as the regulations stipulated in the act. The main topics regarding this issue are:-

1. Internal factors regarding the participant and his organization.
2. Internet security
3. Purpose of internet usage
4. Frequency of backups and password change
5. Known or experienced threats
6. No. of these threats that hit your organization
7. His Opinion on most known offences
8. Awareness of the Cyber crime act

3.4.2 Interview

Interviews were carried out with senior officer of the police force to understand current status of the cyber crimes and also their logistics in place.

The interviews were carried out on: -

- Application of the ACT
- Type of frauds or crimes
- Available logistics
- Statistics

3.4.3 Focus group/Discussion

A seminar on the anti-piracy, intellectual property rights (IPR) and related crimes organized by the AMCHAM was attended on the 4th December 2004. A panel of international jurists specialised in these fields enhance the exposure of the cyber crimes. The workshop that followed generated more information and the discussions contributed a lot regarding the recent cases. The legal advisers also gave their opinion on the Cyber Crimes trend in the United States.

3.4.4 Data Analysis procedures

Microsoft Word has been used to capture the primary data and processed by Microsoft Excel. The data was then analysed and the results presented in tables and figures which appear in the result section.

A summary of the actual data collected is found in appendix III.

3.4.5 Validity and Reliability

There has been an adequate number of participants with the completion of 68 questionnaires. Interviews of senior officers of the police force were appropriate to meet the theoretical needs of the study.

The use of both questionnaires and interviews shows that there has been some triangulation. This means that data has been solicited from multiple sources.

3.5 Limitations of the study

Delimitation:-

- The research survey has been conducted according to law and regulations on THE COMPUTER MISUSE AND CYBERCRIME ACT 2003 of Mauritius (http://ncb.intnet.mu/mitt/ministry/download/misuse.pdf). Thus the table of offences and penalties referred in this study applies to Mauritius.
- The sampling was based on only IT literate organisations.

Limitation:-

- Even though all precautions have been taken to have a broad coverage of all the stakeholders in the ICT sector, there has been some reluctance from a few sectors like the banking sector for obvious reasons.
- Due to end of year festivities, a few questionnaires from the Manufacturing Sectors were not returned. It may have some negligible effect on the findings.

3.6 Summary

The methodology chapter has created the interactions between the above sections to meet the requirements of the Research Design. The primary data sources are from the Questionnaire, Interviews and Seminar attended. The secondary data were collected from the internet and Surveys previously conducted. The hypotheses are tested and discussed in section 4.2 of the next chapter which describe the results of the data collected.

4 Findings and Discussions

This chapter is organized in 2 sections.

1) The findings of the data collected and a detailed presentation of the results using charts.
2) The statistical analysis and discussions.

4.1 Findings

The interview realized shows that there has been a slight increase in the number of frauds committed on the internet and a few cases of unauthorized access.

The frauds have been made by hackers and unsolicited emails. These include:-

- Loss of data
- Nigerian Spam email
- Viruses

Regarding the unauthorized access, most of the reported cases were made by organizations which do not have a proper security procedure. Employees leaving a company have easy access to copy and even erase data which belongs to the latter.

Whenever necessary, the police officers call upon the State Informatics Limited services to verify the sayings of the complaints.

According to the assistant commissioner of Police, a bank of IT Specialists in Mauritius should be made available. Furthermore a centralized knowledge management is needed to offer a faster response time. He think that the provision made by the Computer Misuse and cyber crime Act 2003 is appropriate and believe that more awareness has to be made to the general public.

After that a quantitative analysis has been performed on the conducted survey, the following charts are accompanied by a brief explanation is presented. A deeper analysis on the statistics will be discussed in section 4.2.

The results of these data will be able to give better direction into the appropriate measure and recommendation to be formulated.

The section that follows presents the data collected in charts. Section 4.2 will discuss and provide further analysis to the different research questions.

4.1.1 Demographics

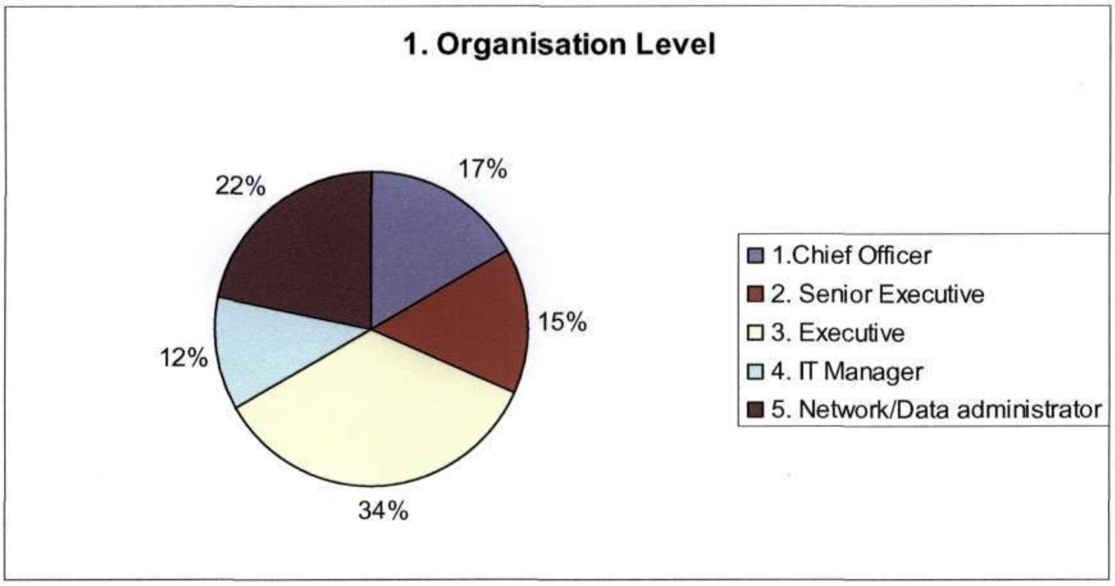

Figure 4.1

The above pie chart gives a representation of the % post occupied by the participants. Quite interesting to note that more than 2/3rd are at management level.

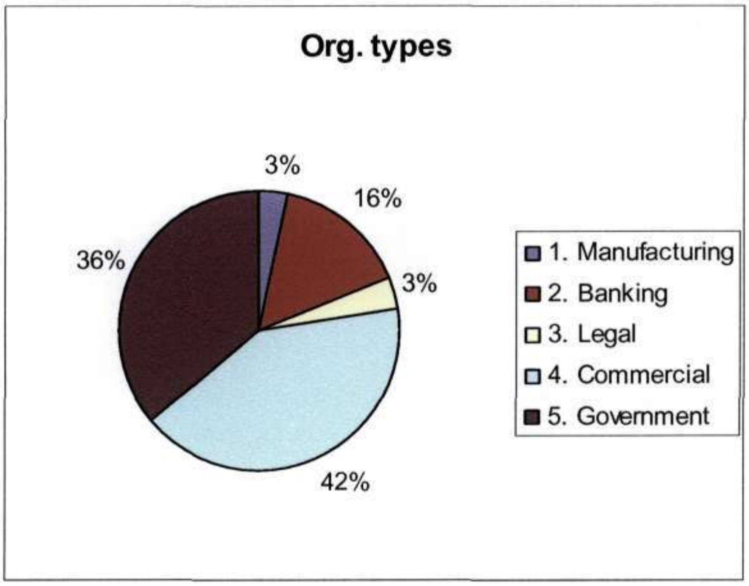

Figure 4.2

The private/commercial sector and the government sector represent the majority of participants. Due to end of year holidays, few replies were received from the manufacturing sector even though it should have represented at least 10% of all the sectors.

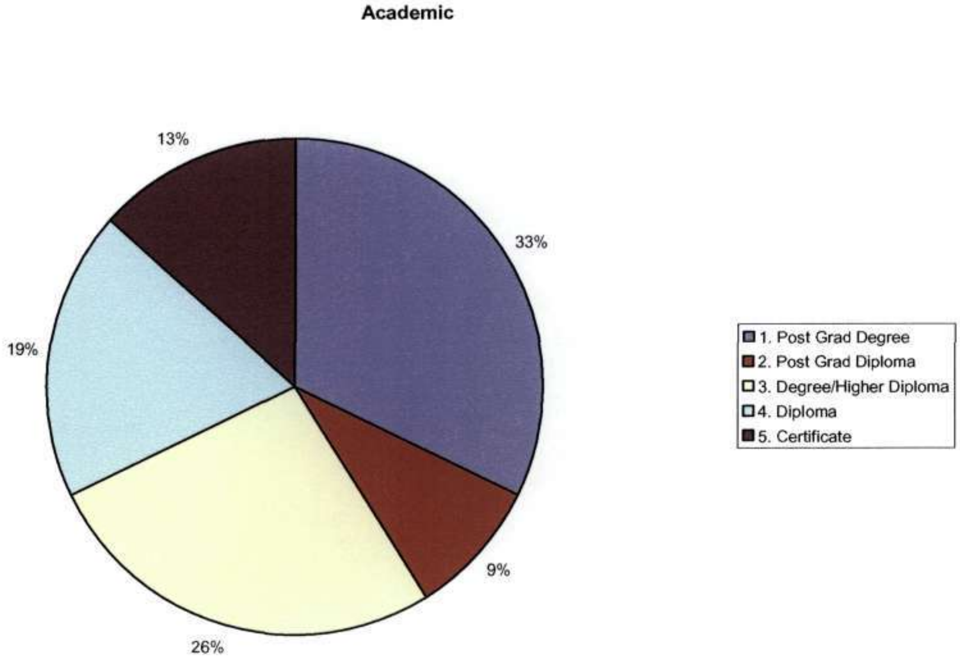

Figure 4.3

The above chart shows that 68% of the sampling participant is a graduate, the remaining having at least a Diploma or Certificate level. This shows that we are dealing with an educated sampling.

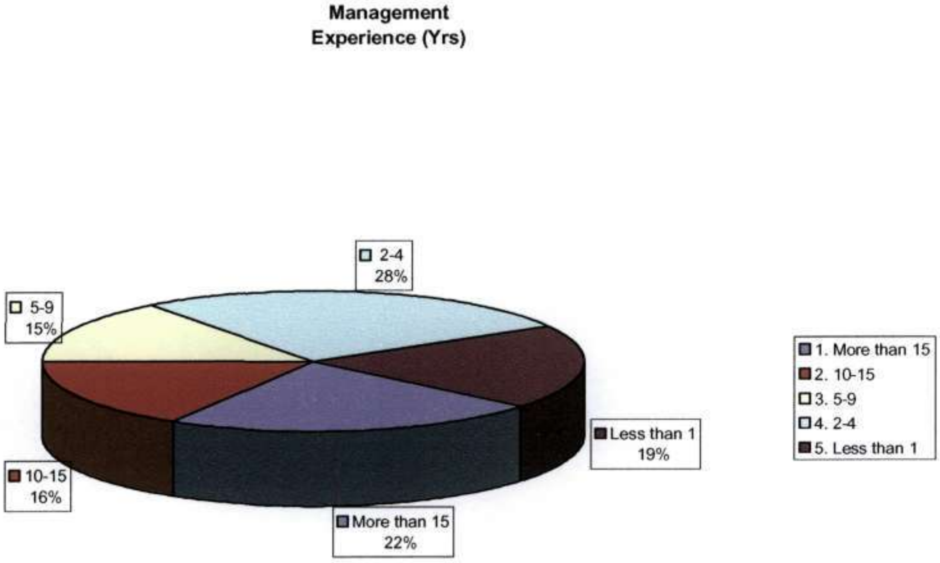

Figure 4.4

The sampling also shows that more than 50% of the participants have more than 5 years working experience at management level. They should be aware of the importance of security in their organization.

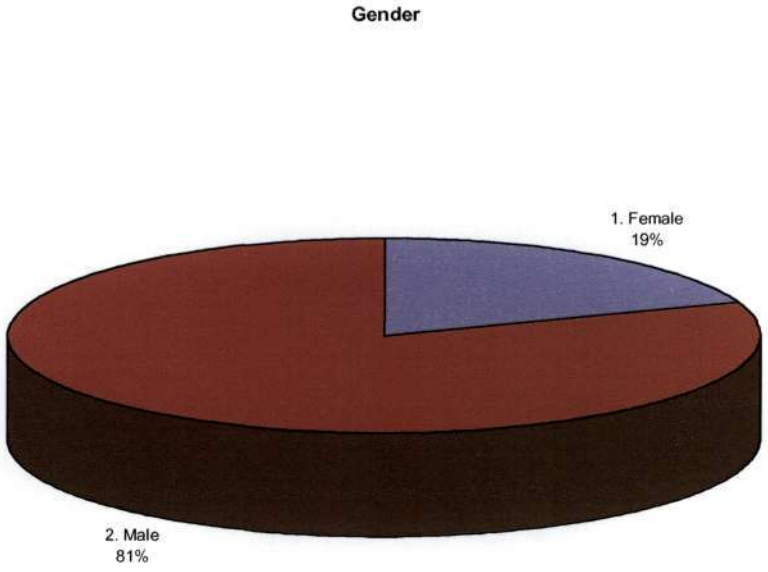

Figure 4.5

Quite interesting to note that most of the respondents were male. Does this mean that there are fewer female gender that become senior officers or likely to take responsibilities? The returned questionnaires show 81% male respondents.

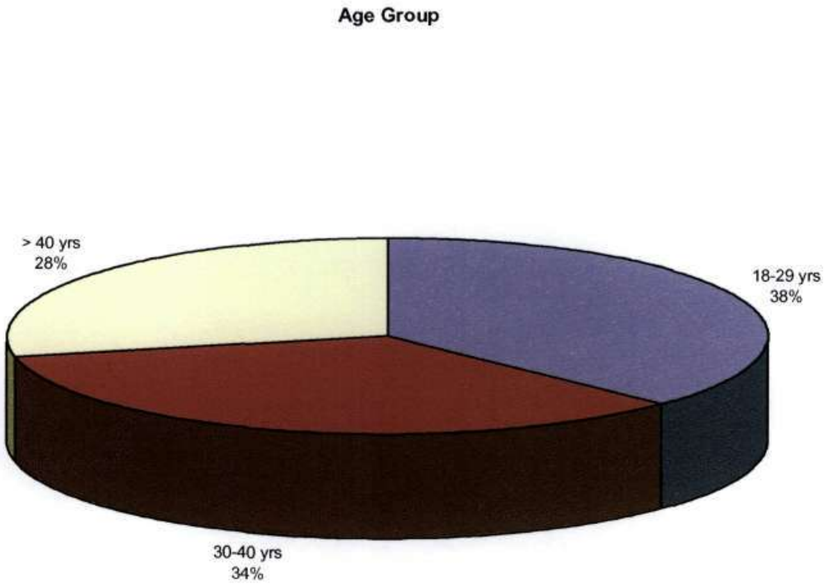

Figure 4.6

The age groups confirm the seniorities of the majority of the participants.

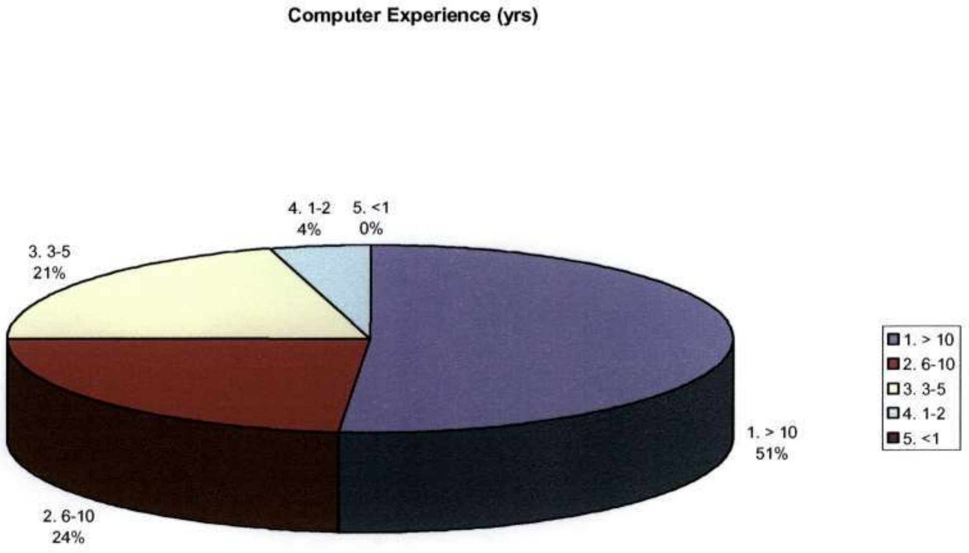

Figure 4.7

It is quite interesting to note that more than 50% of them have more than 10 years of computer experience.

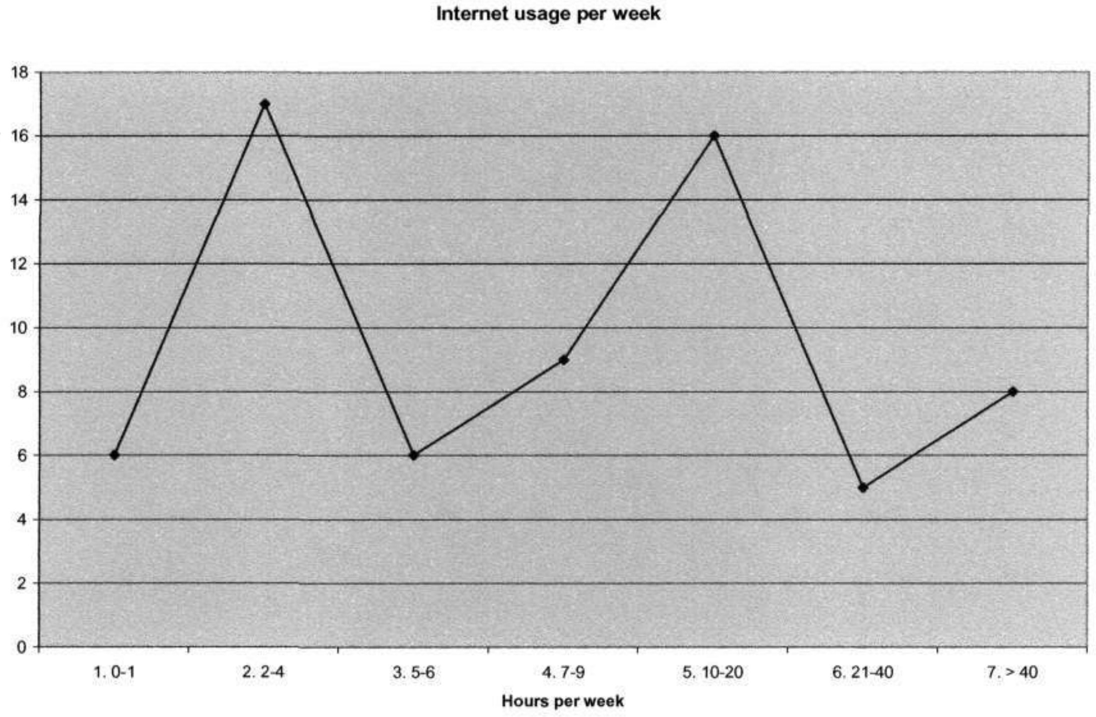

Figure 4.8

The above graphic shows that most participants spend between 2 to 40 hours on the internet per week. Since most of the business work 5 days a week, this mean that the average user spends 2-3 hours a day on the internet.

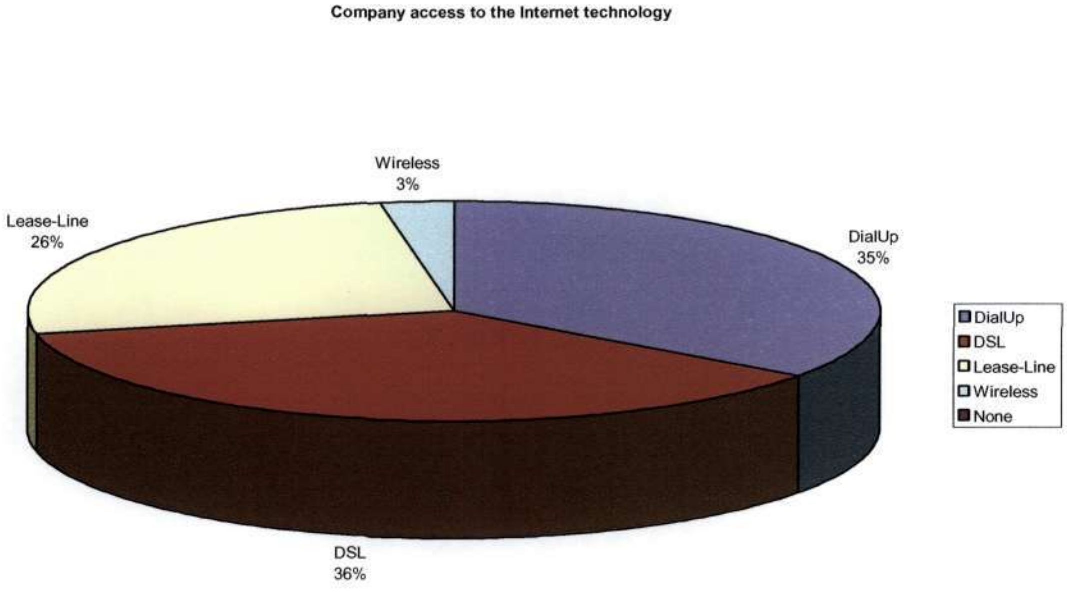

Figure 4.9

While the majority of users have access to a high speed bandwidth, there are still 35% of organizations that are using dial-up networks. Also note that the number of WiFi users is also increasing

4.1.2 General Environment

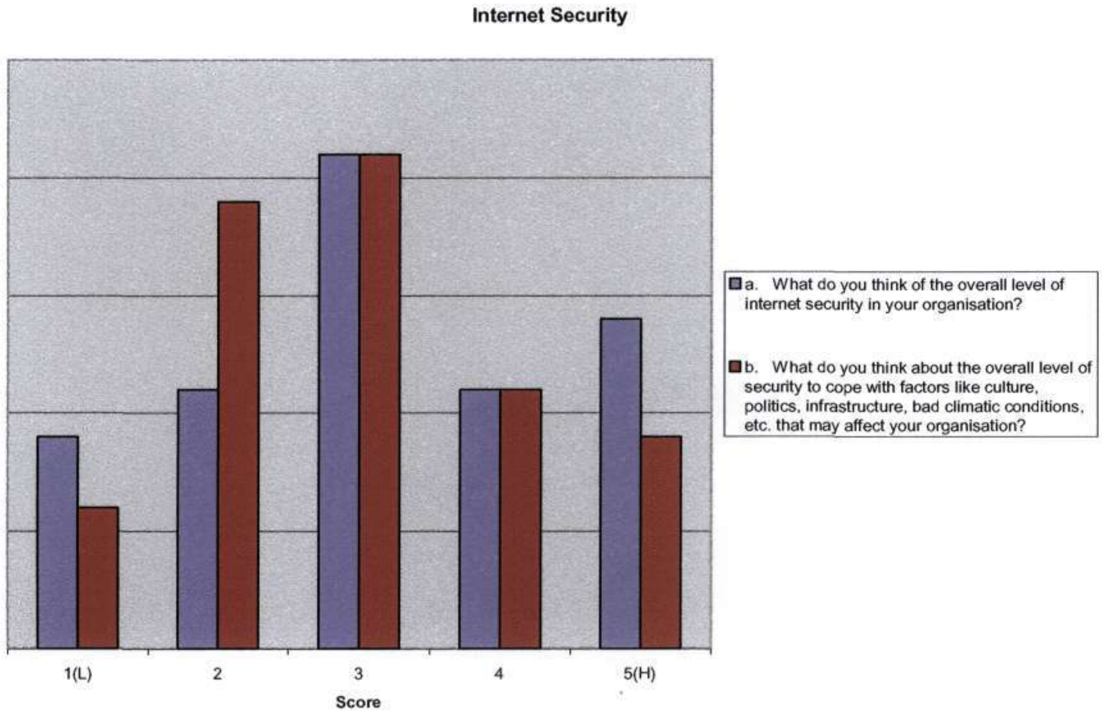

Figure 4.10

On a score of 1-5, the participants are being tested on the level of internet security in their organization as well as those external factors which may affect their organization. Quite surprising to note that around 50% of the participants believe that their internal security is not adequate while more than 50% think that major environmental factors have a direct effect on their organization's security.

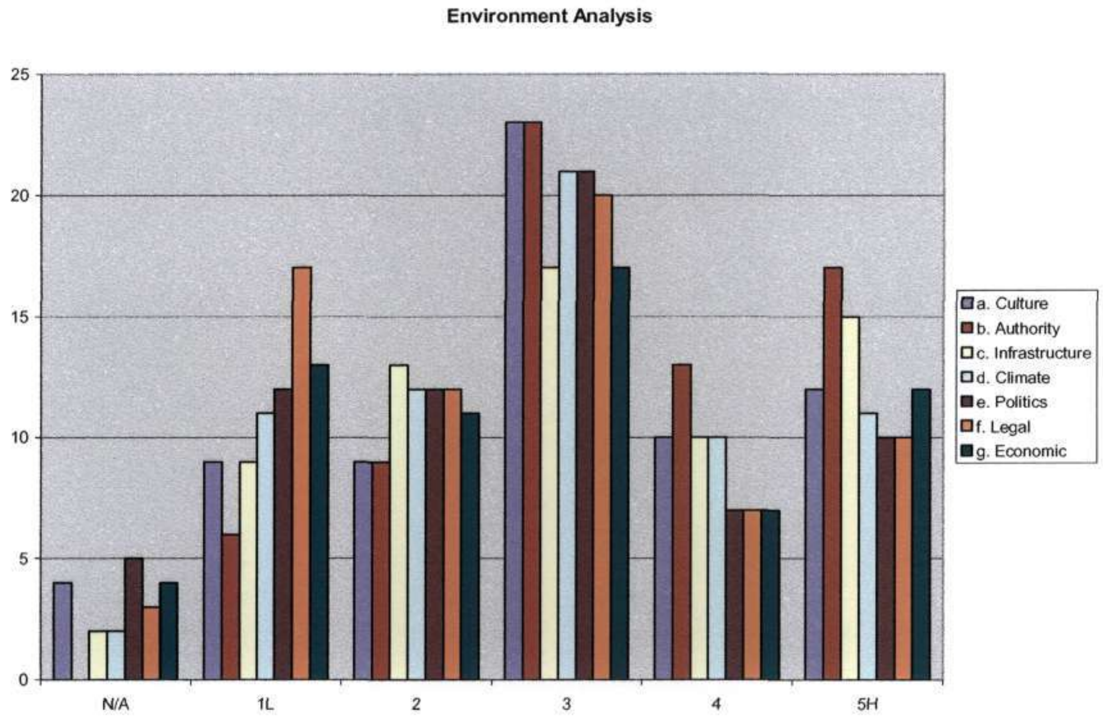

Figure 4.11

The major environmental factors (Culture, Authority, Infrastructure, Climate, Politics, Legal and Economics) are being tested individually. While only a few do not feel concerned by this question, there is a mixed feeling on the external factors, with the exception of Legal shortcomings where most organizations agree that it is difficult to fight or control the pirated software.

4.1.3 The Computer Misuse and Cybercrime Awareness

The results of this section will be presented using bar charts and statistics in section 4.2.

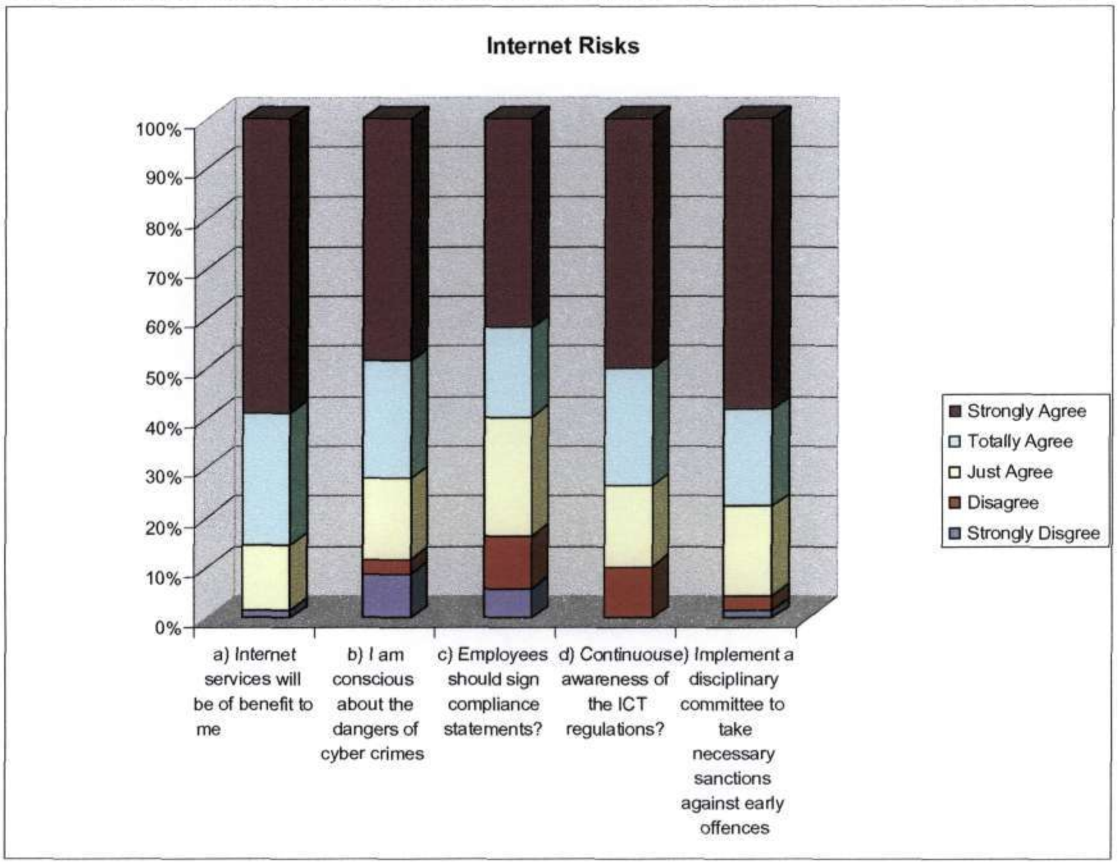

Figure 4.12

The following internal risks present in the organisation have been tested here:

- More than 60% of the participants agree that the usage of internet is benefiting them and that they are conscious about the threats.
- They also agree that employees should sign compliance statements and provided continuous awareness on the ICT regulations.
- It is quite interesting to note that most of them strongly agree to setup a disciplinary committee in their organisation to take corrective actions against early offenders.

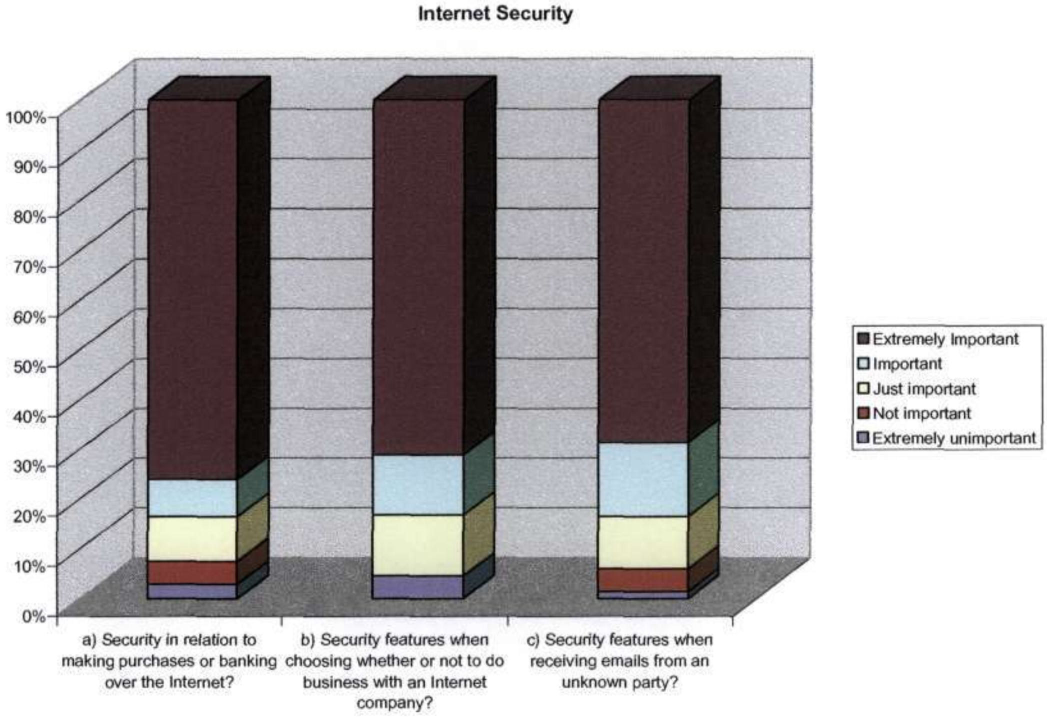

Figure 4.13

The internet security for e-commerce users shows that they all agree that it is extremely important to be fully secured for doing business on the internet.

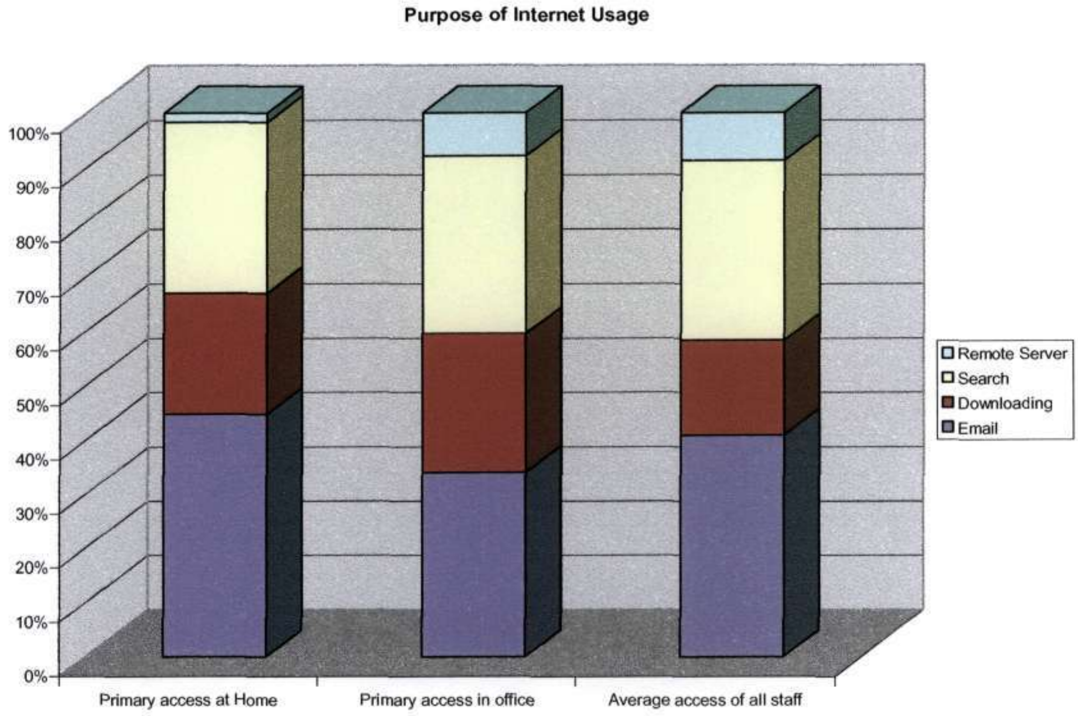

Figure 4.14

The primary usage of internet seems to be email and for research purposes.

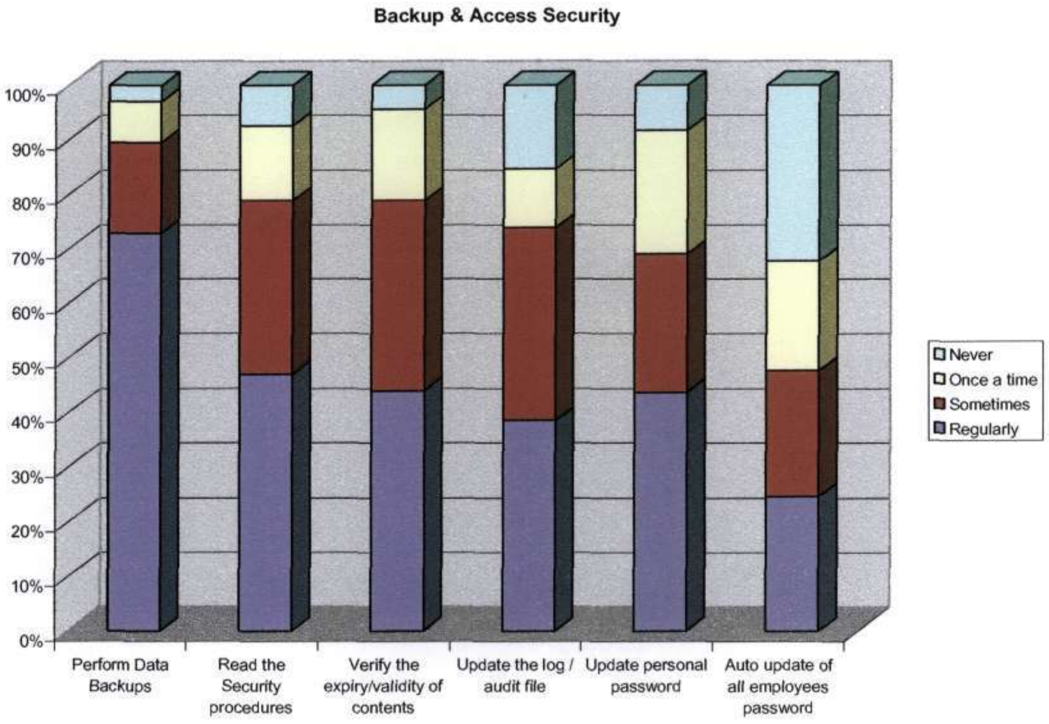

Figure 4.15

While most of the participants are following a proper backup procedure, the above chart shows that they are not taking enough precautions regarding the update of their passwords. If the passwords are not properly managed and secured, doors are opened to hackers. Changing the password regularly will minimise this risk.

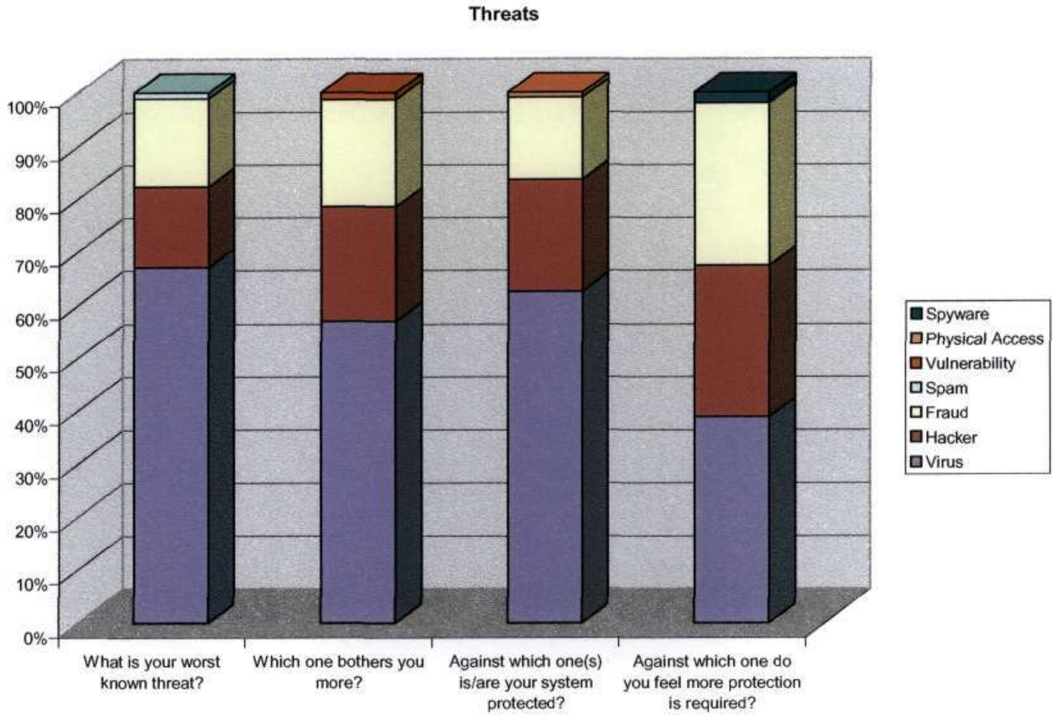

Figure 4.16

The above chart shows the percentage of known threats that the participants are aware of. Viruses are the main concern followed by hackers. A few cases of spyware have been noted.

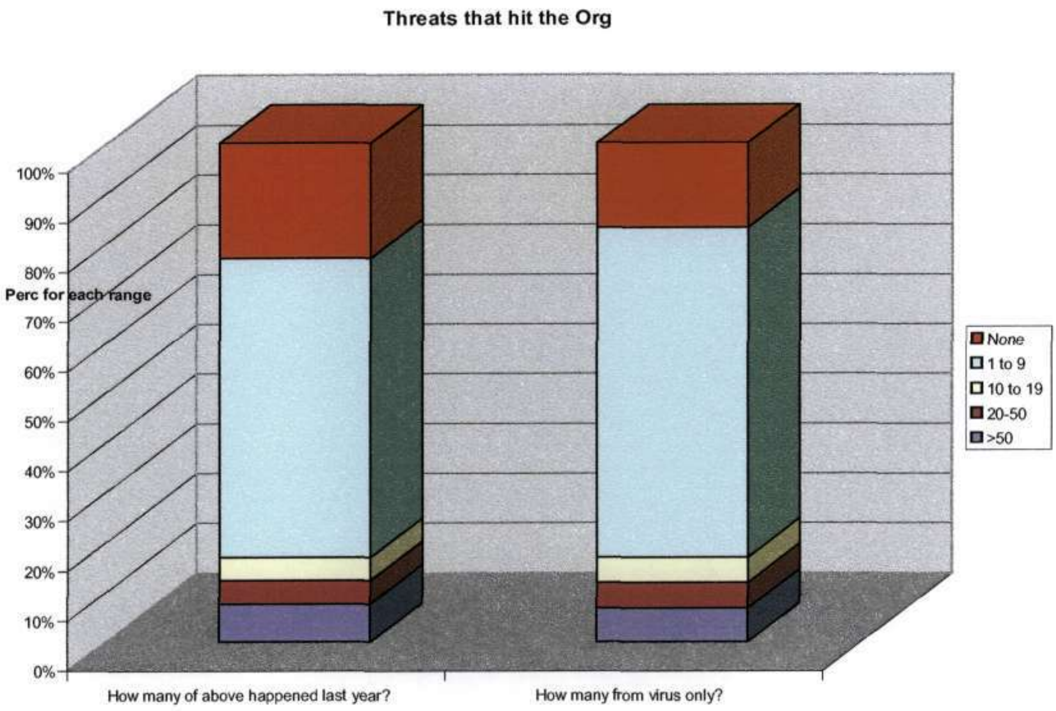

Figure 4.17

Of these known threats, viruses are the ones that have affected most of these organisations. Quite a few have been hit by more than 20 times in a year but most of them between 1-9 times in a year.

This shows that the risks of doing business on the internet is quite high and there have been so many cases unreported.

4.2 Discussion on the Statistical Analysis.

After reading the above charts and performing a cross analysis, some further statistics are obtained. It is noted that for each question a number of possible answers were given. Respondents were asked to tick off their answer(s) to each question. The purpose of this analysis is to answer each of the first 3 research questions, while the 4th one will be addressed in the Recommendation chapter.

4.2.1 How much at risk is the Mauritian business community?

4.2.1.1 Rating of overall internet security

The rating is on a scale from 1 (low) to 5 (high). A summary of the results are shown in the table below.

Table 2 - Rating of overall internet security

Rating	1	2	3	4	5
Number	9	11	21	11	14

mean = 3.15 standard deviation = 1.315

Nearly two-thirds (65.15%) of the respondents rated the overall security from 2 to 4, while about 1 in 5 (21.21%) gave it the maximum rating. There appears to be room for improvement of this rating.

4.2.1.2 Concern about certain security issues

Respondents were asked to rate their concern about security (on a scale 1 to 5) regarding (a) purchases or banking (b) doing business and (c) receiving e-mail.

Table 3 - Concern about certain security issues

Rating	1	2	3	4	5	Mean	% maximum rating
Purchases/banking[1)]	2	3	6	5	51	4.49	76.12
doing business	3	0	8	8	47	4.45	71.21
receiving e-mail	1	3	7	10	46	4.45	68.66

[1] The figure stated under the rating is the number of responses.

Respondents rate these security issues as extremely important (the mean is about halfway between 4 and 5 in all cases). A very high percentage (nearly 70 or more) allocate a maximum rating (5) to these issues. They seem to expect a higher rating than the one achieved according to the information in table 2.

4.2.1.3 Threats to computer security

Respondents were asked to answer 4 questions on threats. A summary (percentage responses) is shown in the table below.

Table 4 - Threats to computer security

Threat	virus	hacker	Fraud	spam
Worst known threat	67.1	15.3	16.5	1.1
Bothers most	57.7	21.8	20.5	0
Protection	63.1	21.4	15.5	0
More protection needed	39.6	29.2	31.2	0

Virus is by far the worst threat, has the most protection and will most need more protection in future. Hackers and fraud are not perceived to be big threats at the moment, but there is some indication that this might change in future. This can be seen from the fact that the percentages under "more protection needed" are considerably higher than those under "protection". There seems to be little threat besides virus, hacker and fraud (spam was mentioned as a threat by one respondent).

4.2.1.4 Number of threats

Table 5 – Number of threats last year (12 months)

Number	none	1 to 9	10 to 19	20 to 50	above 50	mean	% below 10
Number all threats	15	39	3	3	5	10.28	84.4
number viruses only	10	39	3	3	4	10.23	83.1

The above table shows that

1 on average about 10 threats a year occurred.

2 very few threats other than viruses occurred. The counts and the means for all threats and viruses are virtually identical. This confirms the point made in section 2.3 (that viruses are by far the worst threat).

3 for over 80% of the respondents less than 10 threats occurred.

4.2.1.5 Rate of occurrence of threats

A frequency distribution of internet usage is given in the next table.

Table 6 – Hours per week internet usage

Hours	**0 to 1**	**2 to 4**	**5 to 6**	**7 to 9**	**10 to 20**	**21 to 40**	**above 40**
Number	6	17	6	9	16	5	8

mean = 14.20 hours per week = 14.20 x 52 = 738.4 hours per year.

Nearly 80% (79.10%) of the respondents use the internet from 2 to 40 hours per week i.e. from 104 to 2080 hours per year.

On average the threat of a virus should occur every 738.4 / 10.23 = 72.18 hours of internet use. This amounts to roughly 1 virus threat every 5 weeks on average. Using the Poisson probability distribution, the following probabilities can be calculated.

Table 7 – Probability distribution for number of viruses for 5 weeks internet use

Number	**0**	**1**	**2**	**3**	**4 or more**
Probability	0.368	0.368	0.184	0.061	0.019

From the above table it can be seen that probability (2 or less viruses in 5 weeks) = 0.92.

In reply to question 4.2.1 regarding the level of risk the Mauritius Business is facing, the following points are noted:-

i) While table 2 shows that there is room for improvement, table 3 shows that the respondents are very much concerned with the security issues. This confirms that Security still remains a major concern for them.

ii) While tables 4 & 5 indicate that viruses are the main threats coming from the cyber criminals, tables 6 & 7 show that there is a probability that a computer is being attacked once or twice every 5 weeks.

These 2 points summarise the business community concern regarding the risk their business are facing. At the same time they are conscious about the potentiality of the other cyber crimes. These points confirms the trend that is referred in section 2.3.2 of the literature review regarding this issue where 75% of emails circulated in 2004 were junk and over 100,000 viruses were created.

4.2.2 Structures for dealing with cyber crimes

4.2.2.1 Backups / Password Security

Table 8

How often	never	once a time	sometimes	regularly	mean[1)]
Data backups	2	5	11	48	2.59
Read security procedures	5	9	21	31	2.18
Verify validity of contents	3	11	23	29	2.18
Update log / audit file	10	7	23	25	1.97
Update password	6	16	18	31	2.04
Auto update all passwords	21	13	15	16	1.40

1 The calculation of the mean is based on coding "never" as 0, "once a time" as 1, "sometimes" as 2 and "regularly" as 3.

From the above table it can be seen that all the measures except data backups and auto update of all passwords are done "sometimes" on average. Data backups are done a bit more frequently on average (between "sometimes" and "regularly") and auto update of all passwords less frequently (between "once a time" and "sometimes").

4.2.2.2 Cyber crimes, the cyber crime act and how to deal with it

Respondents had to rate their knowledge of cyber crime issues on a scale from 1 (low) to 5 (high). The results are summarized in the following table.

Table 9 - Cyber crime issues

Issue	**1**	**2**	**3**	**4**	**5**	**Mean**	**rank[1)]**	**% max**
Awareness	13	15	18	6	11	2.79	3	17.5
Have copy of act	28	4	10	6	12	2.50	4	20.0
Awareness of penalty	24	13	9	3	5	2.11	6	9.3
Feeling more secure with act	11	11	19	11	12	3.03	2	18.75
Know how to report cyber crime	36	9	7	6	4	1.92	7	6.5
Resources available	32	11	14	6	0	1.90	8	0
Enough qualified lawyers	32	17	7	2	2	1.75	9	3.3
Local cyber criminals	19	15	15	9	3	2.38	5	4.9
Foreign cyber criminals	9	5	11	16	20	3.54	1	32.8

[1] Rank 1 means respondents rate the issue highest, rank 2 second highest etc.

From the table above it can be seen that respondent's knowledge of the issues can be improved upon. A lack of qualified lawyers, resources and knowledge on how to report a cyber crime seems to be the most serious of the respondent's problems.

However, from table 8, the structures within the organisations seem to be in control of the cyber crimes except for the frequency of updating the passwords regularly is below average.

The results to this question show some contrast. While the internal system is quite secure, the respondents feel that there are not enough resources to control these avenues.

4.2.3 General feeling of cyber community on cyber crime practices and act

4.2.3.1 Computer misuse and cyber crime awareness

The respondents had to state their degree of agreement (or disagreement) with some aspects of internet computer use and misuse.

Table 10 – Computer use, misuse and cyber crime awareness

	Agreement[1]						
Factor	-2	-1	0	1	2	mean	Rank
Internet services beneficial	1	0	9	18	40	1.41	1
Aware of dangers of cyber crime	6	2	11	16	33	1.00	4
Sign compliance statements	4	7	16	12	28	0.79	5
Awareness of ICT regulations	0	7	11	16	34	1.13	3
Disciplinary committee for early offences	1	2	12	13	39	1.30	2

[1] Strongly disagree was coded as -2 and strongly agree as 2.

The answers are all just above or just below the "agree" rating. Respondents rate their agreement strongest on the issue that internet services are beneficial and weakest on signing compliance statements.

4.2.3.2 Backups / access and cyber crime issues

See section 4.2.2 for discussion.

4.2.3.3 Opinion on seriousness of known offences

The respondents had to express their opinion [on a scale from 1 (low) to 5 high)] on the seriousness of some known offences.

Table 11 - Opinion on seriousness of known offences

Offence	**1**	**2**	**3**	**4**	**5**	**mean**	**Rank**
Data/programs manipulation	4	10	18	11	21	3.55	2
Theft of data/programs	9	5	18	14	17	3.40	4
Data/programs alteration	6	8	18	15	17	3.45	3
Unauthorized copying of data/programs	5	1	23	13	22	3.72	1
Computer forgery	8	8	18	11	18	3.37	5
Disgruntled employee	11	12	17	11	13	3.05	7
Independent hacker of info broker	12	10	19	10	11	2.97	8
Industrial espionage	14	17	12	8	13	2.83	10
Ignorant user	17	10	16	9	12	2.83	10
Hackers	11	8	17	9	19	3.26	6
Cyber terrorism	16	17	8	7	15	2.81	12
Cyber vandalism	16	13	11	8	15	2.89	9
Cyber stalking	19	12	12	5	15	2.76	13

According to the respondents the most serious known offences have to do with tampering with or unauthorized copying of data/programs and computer forgery. Cyber crimes are rated less serious than these offences.

Referring to table 10, the respondent agrees to the fact that the internet has been beneficial to businesses but they are quite reluctant to sign compliance certificates. From table 11, surprisingly it is noticed that the respondents are more concerned about internal threats such as data manipulation and copying than about hackers.
Here there may be a need to do some further research on the reasons of such behaviours and what is wrong in their procedures.

The above sections 4.2.1 to 4.2.3 resumes the first 3 research questions and the 4th research question on prevention and control will be answered in the next chapter.

5. Recommendation/Conclusion

The following sections may appear harsh and overly dramatic. But it needs to be stated. The cyber-crime attack threat and the enormous potential financial losses are very real. The awareness wake-up call needs to be shouted from the roof tops. Furthermore, every organization, officer, director and professional needs to note that his organization is most of the time exposed to significant damage and direct financial losses. Continuous review is required to mitigate this current exposure.

In light of the existing research studies and in consideration of the findings, cyber crime attacks will continue to escalate until a proper Network Security System is implemented and the law has taken control over this wild territory.

These major crimes are committed by virus writers, hackers and the spywares. Furthermore new types of escalating crimes including phishing, teenage kicks and moving target need to be monitored closely in this new era of the wireless (WiFi) environment. Hardware manufacturers, system integrators and other network security providers have to work together to design a new 'attack proof' device for the safety and security of their respective networks. These networks can be the internet service providers, telephone networks, mobile phone networks and all types of wireless networks.

5.1 Recommendation

Referring to the findings in chapter 4 and in line with the literature review in chapter 2, there is an indication for an urgent plan on awareness on cyber crimes. This reflection may answer the 4th research question "Proactive roles of business organizations to prevent and control cyber crimes"

The role of business in the prevention and control of cyber crimes can be classified into 2 broad categories.

A) Making available to the business community up to date information on cyber crimes and how to combat them.

1.1 Information on viruses.

1.2 Information on hackers and fraud.

1.3 Knowledge on how to report cyber crimes.

1.4 Knowledge of cyber crimes act.

1.5 Make community more aware of the dangers of cyber crimes.

B) The use of tried and trusted resources to combat such crimes.

2.1 Regular updates on all passwords.

2.2 Train more lawyers that are qualified to deal with the legal aspects of cyber crimes.

2.3 Make more resources available. This can range from programs for combating viruses, theft and hackers to security protocols.

2.4 Limit access (even among employees) to important data and programs.

2.5 Stay up to date with the latest methods of checking the integrity of incoming e-mail and any other internet information that might be down loaded.

There is also a need for the process of reporting and controlling these crimes.

5.1.1 Reporting a Cyber Crime.

To some extent, how to report a cyber crime depends on what kind of crime has been committed. As a general rule, though, the local law enforcement authorities like the nearest police station should be informed. It is also important to report the case to the Specialized IT unit in the police head quarters. This will give both the policy unit and the police a chance to address the offence in question.

5.1.2 Controlling Cybercrimes.

✓ Install hardware and software that will recognise hacker attacks, data spying and data altering, like firewalls, encryption (for e-mail, the encryption program called Pretty Good

Privacy can be used), virus detection and smartcards. An Intrusion Detection System can protect your information systems in the event of the failure of the firewall and from internal attacks. An Incident Handling System will be able to identify hacker attacks as they happen. Full backups are important so that evidence like damaged or altered files, files left by the intruder, the relevant IP address and login times can be collected. A police report should then be made.

✓ Assess your information systems to identify weaknesses.

✓ Ensure that computers that run critical infrastructure are not physically connected to any other computer that is possibly connected to the Internet.

✓ Maintain clear and consistent security policies and procedures.

✓ Use alphanumeric passwords (i.e. passwords with letters and numbers in them). Login passwords should be changed frequently.

✓ Employees have to be trained to understand security risks – this practically means that they must know that they should never give out PINs, passwords and calling card numbers of the company without proper third party verification.

✓ Correct identified problems – although this may seem straightforward and logical, I have seen many cases where security of certain information systems was compromised because problems were not fixed.

✓ Report attacks to the local ICT Security and Emergency Response Centre so that any pattern of cybercrime in the Country can be detected and large-scale attacks prevented.

✓ There must exist incident response capabilities so that there is appropriate action taken against impending attacks.

✓ When external parties service your system, save confidential information on other media before the service. Observe them during the service. Never let external people take computers or servers with confidential information from your site.

✓ When an employee resigns or is terminated, employers must always ensure that the former does not have access to their computers anymore and ensure that all relevant passwords have been changed.

5.2 Conclusion

Although this report can provide a snapshot of the prevalence and impact of Internet crimes, care must be taken to avoid drawing conclusions about the "typical" victim or perpetrator of these types of crimes. Complainants can be found in dozens of countries worldwide, and have been affected by everything from work-at-home schemes to identity theft. The ability to predict victimization is limited, particularly without the knowledge of other related risk factors (e.g., the amount of Internet usage or experience), the survey shows that many organizations agree that education and awareness are major tools to protect individuals.

Despite all the proactive efforts, some individuals may find themselves the victims of computer-related criminal activity because they have not exerted that minimum precaution.

In reviewing statistics contained in this report, it is recognized that consumers may characterize crime problems with an easier "broad" character, which may be misleading. There are indications that Mauritius will follow the same trend of developing countries. The % occurrences in the United States from section 2.3 of the literature review compared to the results and statistics in chapter 4, confirms that Mauritius will not be an exception to Cyber Criminals. The internal threats the organisations are facing, like data manipulation and forgery need to be fixed urgently. The cyber crimes are however more difficult to handle since they keep on evolving.

For instance, someone that gets lured to an auction site, which appears to be eBay, may later find that they were victimized through a cyber scheme. The scheme may in fact have involved SPAM, unsolicited e-mail inviting them to a site, and a "spoofed" website which only imitated the true legitimate site.

Support from many key Internet E-Commerce organizations is important to trace cyber criminals. An association regrouping all these stakeholders has become a reality to adopt a pro-active posture in teaming with the IT Policy unit and responding to cyber crime schemes.

Whether a bogus investment offer, a dishonest auction seller, or a host of other Internet crimes, the Internet Crime Complaint Center should be in the position to offer assistance. Government-private sector cooperation of this kind is not always easy, and has been particularly fraught in the area of information security, particularly regarding the issue of reporting. There is broad agreement that cyber-crime is under-reported. One of the most important and understandable reasons is concern on the part of financial institutions and businesses about reputation damage. For e-commerce to continue to expand rapidly, transactions must be perceived to be secure – and there is a natural desire to avoid any disclosures that might undermine customer confidence and place a company at a competitive disadvantage. Unfortunately, this reticence works in favour of the criminals. One useful approach, therefore, would be for organisation within a particular sector to agree to share information about cyber-crimes among themselves, on the assumption that similar methods and techniques that are used against one are also likely to be used against others. Even more important though is the development of mutual trust between business and law enforcement. Indeed, there are several instances of companies working closely with law enforcement in responding to cyber-threats.

Individual firms obviously have to tailor their security programs to their particular vulnerabilities and needs. Unless they recognize that organized crime and cyber-crime are becoming more convergent, however, their programs are unlikely to be sufficient.

Through an online complaint and referral process, victims of Internet crime can be provided with an easy way to alert authorities, at many different jurisdictional levels, of a suspected criminal or civil violation.

Generally speaking, the internet offers for business growth but it is wise to consider the recommended proposition before any major attack happened. At the moment there is a major concern that Virus is the main threat but there is also a high perception that the businesses are not enough protected against other threats.

The impact of cyber crimes on the Mauritius business community has created a lot of stress on the development of e-commerce and lack of trust to maximise the usage of the internet services.

The absence or lateness in the appropriate regulations is calling organisations to remain cautious. The amount of idle time may be the reason for the slow integration of e-business.

From the answers of the research questions, the business community feels that doing business on the internet is still at risk and some believes that the country does not have all the necessary resources to deal with the cyber crimes. One reason could be the lack of awareness of the Computer Misuse and Cyber Crime Act 2003 (ACT). Another reason could be that their focus is too much on the internal frauds.

In any case the ACT (refer to table 1) has catered for all types of crimes but unfortunately there is a misperception about this law due to a lack of awareness.

This situation shows that an immediate campaign for awareness and prevention of cyber crimes is required.

The findings of this research show that there is a need to make additional research on:-
“Why is the % threat on computer tampering so high”?

List of Acronyms

ACT	Computer Misuse and Cyber Crime Act 2003
AMCHAM	American Chamber of Commerce, Mauritius
CIO	Chief Information Officer
CTO	Chief Technology Officer
I.S or IS	Information System
I.T or IT	Information Technology
ICT	Information Communication and Technology
NCB	National Computer Board
WiFi	Wireless network Environment
ISP	Internet Service Provider

Bibliography

- A recent survey by Earthlink and Webroot , http://www.earthlink.net/spyaudit/press/
- Advanced Cyber-crime Attack Protection (ACAP)
- AusCert, Deloitte Tocuhe Tohmatsu and NSW Police, 2003 Australian Computer Crime and Security Survey, by AusCERT,
- AusCERT, Deloitte Touche Tohmatsu and the NSW Police. 2002. Australian
- Cahoot Bank case, http://news.bbc.co.uk/go/em/fr/-/1/hi/business/3984845.stm)
- Ciphertrust. Spoofing of IP addresses, http://news.bbc.co.uk/go/em/fr/-/1/hi/technology/3762264.stm
- Common crimes and frauds, http://www.net-intrusion.com/member/data/fraud_info.html
- Computer Crime and Security Survey
- Cyberattacks on financial systems, (http://news.bbc.co.uk/go/em/fr/-/1/hi/world/americas/3761946.stm)
- CyberStalking, (http://www.crimelibrary.com/criminology/cyberstalking)
- Doland,A. International law enforcement, (http://lists.insecure.org/lists/isn/2000/Jul/0056.html).
- E-Crime Watch Survey, (http://www.csoonline.com/releases/ecrimewatch04.pdf
- **Forrester Research, http://www.glreach.com/eng/ed/art/2004.ecommerce.php3**
- **Ghauri P & Gronhaug K. ,2002. Research Methods in business studies. England.** Prentice Hall.
- Gillham, B. (2000). The research interview
- Girden E.R. 1992. Annova repeated measures. USA. Sage Publications Inc.
- Goodman, L.A (1984) The Analysis of Cross-Classified data having ordered categories.
- Hacking, http://archives.cnn.com/2001/TECH/internet/11/19/hack.history.idg/.
- Hardy & Bryma. (2004) Handbook of Data Analysis
- http://www.acapsecurity.com/html/CYBER_SECURITY_REPORT.htm)
- Identity Theft, United States General Accounting Office (GAO) Report to U. S. Congress, GAO-02-363, March 2002

- Internet Crime Complaint Center , (http://www.ifccfbi.gov/strategy/2003_IC3Report.pdf)
- Lawrence E, Newton S, Corbitt B, Braithwaite R and Parker C, 2002, Technology of Internet business.
- Marsh, C. (1988) Exploring data
- Mauritius Police Force & Safer Africa. 2004. Mauritius Crime Survey 2004.
- Microsoft sets sights on spyware, http://news.bbc.co.uk/1/hi/technology/4104129.stm
- Multimedia Super Corridor (MSC), (http://www.msc.com.my/cyberlaws/
- National Cyber Security Alliance (NCSA) of the United States, (http://www.staysafeonline.info/index.html)
- Phishing, (http://news.bbc.co.uk/1/hi/technology/4072647.stm)
- Pilcher, D.M (1990) Data Analysis for the helping professions. USA. Sage Publications, Inc.
- Rudestam K.E & Newton R.R. 2001. Surviving your dissertation. USA. Sage Publications, Inc.
- Santee Worm, (http://news.bbc.co.uk/1/hi/technology/4117711.stm)
- Sapsford, R. (1999). Survey Research. London. Sage Publications Ltd
- Savino, A. Cyber- Terrorism, http://www.cybercrimes.net/Terrorism/ct.html.
- Security loophole, http://news.bbc.co.uk/go/em/fr/-/1/hi/technology/3921515.stm
- Spim, (http://news.bbc.co.uk/2/hi/technology/3581148.stm)
- Swen worm, (http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SWEN.A
- THE COMPUTER MISUSE AND CYBERCRIME ACT 2003 of Mauritius (http://ncb.intnet.mu/mitt/ministry/download/misuse.pdf).
- The National Computer Board (http://www.ncb.mu)
- The National Strategy to Secure Cyberspace, Feb 2003
- The Online Oxford Dictionary(http://www.oxfordreference.com/views)
- The Oxford Reference Online Encyclopedia, (http://www.oxfordreference.com/views)

- Tips on protections of cybercrimes, (http://www.cybercellmumbai.com/General%20Tips/General%20tips.htm)
- Virus and Worms, (http://www.bainet.com/main.php?mode=displaysection&i_d=6&PHPSESSID=)
- Ward, M. Increase in cybercrimes, (http://news.bbc.co.uk/1/hi/technology/4105007.stm)
- Wei, H.K. Computer users, Don't be weakest security link, http://straitstimes.asia1.com.sg
- Weinberg, D. (2002) Qualitative research method
- Wensense inc.Industrial Espionage, http://www.net-security.org/press.php?id=1614

Appendices

I. The Federal Information Security Management Act (FISMA)

The source of FISMA is Public Law 107-347, the E-Government Act.

The E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) which was signed by the President on December 17, 2002 and became effective on April 17, 2003. Title III of the Act is known as the Federal Information Security Management Act (FISMA), which amends and supersedes Public Law 106-398, Title X, Subtitle G, "Government Information Security Reform Act (GISRA)," dated October 30, 2000. Source: ACAP System Introduction Book, Book One, Release 2.0.

II. Survey Questionnaire

Survey on The Impact of the Computer Misuse and Cybercrime Act on the Business Community in Mauritius.

Definitions

This questionnaire has been divided into three sections as follows:-

Part A: Demographics

Part B: Environment

Part C: The Computer Misuse and Cybercrime Awareness

To fill it, please insert an **X**, in the box that corresponds more likely to your answer. The following legends will help you to complete the table.

N/A implies Not Applicable.

1 means the Lowest or poorest in some cases
5 means the Highest or best scenario

This questionnaire has been designed so that you can reply to the questions in a fast and efficient way. I will be grateful if you can allocate about 10-15 minutes of your valuable time for this study. For any additional help please give me a call on 7285991 or email to me below.

Should you wish to receive a copy of this research, kindly fill in the (optional) information below (will be kept confidential):-

1. Name ______________________________
2. Position held ______________________________
3. Please provide your email/postal address
____
____
____

I thank you for your cooperation and the time allocated to make this survey a success.

Regards,

Nasser Jamalkhan.
Email: Packard@intnet.mu

A. Demographics

1.Organizational Level	
1. Chief Officer	
2. Senior Executive	
3. Executive	
4. IT Manager	
5. Network/Data administrator	

2. Type of organization	
1. Manufacturing	
2. Banking	
3. Legal	
4. Commercial	
5. Government	

3. Academic	
1. Post Grad Degree	
2. Post Grad Diploma	
3. Degree/Higher Diploma	
4. Diploma	
5. Certificate	

4. Management Experience (in years)	
1. More than 15	
2. 10-15	
3. 5-9	
4. 2-4	

5. Less than 1	

5. Gender	
1. Female	
2. Male	

6. Age	
1. 18-29	
2. 30-40	
3. > 40	

7. Years experience as a computer user	
1. > 10	
2. 6-10	
3. 3-5	
4. 1-2	
5. <1	

8. Internet usage – hours per week	
1. 0-1	
2. 2-4	
3. 5-6	
4. 7-9	
5. 10-20	

6. 21-40	
7. > 40	

9. Basic Infrastructure Existence	**Dial Up**	**DSL**	**Lease-Line**	**Wireless**	**None**
Company access to the Internet technology					

B: General Environment

1. Internal - Security	**1(L)**	**2**	**3**	**4**	**5(H)**
a. What do you think of the overall level of internet security in your organisation?					
b. What do you think about the overall level of security to cope with factors like culture, politics, infrastructure, bad climatic conditions, etc. that may affect your organisation?					

2. External factors	**N/A**	**1 L**	**2**	**3**	**4**	**5 H**
a. Culture Existence of an organisational culture as an integrated team.						
b. Authority Management Pro-activeness so that decisions are not delayed. (Awareness, prevention, etc).						
c. Infrastructure Ability to cope with infrastructure problems (e.g. Networks LAN, WIFI, training, communication etc).						

d. Climate Ability to cope with delays due to natural calamities (like storms and thunder) which damage power and tel. lines.						
e. Politics Ability to cope with politics which may influence the ICT regulations.						
f. Legal Ability to cope with legal shortcomings (e.g. inadequate protection against software piracy, etc)						
g. Economic Ability to cope with economic situation (e.g. A bad economic situation may discourage usage of proper security investments).						

C: The Computer Misuse and Cybercrime Awareness

1. Internet Risks	**Strongly disagree**				**Strongly agree**
	1	**2**	**3**	**4**	**5**
a) Internet services will be of benefit to me					
b) I am conscious about the dangers of cyber crimes					
c) Employees/Customers should sign compliance statements?					
d) Continuous awareness of the ICT regulations?					
e) Implement a disciplinary committee to take necessary sanctions against early offences					

2. Internet Security	**Extremely unimportant**				**Extremely important**
How concerned are you about	**1**	**2**	**3**	**4**	**5**
a) Security in relation to making purchases or banking over the Internet?					

b) Security features when choosing whether or not to do business with an Internet company?					
c) Security features when receiving emails from an unknown party?					

3. Purpose of Internet usage	**Email**	**Downloading**	**Search**	**Remote Server**
Primary access at Home				
Primary access in office				
Average access of all staff				

4. Backups / Access	**Regularly**	**Sometimes**	**Once a time**	**Never**
Perform Data Backups				
Read the Security procedures				
Verify the expiry/validity of contents				
Update the log / audit file				
Update personal password				
Auto update of all employees password				

5. Threats	**Virus**	**Hacker**	**Fraud**	**Othr(Spcfy)**
What is your worst known threat?				
Which one bothers you more?				
Against which one(s) is/are your system protected?				
Against which one do you feel more protection is required?				

6. No. of Threats hit your Org.	**>50**	**20-50**	**10-19**	**1-9**	**None**
How many of above happened last year?					
How many from virus only?					

7. Your opinion on most known offences	**1(L)**	**2**	**3**	**4**	**5(H)**
Manipulation or alteration of data / programs					
Theft or misappropriation of data / programs					
Alteration to data / programs					
Unauthorised copying of data / programs					
Computer forgery or counterfeiting					
Disgruntled employee					
Independent hacker of info broker					
Industrial espionage					
Ignorant user					
Hackers					
Cyberterrorism					
Cybervandalism					
Cyberstalking (Harassing)					

8. About the Computer Misuse & Cybercrime Act	**1(L)**	**2**	**3**	**4**	**5(H)**
How much aware are you about it?					
Does your organization have a copy of above?					
Are you aware that Unauthorized access to a computer is liable to 5 years imprisonment?					
Do you feel more secure with this act?					
Do you know how to report a cyber crime?					
Do you think that the necessary resources are available?					
Are there enough qualified lawyers?					
Is the threat coming from local cyber criminals?					
Is the threat coming from foreign cyber criminals?					

THANK YOU FOR YOUR TIME

III. Summary of Results

A. Demographics

1.Organizational Level	Reply Received
1. Chief Officer	10
2. Senior Executive	9
3. Executive	21
4. IT Manager	7
5. Network/Data administrator	13

2. Type of organization	
1. Manufacturing	2
2. Banking	9
3. Legal	2
4. Commercial	24
5. Government	21

3. Academic	
1. Post Grad Degree	22
2. Post Grad Diploma	6
3. Degree/Higher Diploma	18
4. Diploma	13
5. Certificate	9

4. Management Experience (in years)	
1. More than 15	15
2. 10-15	11
3. 5-9	10
4. 2-4	18
5. Less than 1	13

5. Gender	
1. Female	13
2. Male	54

6. Age	
1. 18-29	25
2. 30-40	23
3. > 40	19

7. Years experience as a computer user	
1. > 10	35
2. 6-10	16
3. 3-5	14
4. 1-2	3
5. <1	-

8. Internet usage – hours per week	
1. 0-1	6
2. 2-4	17
3. 5-6	6
4. 7-9	9
5. 10-20	16
6. 21-40	5
7. > 40	8

9. Basic Infrastructure Existence	DialUp	DSL	Lease-Line	Wireless	None
Company access to the Internet technology	26	26	19	2	1

B: General Environmental					
1. Overall Level Internet Security	1(L)	2	3	4	5(H)

a. What do you think of the overall level of internet security in your organisation?	9	11	21	11	14
b. What do you think about the overall level of security to cope with factors like culture, politics, infrastructure, bad climatic conditions, etc. that may affect your organisation?	6	19	21	11	9

2. Environment	**N/A**	**1(L)**	**2**	**3**	**4**	**5(H)**
a. Culture Existence of an organisational culture as an integrated team.	4	9	9	23	10	12
b. Authority Management Pro-activeness so that decisions are not delayed. (Awareness, prevention, etc).	-	6	9	23	13	17
c. Infrastructure Ability to cope with infrastructure problems (e.g. networks LAN, WIFI, training, communication etc).	2	9	13	17	10	15
d. Climate Ability to cope with delays due to natural calamities (like storms and thunder) which damage power and tel. lines.	2	11	12	21	10	11
e. Politics Ability to cope with politics which may influence the telecom regulations.	5	12	12	21	7	10
f. Legal Ability to cope with legal shortcomings (e.g. inadequate protection against software piracy, etc)	3	17	12	20	7	10
g. Economic Ability to cope with economic situation (e.g. A bad economic situation may discourage usage of proper security investments).	4	13	11	17	7	12

C: The Computer Misuse and Cybercrime Awareness					
1. Internal Risks	**Strongly disagree**				**Strongly agree**
	1	2	3	4	5

a) Internet services will be of benefit to me	1		9	18	40
b) I am conscious about the dangers of cyber crimes	6	2	11	16	33
c) Employees should sign compliance statements?	4	7	16	12	28
d) Continuous awareness of the ICT regulations?	-	7	11	16	34
e) Implement a disciplinary committee to take necessary sanctions against early offences	1	2	12	13	39
2. Internet Security	**Extremely unimportant**				**Extremely Important**
How concerned are you about	**1**	**2**	**3**	**4**	**5**
a) Security in relation to making purchases or banking over the Internet?	2	3	6	5	51
b) Security features when choosing whether or not to do business with an Internet company?	3	-	8	8	47
c) Security features when receiving emails from an unknown party?	1	3	7	10	46

3. Purpose of Internet usage	**Email**	**Downloading**	**Search**	**Remote Server**	
Primary access at Home	54	27	38	2	
Primary access in office	52	39	50	12	
Average access of all staff	42	18	34	9	

4. Backups/Access	**Regularly**	**Sometimes**	**Once a time**	**Never**	
Perform Data Backups	48	11	5	2	
Read the Security procedures	31	21	9	5	
Verify the expiry/validity of contents	29	23	11	3	
Update the log / audit file	25	23	7	10	
Update personal password	31	18	16	6	
Auto update of all employees password	16	15	13	21	

5. Threats	**Virus**	**Hacker**	**Fraud**	**Other(Specify)**
What is your worst known threat?	57	13	14	Spam & Spyware
Which one bothers you more?	45	17	16	Vulnerability

Against which one(s) is/are your system protected?	65	22	16	Physical Access	
Against which one do you feel more protection is required?	38	28	30	Spyware	
6. No. of Threats hit your Org.	**>50**	**20-50**	**10 to 19**	**1 to 9**	**None**
How many of above happened last year?	5	3	3	39	15
How many from virus only?	4	3	3	39	10

7. Your opinion on most known offences	**1(L)**	**2**	**3**	**4**	**5(H)**
Manipulation or alteration of data / programs	4	10	18	11	21
Theft or misappropriation of data / programs	9	5	18	14	17
Alteration to data / programs	6	8	18	15	17
Unauthorised copying of data / programs	5	1	23	13	22
Computer forgery or counterfeiting	8	8	18	11	18
Disgruntled employee	11	12	17	11	13
Independent hacker of info broker	12	10	19	10	11
Industrial espionage	14	17	12	8	13
Ignorant user	17	10	16	9	12
Hackers	11	8	17	9	19
Cyberterrorism	16	17	8	7	15
Cybervandalism	16	13	11	8	15
Cyberstalking (Harassing)	19	12	12	5	15

8. About the Computer Misuse & Cybercrime Act	**1(L)**	**2**	**3**	**4**	**5(H)**
How aware are you about it?	13	15	18	6	11
Does your organization have a copy of above?	28	4	10	6	12
Are you aware that Unauthorized access to a computer is liable to 5 years imprisonment?	24	13	9	3	5
Do you feel more secure with this act?	11	11	19	11	12
Do you know how to report a cyber crime?	36	9	7	6	4
Do you think that the necessary resources are available?	32	11	14	6	
Are there enough qualified lawyers?	32	17	7	2	2
Is the threat coming from local cyber criminals?	19	15	15	9	3
Is the threat coming from foreign cyber criminals?	9	5	11	16	20