AN ASSESSMENT OF INFORMATION SYSTEMS RISK MANAGEMENT PRACTICES: A CASE OF PRACTICAL ACTION (INTERNATIONAL)

By

Samuel G. Weru

A Management Research project submitted in partial fulfilment of the requirements for the award of Master of Business Administration (MBA) Degree

SCHOOL OF BUSINESS
UNIVERSITY OF NAIROBI

OCTOBER 2008

DECLARATION

This research project is my original work and has not been presented for a degree programme in any other university.

Signed______________________________**Date** ±/fl/O?

Weru, Samuel Githemo
D61/P/7158/03

This research project has been submitted for examination with our approval as university supervisors:

Signed: W^Ull^ Da.e:

J. K. Lelei
Lecturer
Department of Management Science
University of Nairobi

Signed. OjftZ^ **Date:**

O. Okwiri
Lecturer
Department of Management Science
University of Nairobi

DEDICATION

This research project is dedicated to my darling wife Grace Githemo and our two sons, Mark Weru and Stephen Wahome for being such an encouragement and joy; my mother Mrs. Felishina Wambui for being such a good mentor to me and making much sacrifice in laying a strong foundation for me which has stood the test of time.

ACKNOWLEDGEMENT

I am greatly indebted to the following that made this study a success:

The Almighty God for the strength and the courage that He gave me to undertake this study and for giving me a new lease of life to complete this report.

My supervisors: Mr Lelei and, Mr. Okwiri for their professional guidance and moral support during the entire study period.

Mr. Magutu, project moderator for all the useful insights to make my project a reality.

My wife Grace Githemo for the great support that she gave me during the study period and for all the support she offered to see this work come to this good end.

Our children Mark and Stephen for being so understanding even when I had to be away from home to undertake this study.

I am greatly indebted to Practical Action (International) for allowing me to carry out this study. The organisation offered much support and allowed me to study and work at the same time and contributed financially towards this study.

My colleagues in the International Information Technology Team (IIT Team) for being very supportive and responding to my request for information within a short time.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

CD	Compact Disks
CFO	Chief Financial Officer
COBIT	Control Objectives for Information Technology
DSS	Decision Support Systems
ESS	Executive Support Systems (s)
ICT	Information and Communication Technologies
IS	Information Systems
ISO	International Standards Organization
IPR	Intellectual Property Rights
IT	Information Technology
ITDG	Intermediate Technology Development Group
ITDG	Intermediate Technology Development Group
ITIL	Information Technology Infrastructure Library
ITRM	Information Technology Risk Management
LAN	Local Area Network
MIS	Management Information Systems
MIS	Management of Information Systems
NGO	Non-Governmental Organization
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
TPS	Transaction Processing Systems (s)
VPN	Virtual Private Network
WAN	Wide Area Network

ABSTRACT

This study focused on information systems risk management practices within Practical Action. The study assessed Practical Action's level of assurance in terms of information availability, security, optimal performance and compliance as related to guarantee of business continuity in view of vulnerability of information processing and flow channels. The study investigated risk awareness, the frequency of occurrence of human related risks and the general level of preparedness in mitigating human related risks, natural risks and environmental risks situations in the organisation. The purpose of the study was to establish the importance of information systems in regard to business continuity.

This was a descriptive case study that aimed at assessing information systems risk management practices in Practical Action. This study reviewed literature on general risk management and information systems risk management in order incorporate other views in the study. The research targeted seven (7) countries in four different continents of the world. The study population included all the 14 information technology staff in the seven countries. Data was collected by use of standard structured questionnaires which were emailed to the respondents and online communication from the respondents. The study achieved 68.5% response rate. The data was analysed quantitatively (means, frequencies and percentages) using SPSS and presented by use of frequency tables, histograms and pie charts.

The study findings revealed that Practical Action has averagely performed well in terms of risk management with an average of 54.5% showing success in key preparedness indicators and 45.5% showing lack of success in key preparedness indicators used in the study. The results also showed that 49% have no awareness at all which closely related to low level of preparedness. There is therefore a relationship between the awareness levels and the level of preparedness. The results also showed that IT risk management is on ad hoc basis. The senior management teams in each country has left the role of managing information systems risk to IT experts instead of integrating it within the general organisational risk management.

There is great need for organisations to develop a comprehensive and all inclusive policy on the use of information systems to reduce the risks arising from insiders (employees). There is generally low awareness among staff on information systems risks that could arise from natural, environmental and human related risk causes. For effective information systems risk management, the senior management have to deal with the issues of information systems risks in an integrated manner and not consider other risks and leave out what has turned out to be the backbone of the organisation - information systems. The low levels of preparedness in case of a disaster is a clear indication that the management has not embraced information systems risk as part of the overall organisational risk management.

CHAPTER ONE: INTRODUCTION

1.1. Background

Information systems are key to the success of every organization because they aid in: more systematic use of the available data at the right time in the business process; more systematic information storage and data reuse; information integration and; organizational knowledge management and institutionalizing of organizational memory. An information system has been defined by O'Brien (2000) as an organized combination of people, hardware, software, communication networks, and data resources that collect, transform, and distribute information throughout the organization. Thus, information systems should produce useful information for organizations. Ritchie (1998) identify the five most important functions of information as: reduction of uncertainty in decision making; control over operational performance through defect signaling; communication of plans, expectations for the future, and procedures; historical data about transactions, performance levels and effects of decisions and; reduction of complexity through upgrading the knowledge of the user.

According to O'Brien (2000) information systems can be categorized in terms the level of application in the organization. O'Brien identifies these categories as operational level information systems, tactical level information systems, and strategic level information systems. Information systems therefore play a key role in ensuring business continuity and also are a major tool for competitive advantage. The use of information systems in all levels of operations has come with a number of risks which organizations must be aware of and develop a plan of how to mitigate them. There is need to manage risks that could arise at each of these levels to guarantee business continuity.

1.1.1. Risks relating to information systems and ICTs

Risk has been defined as a condition in which there is a possibility of an adverse deviation from the desired outcome that is expected or hoped for (Emmett, 1995). In business terms, risk can be looked at as the potential that a given threat will exploit vulnerabilities of an asset or a group of assets to cause loss and/or damage to the assets. Risk can be quantified in terms of the combination of impact and probability of occurrence (The IT Governance Institute (www.itgi.org), accessed in April 2008).

Each organization has a unique information systems risk profile. Every organization tries to respond to global changes in information systems in order to remain competitive and ensure business continuity. Some of the effects of these information systems risks have had great impact on companies making them incur massive losses or have affected business continuity in tremendous ways. This is made worse by professionalization and commercialization of malicious activities, along with more intense attacks and more frequent outages. This has brought into focus the need to look at the entire spectrum of information systems risk (Hughes, 2008).

Stoneburner (2002) has categorised risks to information systems into three: natural risks which arise from the threats of floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, frost and other such events; human related risks, which relate to events that are either enabled by or caused by human actions, such as unintentional acts (inadvertent data entry/deletion) or deliberate actions (network based attacks, malicious software upload, and unauthorized access to confidential information) and; environmental risks, which includes such threats as long-term power failure, pollution, chemicals and liquid leakage.

1.1.2. Integrated information systems risk management

Information Systems (IS) risks are a threat to data integrity, productivity and business operations. Thus factors of security, availability, performance and compliance are fundamental to successful overall organisational risk management. Treating information systems risk management process as primarily a technical function to be carried out by the IT experts who operate and manage the IT system, fails to recognize the reality that the threat is an essential management issue (Stoneburner, 2002).

As corporations and in general world economies become increasingly dependent on the Internet and IT systems, the consequences of breaches or failures of information systems are far reaching. The consequences include reputation damage and business losses if not survival of the organisation itself. This therefore implies that managing of information systems related risks becomes central in ensuring business continuity. This is no longer purely an information technology issue but a management as a whole.

A model developed by Symantec (2007), considers information systems risk management in terms of a spectrum. On one side of the spectrum we, have IT services where risk management involves: detections and prevention of threats/issues; fixing vulnerabilities/weaknesses and; handling of response and recovery from threats/risks. On the other side of the spectrum we have business organisation where risk management involves: general risk analysis; handling of management programmes and; giving strategic directions.

Figure 1.1: An integrated IT risk management model (Symantec 2007)

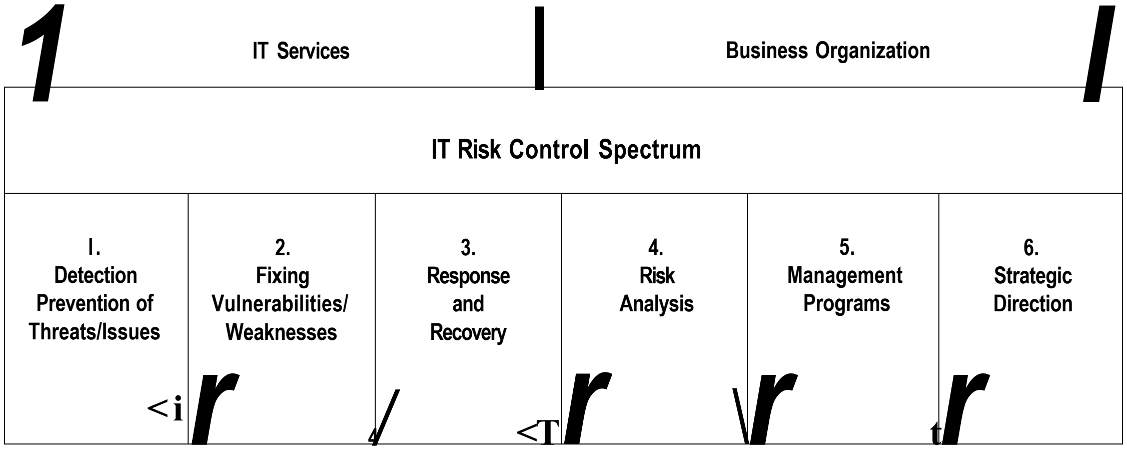


Figure 1

Information systems risks need to be identified, measured and managed as part of a singular attention of all risks in the corporation, with oversight by senior management to understand and guide the appropriate risk/reward tradeoffs to achieve the overall objective of any organization (Hughes, 2007). Information risk management involves managing and balancing information risks and rewards.

There is need for business leaders to: develop an awareness of the nature of the different IT risks to the business; assess and quantify the potential impact to their business resulting from the loss of information or access to applications; understand the range of tools available to manage IT risks; align the costs of IS risk management to the business value and; build a systematic, corporate capability to manage (Hughes, 2006).

These are critical issues and their effects become apparent when considered in the context in which an information systems infrastructure forms a critical platform for control and decision making. The issues were investigated in the context of Practical Action, an organisation whose operations span four continents.

1.1.3. Practical Action

Practical Action was founded in 1966, as Intermediate Technology Development Group (ITDG), by the economist Dr. EF Schumacher to prove that his philosophy of 'Small is Beautiful' could bring real and sustainable improvements to people's lives. Its vision is a "sustainable world free of poverty and justice in which technology is used for the benefit of all". It is registered in the United Kingdom as a charity and operates directly in four regions of the developing world - Latin America, East Africa, Southern Africa and South Asia, with particular concentration on Peru, Kenya, Sudan, Zimbabwe, Sri Lanka, Bangladesh and Nepal. Its operations also spill to other neighbouring countries of each of the regional offices. These include Sudan, Tanzania Somalia, and Mozambique among others (Practical Action Annual Report, 2007).

In the countries in which Practical Action operates directly, it works with poor communities to develop appropriate technologies in food production, agro-processing, energy, transport, water and sanitation, shelter and disaster mitigation. Currently Practical Action is implementing over 100 projects worldwide. In addition to this, consultancy and educational work extends its reach of practical approach to tackling poverty. In the 2006/2007 operating year, the organization reached 664,000 people. The organization's annual budget for the year 2007 is Kshs. 3375 million, equivalent to 25 million UK pounds (Practical Action Annual Report, 2007).

The organisation is controlled by a Board of Trustees who oversees the global management of all its affiliate regions. Each region is headed by the regional director who exercises full autonomy of operation in all matters of the projects and management and is answerable to the Chief Executive officer (CEO) through the International Director.

For effective management of the global network. Practical Action has invested a significant portion of its resources in information systems. A Wide Area Network (WAN), with Virtual Private Network (VPN) connection to each office has been implemented. Each office has high speed Internet capacity (bandwidth) and information systems staffs that manage smooth operations of organisations systems on a 24 hour basis. This implies that information systems are key to delivery of all the global projects that the organisation is involved in (IT strategy 2007-2012). Practical Action reliance on information systems implies that failure to manage and prepare to handle risks arising from use of information systems poses a great risk to the survival of the organisation. There is therefore the need to be aware of the risks involved and be prepared to mitigate these risks if they happen to occur in order to ensure business continuity.

The issues involved in the organisations dependence on the information systems and their related technologies are the managerial activities focused at the potential adverse consequences of occurrence of natural risks, human related risks and the environmental risks.

1.2. Statement of the problem

Balancing consolidation of the efforts of each country by Practical Action and summing it up in a group report to donors and trustees on how funds have been spent, relies heavily on reliability, integrity, availability and security of its information systems. Integration of financial systems in all the countries, use of single messaging systems, file sharing systems and donor reporting systems implies that information systems are critical to the realisation of the organisation's vision and mission. Failure of information systems amounts to failure of the organisation as a whole in delivering of projects to the poor communities. Practical Action therefore need to analyse IS risks and be prepared to respond to the risks that relate to information systems and can lead to loss of business continuity that is paramount to Practical Action. There is need to be aware of all the risks that are likely to affect an organisation, the frequency of occurrence and establish the level of preparedness in the event that these risks happen to occur.

A risk to information remains a risk to an organisation (Stonebumer, 2002). Diversity in terms of skills in each country, different time zones, different regulations and law governing information systems and management, digital divide between the rich and the poor countries, poor infrastructure especially in Africa, different regional/country strategic plans and priority areas, management perception of the role of IS, and the overall integration of systems that the organisation heavily relies upon for operation are some of the few challenges that Practical Action has to address to be assured of information systems availability and business continuity.

The already installed systems have added much value in terms of efficiency. IT has also enabled collaboration among country offices. This has come however with high potential risks with a possibility that impacts from the risks may seriously affect business continuity and erode the confidence of donors and communities served by the organisation. This is in addition to other stakeholders and employees. This therefore raises a number of questions: Is Practical Action aware of information systems risks?; Is the organisation aware of the types of risks that have the potential of affecting business continuity? and; Is the organisation prepared to mitigate information systems risks if they happen to occur in any of the country offices?

A lot of research has focused on the efficiency of information systems as such (O'Brien, 2000; Ritchie, 1998; Laudon and Laudon, 2002), while the improvement of organizational efficiency by means of information systems has received far less research attention. None of the cited studies has specifically tried to establish an organizations awareness and preparedness and to establish methods of establishing an organizations risk profile. This study therefore sought to establish Practical Action risk awareness, types of information systems risks that can affect business continuity and organisations preparedness in handling these risks if they happen to occur.

Likewise in Kenya, although a number of studies have been done in relation to information systems management (Nzuki, 2006; Muriuki, 2006; Anyanje, 2005; Ngemu, 2005), none has been done in an organisation within an international context integrating the diversities in regards to information systems risks. The study therefore sought to establish Practical Action's level of information systems risk awareness, frequency of risk occurrence and the level of preparedness in mitigating such risks.

1.3. Objective of the study

The main objective of the study was to assess information systems risks and risk management practices within Practical Action. The results would establish the level of assurance in terms of information availability, security, optimal performance and compliance as related to business continuity in view of vulnerability of information processing and flow channels.

1.4. Specific research objectives

(a) To determine Practical Action's awareness of information systems risks

(b) To determine the frequency of occurrence of the human related risks in Practical Action.

(c) To determine the level of preparedness in mitigating human related risks, natural risks and environmental risks situations in Practical Action.

1.5. Importance of the study

The findings of this study will be of great interest to the top management of Practical Action and other **NGOs** with global operations. The results will be useful to the top management of similar organisation in making important decisions regarding information systems, staff training needs, developing strategic plans which will factor in the element of information systems risks as part of organisation**'s** operational risk planning among others.

The findings will be of importance to academics and researchers. The findings may form a basis on which other studies could be done in order to develop an information systems risk model that could guide organisations irrespective of the nature of business. Academic institutions also will find this useful in developing the new discipline of information systems risk management as a branch of operational risk management.

The research findings will also be useful in government institutions in establishing risk management programmes for their interconnected solutions that offer services to the citizens. The findings will also be useful to consultants in developing risk management profiles of their clients.

CHAPTER TWO: LITERATURE REVIEW

2.1. Introduction

Risk is a condition in which there is a possibility of an adverse deviation from a desired outcome that is expected or hoped for (Emmett, 1995). The existence of risk is a source of discomfort to most people and the uncertainty accompanying it causes anxiety and worry. Since risk is distasteful and unpleasant, people's rational nature leads them to attempt to do something about it. Basically people deal with risk in five ways. They avoid, retain, transfer, share or reduce it (Emmett, 1995). Risk in business, is the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss and/or damage to the assets; usually measured by a combination of impact and probability of occurrence (IT Governance Institute, 2007).

There is a large body of research on information systems management; however, little attention has been given to the risks arising from the use of information systems. An extensive analysis of the IS risk management literature reveals an area rich in terms of approaches (case studies, surveys) and theoretical foundations (structural contingency theory, prospect theory (Ropponen, 1999). Other studies relating to information systems risks have been conducted and their impact on the business continuity (Hughes, 2008; Steve, 2006; IT Governance Institute, 2007; Benaroch, 2006; Swanson, 2002, Stonebumer, 2002). A lot of research has been done in the past and most of them are dealing with security issues only and not considering the issues of availability, performance and compliance issues (Nzuki, 2006; Muriuki, 2006; Anyanje, 2005; Ngemu, 2005).

The World economic Forum provides a sense of scale. They rank a breakdown of critical information infrastructure among the most likely core global risks, with 10 to 20 percent likelihood over the next 10 years and potential worldwide impact of $250 billion. Sustained investment in information systems—almost $1.2 trillion or 29 percent of 2006 private-sector capital investment in the U.S. alone—is an indication of growing exposure to information systems risk (World Economic Forum-Global Risks, 2007).

2.2. Information systems and ICTs

Automated information systems are vital elements in any business process and are therefore critical that they are able to operate effectively without excessive interruption (Swanson, 2002). Every organization therefore requires a coordinated strategy involving plans, procedures, and technical measures that enable recovery of IT systems operations, should a risk happen to exploit any vulnerability in information systems. This assures business continuity (Swanson, 2002).

According to O'Brien (2000) information systems can be categorized in terms the level of application in the organization. O'Brien identifies these categories as operational level information systems, tactical level information systems, and strategic level information systems. In the following subsections information systems at each of these levels will be described.

Transaction Processing Systems (TPSs) are found at the operational level. These are systems that record elementary activities and transactions of the organization. Examples of these systems are pay-administration, stock control, production and sales information and other context related deployments. These TPSs are data oriented and focus on data relating to process activities in the organization. They provide the necessary means for monitoring the status of internal processes and relations with the external environment. These systems help in enforcing policies and procedures of the organizations as they empower operational employees to make the right decisions. They provide a means to avoid inadvertent mistakes and reduce or eliminate need for rework. The outputs of these systems provide input to the tactical and strategic level information systems (O'Brien, 2000).

Management Information Systems (MISs) for repetitive and routine decisions and Decision Support Systems (DSSs) for unstructured and ad hoc decisions are found at the tactical level. At this level the most important question is: How is the organization performing? Therefore, support is needed by means of systems for monitoring, controlling and decision making (O'Brien, 2000).

At the strategic level, management is focusing on strategic issues and long term trends and signals. The systems used are categorized as Executive Support Systems (ESSs). These are flexible systems and are used for non-routine issues and problems in which information from various sources (both internal and external) is needed with human inputs that include assumptions, and personal insight of the manager (O'Brien, 2000).

2.3. Information systems risk categories

Swanson (2002) points out that information systems are vulnerable to a variety of disruptions, ranging from mild to severe arising from a variety of sources such as natural disasters to terrorists actions. While much vulnerability may be minimized or eliminated through technical, management, or operational solutions as part of the organization's risk management effort, it is virtually impossible to completely eliminate all risks. In many cases, critical resources may reside outside the organization's control (such as electric power or telecommunications), and the organization may be unable to ensure their availability. Thus effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. Swanson (2002) categorised sources of risks are categorised into natural (hurricane, tornado, flood, and fire); human (operator error, sabotage, implant of malicious code, and terrorist attacks); and environmental (equipment failure, software error, telecommunications network outage, and electric power failure).

Human related risks fall in various categories depending on their source and the motivation behind them. Hackers or crackers are more interested in challenging others, raising their ego, and rebellion. They normally hack into other systems where they are not authorised to access to achieve their ambitions. Computer criminals are motivated to gain illegal information disclosure, monetary gain, unauthorised data alteration and destruction of information. Their actions include fraudulent acts like impersonation and interception, information bribery, spoofing and systems intrusion (Stoneburner, 2002)

A major risk in the world today is terrorism. Terrorists' main intentions are revenge for some alleged wrong and blackmail. Their actions include bombing, information warfare, systems attack such as denial of service attacks, system penetration and tampering. The 1998 bomb attack in Nairobi affected many institutions, destroying their information systems and data. While some may have recovered others could be still affected by the loss to date. Kikambala attack in 2002 is one other example whose effects are probably still being felt today (Kyama, 2006).

Industrial espionage is another threat used by companies, as organisations try to gain competitive advantage by obtaining access to critical and confidential information from their competitors. Their actions include reverse from product obtained through unauthorised systems access, systems penetration and information theft. The highest human related risk to an organisation and which is hardest to deal with are those that concern insiders. These are the people working for an organisation but for one reason or the other disgruntled are malicious, negligent, and dishonest. Other source of this category of this risk can be terminated employees whose exit process has not been effected well. Effects can be systems access on termination, as a form of revenge or sabotage or some other destructive action (Kapuria, 2007).

2.4. Management of information systems risks

Hughes (2008) findings suggests that there can be four types of risks arising from these risk sources as identified by Swanson (2002) The three sources of risks have translated into four types of risks in terms of information systems. These are security, availability, performance and compliance. According to Hughes, (2008) risk is potential damage to an organization's value, often from inadequate management of processes and events.

IT risk is emerging as a significant component of total business risk as information systems assumes a more prominent role in organizations, and can account for more than 50% of total capital expenditure in some companies (Kapuria, 2007). Kapuria (2007) points out that information systems risks may be therefore classified as:

(a) Security—resulting in the use or alteration of information by unauthorized people such as computer crime, internal security breaches or cyber terrorism;

(b) Availability—resulting in information being inaccessible. For example from poorly managed configuration changes, human errors or disasters that cause system failure, slowdown or incidents from which recovery is slow or incomplete;

(c) Performance—resulting in failure to meet information demand in a cost-effective manner such as poor system architecture or poor demand management;

(d) Compliance—resulting in not meeting legal, regulatory or industry-driven requirements. These include inadequate technology/process, from human error or malfeasance.

2.4.1. Security risks

Research by International Standard Organisation (2007) defines information security as the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. This is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes (ISO/IEC 17799:2005, 2007).

Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image. Organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage such as malicious code, computer hacking and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

Information security is important to both public and private sector businesses. In both sectors, information security will function as an enabler such as helping to achieve e-govemment or e-business, and to avoid or reduce relevant risks. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has also weakened the effectiveness of central, specialist control (Hughes, 2006).

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures (Kapuria, 2006).

A survey carried out by Symantec (2007) in effort to understand how organisations were managing security issues drew a number of conclusions from a sample of three hundred and ten

IT professionals. "Authentication, Authorization and Access" was rated highest for effectiveness, with 68% of respondents rating their organizations more than 75% effective. "Asset Inventory Classification and Management" was lowest, with only 38% rating their organizations more than 75% effective. The findings show that most IT professionals feel their organizations are most effective deploying tactical controls for which they are accountable: organizational structure, and authentication, authorization, and access. They rated themselves moderately effective at policy-setting and compliance, assessment and audit, and incident response. A few felt they performed effectively in employee and IT staff training and awareness, operational design, or asset management.

The data showed that the path from basic performance to best practice requires moving IT risk management programs away from a reactive posture, designed for protection against malicious external threats. Instead, programs should raise IT risk awareness and spread avoidance and mitigation efforts throughout their organizations.

Symantec (2007) survey also rated "Asset Inventory Classification and Management" least effective of all their deployments. This discipline is fundamental to build an IT risk management program that reflects the organization's priorities. Without careful risk assessment, all assets are likely to be treated equally, so that some will be overprotected and others under protected. "Network Protocol and Host Security" and "Physical Security" were the top-rated technology control deployments, with 80% and 77% of respondents, respectively, rating their organizations more than 75% effective. These are the strongest ratings of all controls, process or technology. "Configuration and Change Management" received such ratings from only 55% of respondents, and "Performance Management" from just 52%. "Secure Application Development" was least-frequently rated effective, with only 43% rating their deployments 75% effective or higher.

The low ratings of configuration and change and performance management deployments are significant. Organizations use these technologies to understand the configurations and performance levels of IT assets so they can minimize service disruptions and increase throughput (www. Symantec.com, Accessed in June 2008).

Sterling (2006) argues that poor configuration and change management also constrains efforts to adapt and modernize systems for new opportunities or threats. Although the survey identifies change management as a problem area, there are recent signs of improvement. ITIL "Change Management Maturity Benchmark Study" concluded that IT executives are increasingly integrating and internalizing change management procedures, processes and tools as core components of the organization (Sterling, 2006).

2.4.2. Availability risks

Availability risks arise from failure or delay in delivering information systems processes or information needed for business transactions or operations. This may be as a result of hardware failures, power outages, poor change management processes, and data centre failures among others (Stoneburner, 2002). These risks have great impact to business continuity as may cause reduced customer, partner or employee confidence; interruption or delay in business-critical processes; reduced information systems staff productivity and even abandoned transactions and loss of sales (Hughes, 2007). The main objective is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

A business continuity management process should be implemented to minimize the impact on the organization and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities. The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the organization (ISO/IEC 17799:2005, 2007).

Business continuity management should include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available. Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences. Information security aspects of business continuity should be based on identifying events (or sequence of events) that can cause interruptions to the organizations business processes, such as equipment failure, human errors, theft, fire, natural disasters and acts of terrorism. This should be followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period (ISO/IEC 17799:2005,2007).

Depending on the results of the risk assessment, a business continuity strategy should be developed to determine the overall approach to business continuity. Once this strategy has been created, endorsement should be provided by management, and a plan created and endorsed to implement this strategy. Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes (The IT Governance Institute (www.itgi.org), accessed in April 2008).

When business processes depend—sometimes completely—on IT systems and processes, IT failures cause business failures. Researchers at Dartmouth and the University of Virginia investigated one example: hypothetical failure of the Supervisory Control and Data Acquisition (SCADA) network at an oil refinery. SCADA failure would immediately shut down production because of safety concerns. The researchers estimated economic impact of $405 million from a hypothetical ten-day outage at a supplier that contributed 10 percent of the U.S. gasoline supply. The affected supplier would bear only $255 million of the impact; others in the supply chain would assume the remaining $180 million loss. The example highlights two important facts: First, IT system availability is often equivalent to business availability. Second, in a connected world of global supply chains and collaboration networks, availability failures in one business cascade directly into others (Dynes et al., 2007).

2.4.3. Performance risks

Systems availability must also meet performance benchmarks in order to assure business continuity. Hughes argues that underperforming systems, applications, staff, or organizations will diminish business productivity or value. Performance risk concerns reduce business productivity or value when teams, systems or applications under perform. These arise from poor system architectures, network congestion, inefficient code, inadequate capacity, poor integration and inadequate process designs (Hughes, 2007).

Performance risk concerns reduce business productivity or value when teams, systems or applications underperform. Often overshadowed by security and compliance concerns—and sometimes unrecognized outside IT— these risks differ in several important ways. These are: frequency and impact and; transfer of harm.

First, security and compliance risks attract attention because of their high visibility and impact: virus outbreaks, data loss, or lawsuits may require disclosure, are a staple of the business press, and are devastating to the individuals and companies involved. In contrast, common availability and performance events tend to be incremental, and may escape notice—a few seconds' delay in serving a web site, a few percentage points lower transaction capacity, a near-miss in meeting recovery-time or recovery-point objectives. Yet the cumulative burden of IT underperformance weakens any organization, and a single breakout event may be enough to bring it down (Hughes, 2007).

A second difference is that while security and compliance risks involve transfer of harm—from thief to victim or government to organization—availability and performance risks often play out inside the walls, as reduced revenue, added expense, or lost profit. Stakeholders can, should, and do complain, but incremental availability and performance shortfalls rarely attract outside attention, nor are the affected organizations likely to seek it (Kapuria, 2007).

Just like availability disasters, performance disasters can be nightmare scenarios: transaction processing at a crawl on the busiest shopping day of the year or during a market crash, failures cascading through backup systems during a site or regional disaster, or essential services missing when they're needed most. Worse, availability and performance disasters are often irrecoverable over the short term (Hughes, 2007).

2.4.4. Compliance risks

Compliance risk stems from failure to meet regulatory or business requirements for information handling or processing. In highly regulated industries, compliance failure may compromise the organization's reputation, profitability, or even existence. Since many regulations govern privacy and information security, compliance is sometimes seen as derivative of security. Compliance risk is more than security risk formalized by law (Hughes, 2006).

The main objective is to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow). All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization (UK data Protection Act, 1998, Accessed on Sept, 2007).

In relation to compliance companies must also be cautious about Intellectual Property Rights (IPR). IPR include software or document copyright, design rights, trademarks, patents, and source code licenses. Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. Some records may need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organization operates within statutory or regulatory rules, to ensure adequate defence against potential civil or criminal action, or to confirm the financial status of an organization with respect to shareholders, external parties, and auditors. The time period and data content for information retention may be set by national law or regulation (ISO/IEC 17799:2005,2007).

Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. An organizational data protection and privacy policy should be developed and implemented. This policy should be communicated to all persons involved in the processing of personal information. Compliance with this policy and all relevant data protection legislation and regulations requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a data protection officer, who should provide guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personal information and ensuring awareness of the data protection principles should be dealt with in accordance with relevant legislation and regulations (UK data Protection Act, 1998, Accessed on Sept, 2007).

A number of countries have introduced legislation placing controls on the collection, processing, and transmission of personal data (generally information on living individuals who can be identified from that information). Depending on the respective national legislation, such controls may impose duties on those collecting, processing, and disseminating personal information, and may restrict the ability to transfer that data to other countries. Intrusion detection, content inspection, and other monitoring tools may help prevent and detect misuse of information processing facilities. The legality of monitoring the usage varies from country to country and may require management to advise all users of such monitoring and/or to obtain their agreement. Where the system being entered is used for public access such as a public web server and is subject to security monitoring, a message should be displayed saying so (The IT Governance Institute (www.itgi.org), accessed in April 2008).

Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance checking requires specialist technical expertise. Compliance checking also covers, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for checking how effective the controls are in preventing unauthorized access due to these vulnerabilities (http://www.cio.com).

Penetration testing and vulnerability assessments provide a snapshot of a system in a specific state at a specific time. The snapshot is limited to those portions of the system actually tested during the penetration attempt(s). Penetration testing and vulnerability assessments are not a substitute for risk assessment. This is to help in maximizing the effectiveness of and to minimize interference to/from the information systems audit process. There should be controls to safeguard operational systems and audit tools during information systems audits. Protection is also required to safeguard the integrity and prevent misuse of audit tools (ISO/IEC 17799:2005, 2007).

Access to information systems audit tools should be protected to prevent any possible misuse or compromise. Information systems audit tools such as software or data files should be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection. If third parties are involved in an audit, there might be a risk of misuse of audit tools by these third parties, and information being accessed by this third party organization. Controls can be considered to address this risk, and any consequences, such as immediately changing passwords disclosed to the auditors, should be taken (ISO/IEC 17799:2005,2007).

2.5. General risk management

Risk management is a structured approach to managing uncertainty related to a threat, a sequence of human activities including: risk assessment, strategies development to manage it, and mitigation of risk using managerial resources. The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk (Alberts, 2008).

2.5.1. Assessment and treatment

Once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated guesses possible in order to properly prioritize the implementation of the risk management plan (Alexander, 2005).

The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for immaterial assets like information or data. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for the management of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized (Emmett, 1995).

According to Dorfman (2007), once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories avoidance (eliminate); reduction (mitigate); transference (outsource or insure) and; retention (accept and budget).

2.6. Risk management and business continuity

Risk management is simply a practice of systematically selecting cost effective approaches for minimizing the effect of threat realization to the (organization. All risks can never be fully avoided or mitigated simply because of financial and practical limitations. Therefore all organizations have to accept some level of residual risks (Emmett, 1995).

Whereas risk management tends to be preemptive, business continuity planning (BCP) was invented to deal with the consequences of realized residual risks. The necessity to have BCP in place arises because even very unlikely events will occur if given enough time. Risk management and BCP are often mistakenly seen as rivals or overlapping practices. These processes are so tightly tied together that such separation seems artificial. For example, the risk management process creates important inputs for the BCP (assets, impact assessments, cost estimates etc). Risk management also proposes applicable controls for the observed risks. Therefore, risk management covers several areas that are vital for the BCP process. However, the BCP process goes beyond risk management's preemptive approach and moves on from the assumption that the disaster will realize at some point (Alberts, 2008).

2.7. Summary and conclusion

In conclusion, information systems risk management is a new field and is still emerging, and not all organizations are yet organized to deal with this kind of risk in an integrated fashion. Nor do all companies face the same levels of IT risk or share similar risk profiles. The ease for change, however, is compelling: organizations are experiencing rising incident rates across the areas of security, availability, performance, and compliance, with significant impact to revenue, reputation, productivity, and cost. According to the Computer Security Institute and the FBI, per-incident costs of unauthorized access to information averaged over $85,000 in 2006 (Gordon, 2006), and system downtime costs reached tens of thousands of dollars per hour. It doesn't take long for incidents of this scale to create significant drag on an organization.

The main question therefore remains: How can organizations advance from good IT risk management practice to great? For organizations trying to manage IT risks effectively, the challenge includes understanding their portfolio of information systems risks, quantifying and prioritizing them against the organization's risk profile, and developing an effective program of remediation activities (Hughes, 2007).

CHAPTER THREE: RESEARCH METHODOLOGY

3.1. Research design

This was a descriptive case study that concerned Practical Action (International) information systems risks. This design was appropriate as the researcher aimed to have an in-depth analysis of IT risks management in a single organisation without assessing any causal effect relationship.

3.2. Study population

The information required for this research could only be received from employees of Practical Action. The researcher was in a position to obtain information easily. The study population included all IT staff within Practical Action as shown Table 3.1. The questionnaire was sent to all the IT staff in the seven countries of operation.

Table 3.1: Study population

Country	No. of IT staff
United Kingdom	3
Sri Lanka	2
Peru	1
Nepal	2
Bangladesh	2
Sudan	1
Zimbabwe	2
Kenya	2
TOTAL	**14**

3.3. Data collection tool

A standard structured questionnaire was emailed to respondents. Questionnaires were found to be appropriate due to the wide geographical area that was covered and hence was the most cost effective. Since questionnaires were also standard and structured, reliability was maintained. Low response rate which is inherent in questionnaire was minimised since the researcher also used online facilities within the organisation to clarify and request for questionnaires back.

The questionnaire is divided into 4 sections: Section 1 dealt with human related risks and the frequency at which they have occurred over the last one year; Section 2 concerned the awareness levels of naturally occurring risks; Section 3 dealt with effect of environmental risks to information systems; Section 4 dealt with the level of preparedness while Section 5 sought to get the general view of the respondents in regard to information systems risk management.

3.4. Data collection process

Questionnaires were emailed to the respondents since all the offices are interconnected. This saved time and costs. The researcher was also available to clarify any information online in order to ensure validity of the data collected. The respondents emailed back the filled up questionnaires to the researcher.

Authority to conduct the research was obtained from the International Director. Informed consent was also obtained from individual respondents. Confidentiality was maintained as names were not required in the questionnaire.

3.5. Data analysis

The raw data was cleaned by checking the incomplete or wrongly answered questionnaire to ensure that only the required and correct data was analyzed. Where clarification was required, the researcher used online facilities. Descriptive statistics was used to summarize the data in order to give meaning to the information and for easy interpretation. Data was presented in tables, pie charts, histograms and bar graphs. In all the questionnaire sections, mean and frequency distribution and percentages were used to analyse data in respect to human, natural and environmental risks.

CHAPTER FOUR: RESEARCH FINDINGS

4.1. Introduction

This chapter reports on the research findings. The objectives were to determine Practical Action's awareness of information systems risks, frequency of occurrence of these risks and the organisations level of preparedness in mitigating these risks. A total of 11 IT staff out of 16 responded giving a response rate of 68.75%.

Table 4.1 Total respondents

Country	No. of IT staff	No. that responded	%
United Kingdom	3	3	100.00
Sri Lanka	2	1	50.00
Peru	1	1	100.00
Nepal	2	0	**0.00**
Bangladesh	2	1	50.00
Sudan	1	1	100.00
Zimbabwe	2	2	100.00
Kenya	3	2	66.67
TOTAL	**16**	**11**	**68.75**

4.2. Human related risks

Human related risks are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions such as network based attacks, malicious software upload, unauthorized access to confidential information among others. The study focused on risks related to hackers, computer criminals, terrorists, industrial espionage and insiders or the employees within Practical Action. The results of the analysis are as shown in Table 4.2.

As shown in Table 4.2, 63.6% of the IT staff have not dealt with hackers and crackers while 36.4% have had at least once in the last one year. Over the last one year, 54.5% of the staff have dealt with computer criminals at least once. The data also shows that 9.1% have dealt with computer criminals more that 5 times in one year.

Table 4.2 Human related risks

		Nil	Once	2 - 5 times	>5 times	Total
Hacker	Frequency	7	4	0	0	11
	Percent	63.6	36.4	0	0	100
Computer Criminal	Frequency	4	6	0	1	11
	Percent	36.4	54.5	0	9.1	100
Terrorist	Frequency	6	5	0	0	11
	Percent	54.5	45.5	0	0	100
Industrial Espionage	Frequency	3	5	3	0	11
	Percent	27.3	45.5	27.3	0	100
Insiders	Frequency	0	0	3	8	11
	Percent	0	0	27.3	72.7	100

This shows that this is a risk that Practical Action need to be prepared to deal with due to the integrated nature of information systems within Practical Action. The results also show that 36.4% have not had an incidence of computer criminals over the last one year.

The risk of terrorists is not as high compared to other human related risks. Table 4.2 shows that 54.5% have not had such an incidence over the last one year and 45.5% had it only once. The results showed that 45.5% of the respondents indicated that they have had to deal with issues related to industrial espionage at least once and 27.3% indicated that they have dealt with this risk two to five times within one year.

The data indicates that the greatest human related risk to information systems is the insiders (employees).The data shows that 72.7% of the IT staff have dealt with this type of risk for more than 5 times in one year. One unique observation was that all the respondents have had to deal with issues related to insiders with 27.3% having had to deal with this between 2 to 5 times in one year.

From the analysis, most of the respondents indicted that their greatest fear of all the human related information systems risks are insiders (employees).

4.3. Natural risks

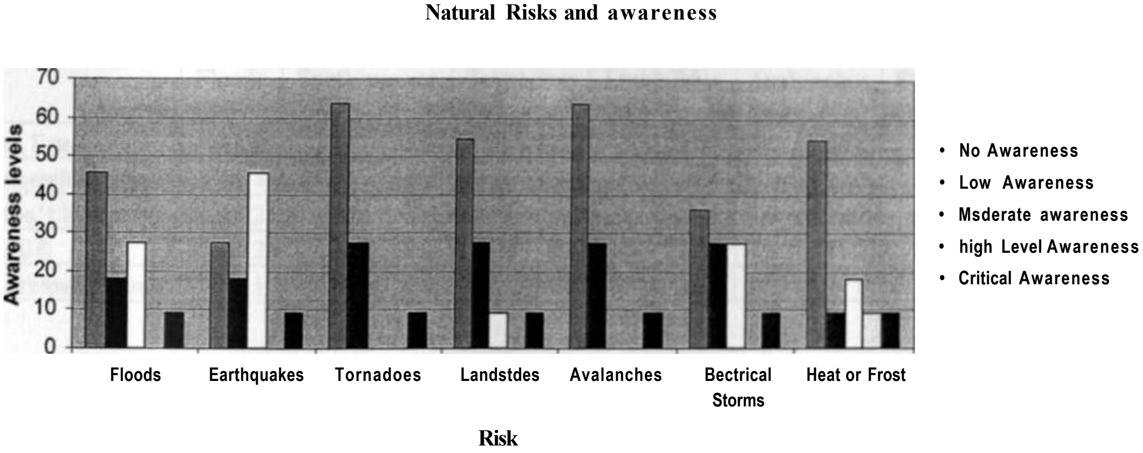
These are risks that are acts of nature and are beyond man's capacity to prevent. However, organizations can only plan and be prepared to mitigate their effects. The natural risks identified appeared to be perceived differently in each of the countries where Practical Action operates. The low level of awareness indicates that no measures have been put in place to deal with these risks. The highest level of awareness was in regard to earthquakes. The data shows that 45.5% are moderately prepared and are aware of the risk that could result from earthquakes.

In summary, Table 4.3 shows a mean of 49.3% indicating that they are not aware of how to handle naturally occurring risks. This is alarming since that can occur any time and cannot be predicted. This implies almost half of the respondents are not prepared to deal with such eventualities in case they happen to occur.

Table 4.3 Natural risks

	'Ö © o u. -T S? ^	Earthquakes (%)	Tornadoes (%)	Landslides (%)	Avalanches (%)	Electrical Storms (%))	Heat or Frost (%)	z s t
No Awareness	45.5	27.3	63.6	54.5	63.6	36.4	54.5	49.3
Low Awareness	18.2	18.2	27.3	27.3	27.3	27.3	9.1	22.1
Moderate awareness	27.3	45.5	0	9.1	0	27.3	18.2	18.2
High Level Awareness	0	0	0	0	0	0	9.1	1.3
Critical Awareness	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1

Figure 4.1: Natural Risks and awareness



Of the risks that are naturally occurring, 18.2% shows that should floods, earthquakes and tornadoes occur in their country office, there are no measures put in place to ensure that the office operates smoothly. They are not guaranteed to be back to operation even one week after the incident.

A high number indicated that the offices are not sure of how they are likely to handle information systems operations should any event occur in their country office. Their response indicated that they are not fully prepared to handle such naturally occurring risks (36.4% floods, 45.5% earthquakes, 36.4% tornadoes, 27.3% for landslides and avalanches.

The results also shows that as far as electrical storms are concerned, 45.5% are not prepared to deal with such events and would not be back to operation within one week while 27.3% are fully prepared.

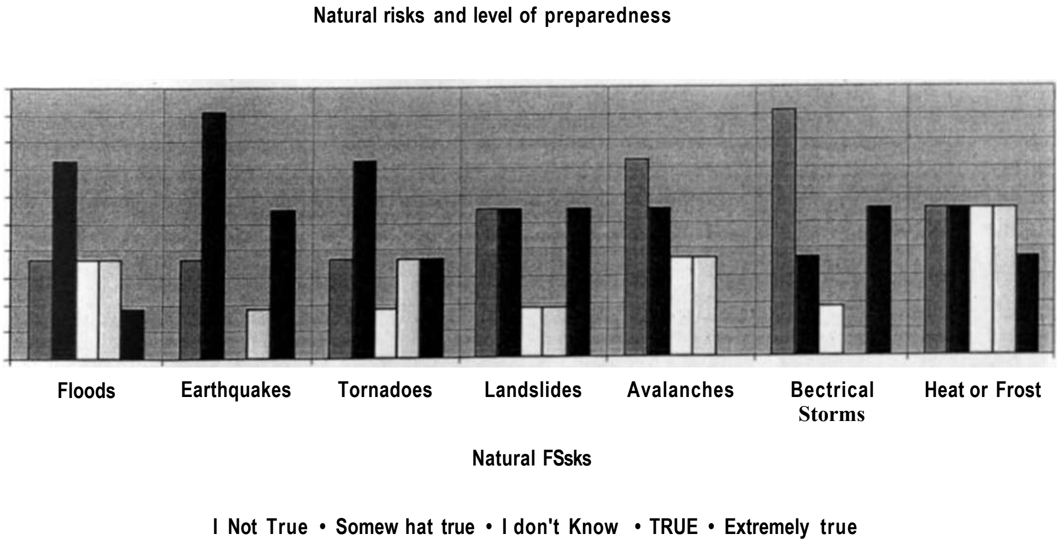
The data also shows low level of awareness and preparedness as far as Tornadoes and landslides are concerned. The results indicate that 9.1% do not know whether the office will operate should any of the two occur.

Table 4.4. Preparedness in dealing with naturally occurring risks

	Floods (%)	Earthquakes (%)	Tornadoes (%)	Landslides (%)	Avalanches (%)	Electrical Storms <%)	Heat or Frost (%)
Not True	18.2	18.2	18.2	27.3	36.4	45.5	27.3
Somewhat true	36.4	45.5	36.4	27.3	27.3	18.2	27.3
I don't Know	18.2	0	9.1	9.1	18.2	9.1	27.3
TRUE	18.2	9.1	18.2	9.1	18.2	0	27.3
Extremely true	9.1	27.3	18.2	27.3	0	27.3	18.2

In regard to dealing with naturally occurring risks, the data (Table 4.4) shows that most of the countries have not put in measures in place for dealing with naturally occurring risks. Preparedness in dealing with electrical storms (45.5%) and avalanches (36.4%) were least handled while 27.3% indicates that they are prepared to deal earthquakes, landslides and electrical storms. This is a low percentage considering the effects this would have on the organization in the event that systems are not available for more than a week.

Figure 4.2: Natural risks and level of preparedness



4.4. Environmental risks

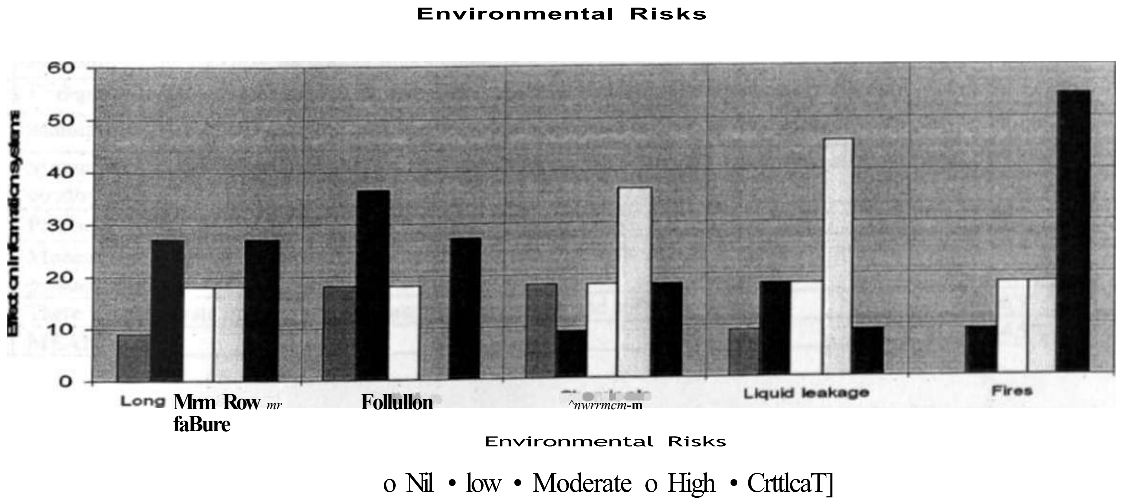
Environmental risks are a major threat source that affects full utilization of information systems in business processes. The study considered long term power failure, pollution, chemicals and liquid leakage as major environmental risks. In relation to environmental risks, the data showed that long term power failure would have critical effect (27.3%) and high effect (18.2%) on information systems. This shows that 45.5% of the organizations operations would be affected by long term power failure. The figures above reversed in relation to effects of pollution.

The data shows that fires registered the highest risk ("critical") as shown in Table 4.5. In the event of fire occurring, 54.5% of the information systems in the country would be affected and not likely to resume within a week after the incident. Liquid leakage and chemicals would highly affect a high percentage of operation (45.5% and 36.4% respectively).

Table 4.5. Environmental risks

	I-ong term Power failure (%)	**Pollution (%)**	**Chemicals (%)**	**Liquid leakage** (%)	**Fires (%)**	**MEAN** <%)
Nil	**9.1**	**18.2**	**18.2**	**9.1**	**0**	**10.92**
low	**27.3**	**36.4**	**9.1**	**18.2**	**9.1**	**20.02**
Moderate	**18.2**	**18.2**	**18.2**	**18.2**	**18.2**	**18.2**
High	**18.2**	**0**	**36.4**	**45.5**	**18.2**	**23.66**
Critical	**27.3**	**27.3**	**18.2**	**9.1**	**54.5**	**27.28**

Figure 4.3: Environmental risks



4.5. Practical Action's general preparedness

The study investigated a number of issues which are generally considered as important in information systems disaster and recovery process. The research considered 25 key indicators as listed in Table 4.6 to help in coming up with a general view of Practical Action's preparedness levels.

Table 4.6 IT risk preparedness indicators

	AWARENESS AND PREPAREDNESS INDICATORS	YES (•/.)	NO (%>
1	Effective and organization-wide disaster recover)' and business continuity programme	18.2	81.8
2	Forma] arrangements/agreements for an alternate processing site and equipment should the need arise to relocate your IS operations	18.2	81.8
3	Procedures for testing backup media at an offsite location	18.2	81.8
4	Formal intrusion program, other than basic logging, for monitoring host and/or network activity	18.2	81.8
5	Conducted awareness building on IS risks to the staff within your country office	27.3	72.7
6	Penetration testing of all public or internet-facing connections been performed	27.3	72.7
7	Whether IS Risk been an agenda your country or Regional Management Team meeting.	36.4	63.6
8	Existence of an inventory of each access point to your network (every connected device, wireless or remote), both inside and outside of the firewall.	36.4	63.6
9	Person in charge of General Risk management	54.5	45.5
10	Country/regional office allocated resources to support IS risks/ contingency funds	54.5	45.5
11	Disaster recovery and business continuity included in your risks assessment	54.5	45.5
12	Physical security reviewed over the last one year	54.5	45.5
13	Maintain topologies, diagrams, or schematics depicting your physical and logical operating environment* s)	54.5	45.5
14	Have an anti-spy ware management program to protect end-user systems	54.5	45.5
15	Protect the intellectual property of individuals such as trade secrets and patentable ideas/concepts	54.5	45.5
16	Performed an initial Information Systems risk assessment	63.6	36.4
17	Servers in environmentally controlled area with Smoke detectors. Water detectors. Fire suppression systems and Temperature sensors	63.6	36.4
18	Policies / procedures for proper disposal of information assets in place	72.7	27.3
19	Maintain offsite backups for critical information	72.7	27.3
20	IT department deactivate accounts for terminated or transferred employees in a timely manner	72.7	27.3
21	Maintain an unmanaged Antivirus management program to protect systems from Malicious content	81.2	18.8
22	Measures already in place to ensure business continuity in case of a major catastrophe affecting your country office	81.8	18.2
23	Practical Action has enough technical capacity to manage IS risks	90.9	9.1
24	Mission critical systems located in a locked location to which access is restricted to authorized personnel only?	90.9	9.1
25	There is an accurate inventory of all computing equipment and software	90.9	9.1
	MEAN	54.5%	45.5%

The data shows that 54.5% of the countries have a staff directly charged with risk management and 45.5% did not have. This shows that nearly 50% of the countries have not considered general risk management with a high priority as it should.

A high percentage (63.6%) has carried out initial risk assessment while 36.4% have never done such an assessment. This is confirmed by the data that indicated the same percentages in response to whether an information systems risk has even been an agenda in their management meetings.

The data shows that only 54.5% of the countries have allocated funds to deal with information systems risks. A high percentage of the respondents (72.7%) have never conducted awareness training to the staff against 27.3% have done capacity building to their local staff.

The data shows that Practical Action has got capacity to handle information systems risks (90.9%). This could be attributed to the fact that the respondents were IT experts. The data shows that there is no organization wide disaster recovery and business programme where 81.8% reported that this does not exist at all.

The results show that the organization has maintained an unmanaged antivirus programme where 81.8% showed that they have it in place. This however is not reflected in relation to the antispy ware program where only 54.5% have such a system in place. The risk exposure is also increased by the fact that within the organization, 81.8% have no formal intrusion program, other than basic logging in for monitoring host and /or network activity.

In regard to risk exposure the results show that 63.6% have no inventory of each access point to the office network for both inside and outside the firewall. Table 4.6 also shows that 72.7% have no penetration testing of public and internet facing connections have been performed.

In regard to preparedness in case of a risk to the organizations systems, the data shows that 81.8% indicated that incase of disaster, there are no formal arrangements to relocate information systems operations. The result shows that the organization heavily relies on offsite backup of critical systems to ensure business continuity (82%). The data shows also that 72.7% maintain an offsite backup of critical information even if not on real-time basis. However, 81.8% do not have in place a way to test whether the backed up data can be restored successfully.

Physical security of information systems infrastructure seems to be a priority within Practical Action. The data shows that 90.9% have all mission-critical systems are kept in a locked location and access in restricted to authorized personnel only. In addition to this, 63.6% have their servers in an environmentally controlled area with smoke detectors, water detectors, fire suppression systems and temperature sensors. The data shows that high percentages (90.9%) have an accurate inventory of all computing equipment and software.

4.6. General IT risk management and preparedness

Table 4.7: General IT risk management and preparedness

	Clear IT structure (%)	Managed and classified inventory (%)	Managed Physical Environment (%)	Compliance to change management (%)	Incidence Response and Problem Management (%)	Managed Service Level Agreements (%)	Service Continuity Management Plans (%)	Authentication, Authorisation and Access management (%)	Enhanced Training (%)
No Extent	9.1	9.1	9.1	9.1	0	9.1	18.2	9.1	9.1
Small Extent	9.1	18.2	27.3	18.2	9.1	18.2	18.2	27.3	27.3
Moderate Extent	63.6	0	18.2	54.5	63.6	36.4	36.4	9.1	45.5
Great Extent	18.2	63.6	45.5	9.1	18.2	9.1	18.2	54.5	18.2
Greatest Extent	0	9.1	0	9.1	9.1	27.3	9.1	0	0

Table 4.7 shows an analysis of general IT risk management and preparedness. In relation to the general IT management the data shows that Practical Action has significantly managed (63.6%) to set a clear IT unit structure, roles and responsibilities and accountabilities for each IT staff. Only 18.2% have achieved to a great extent. The data shows that 63.6% maintain an IT asset inventory, clearly classified and managed within the organisation while 45.5% have managed the physical environment to help preserve information confidentiality, integrity, and availability in compliance with appropriate health and safety and environmental regulations and legislation. The results show that 54.5% of the respondents indicated that they have complied with the laid down configuration, change, and release management policy within the organisation.

In relation to incident management, reporting and handling, the data shows that 63.6% success rate and 36.4% success rate in relation to Service Level Agreements (SLA) with key service providers and in relation to Service Continuity Management (SCM) plans. This includes building and maintenance of effective, business-aligned IT recovery plans and; continuous testing and improvement of IT recovery plans.

The success of country's authentication, authorization, and access a management, the data shows that 54.5% have to a great extent managed to ensure successful implementation. This means that as far as access to business critical data and IT systems; access to applications, systems, and effective and efficient maintenance and updating of user access authorization.

The data also shows that 45.5% of IT staff are trained and made aware of results of incorrect, inappropriate, and insecure behaviour and a reduction in such behaviour; enhanced awareness and understanding of governance, legal, and regulatory requirements; and reduction of errors and omissions.

4.7. General awareness issues

The research also sought to establish the current status of IT risk management. Table 4.8 shows that 45.5% of the respondents described Practical Action's IT risk management as ad hoc. This is a clear reflection of the need to develop well and systematic risk management procedures that are uniform for the whole group.

Table 4.8: Current status of Practical Action's IS risk management

Status	Frequency	Percent	Cumulative Percent
Ad Hoc	5	45.5	45.5
Well Defined	3	27.3	72.7
Managed And Measured	2	18.2	90.9
Optimised	1	9.1	100
Total	11	100	

The results of the risk management status confirms the fact the majority of the respondents expressed the need for developing a comprehensive IT risk management as a high priority (54.5%) and 27.3% expressed the need as critical. The results are as shown in Table 4.9.

Table 4.9 Priority levels

Priority	Frequency	Percent	Cumulative Percent
Critical	3	27.3	27.3
High Priority	6	54.5	81.8
Moderate Priority	2	18.2	100
Total	11	100	

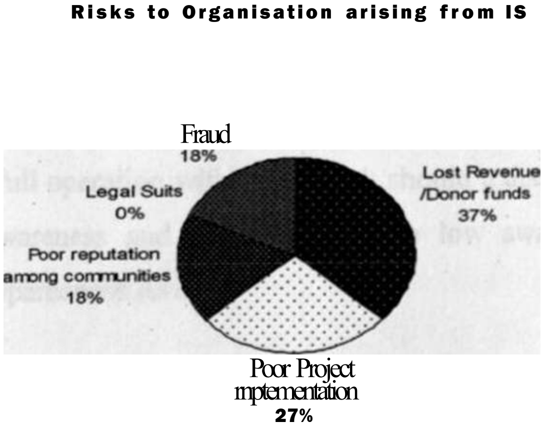
IT Risk management involves people, technology, processes and information. The data shows that to manage IT risk, the success will depend on people (54.5%), Processes (27.3%) and technology (18.2%). This is as shown in Table 4.10.

Table 4.10: Key players in IS risk management

Involvement	Frequency	Percent	Cumulative Percent
Technology	2	18.2	27.3
People	6	54.5	72.7
Processes	3	27.3	100
Total	11	100	

Information systems are a key component to the success of the organization. The data shows that the highest risk (36.4%) to the organization as a result of failure on information system (in terms of performance, security, availability and compliance) is loss of revenue or donor funds. This is followed by poor project implementation (27.3%) which has great impact on the success of the organization. Poor reputation among communities and frauds were rated lowest each with 18.2% risk.

Figure 4.4 Organizations' risks arising from information systems risks



CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1. Introduction

This study concerns the risk exposure of Practical Action. The study objectives were; to determine Practical Action's awareness of information systems risks; to determine the frequency of occurrence of the human related risks in Practical Action and; to determine the level of preparedness in mitigating human related risks, natural risks and environmental risks situations in Practical Action.

In this chapter, a summary of study findings, conclusions and recommendations are presented. In addition suggestions for further research and the limitations of the study are given.

5.1.1. Practical Action's awareness of information systems risks

It is vital to manage risks to systems. Understanding risk, and in particular, understanding the specific risks to a system allow organizations to protect the information system commensurate with its value to the organization. The fact is that all organizations have limited resources and risk can never be reduced to zero. So, understanding risk, especially the magnitude of the risk, allows organizations to prioritize scarce resources.

There is a general lack of awareness of naturally occurring risks. Without this awareness therefore, there is a high probability that the organisation is not fully prepared to handle risks arising from natural calamities or catastrophes.

In addition, the results indicates that most of the offices are not prepared to restore their information systems to full operation within one week should a disaster occur. There is a direct relationship between awareness and preparedness. The low awareness levels had a direct relationship with low preparedness levels.

Practical Action operates in four continents. The events and incidents occurring in each country are unique in nature. Earthquakes appeared to be a common threat in Asian countries and South

America and not considered much in Africa as a likely source of risk. In general, in all the naturally occurring risks, the results show high level of lack of awareness.

Long term power failure would highly affect the business in the countries the Practical Action operated. In the event of fire in the countries of operation, 54.5% indicated that the business would be affected for more that one week in the efforts to build the systems again.

5.1.2. Frequency of occurrence of human related risks

The first objective was to determine the frequency of occurrence of the human related risks in Practical Action. The findings show that 9.1% have dealt with computer criminals more than 5 times in one year. The integrated nature of Practical Action's IT systems require that the management should be prepared to deal with this as effects on one country would definitely have an impact within the group.

The greatest source of all human related risk within Practical Action is the insiders or the employees within the organisation. The results showed that the greatest threat to information systems is the poorly trained, disgruntled, malicious, negligent, dishonest and or terminated employees. Terrorist and computers criminals do not pose a major threat to information systems according to the analysed data.

5.1.3. Practical Actions preparedness in mitigating information systems risks

The study also sought to determine the level of preparedness in mitigating human related risks, natural risks and environmental risks situations in Practical Action. The overall results showed that a number of key issues that indicate the level of awareness are lacking within the country offices. The strengths and weaknesses differ from region to region but there are key issues that are clear and will need to be addressed.

Majority of the respondents indicated that there is no comprehensive and organisational wide disaster recovery and business continuity programme to help should the information systems within the organisation be affected globally.

All countries are keen with backup systems where 72.7% indicated that they maintain off-site backups of critical systems. However, a large percentage (81.8%) indicated they have not tested the backup media at an offsite location. The same was reflected in relation to lack alternative processing site and equipment in case of risk affecting systems within a country.

The level of IT risk awareness among non-IT staff is low as there has been little effort to build capacity of staff on issues of IT risk. A very high percentage (63.6%) indicated that information systems risk has not been discussed in any of the senior management meetings as far as they are aware. Information systems risks have been left in the hands of information technology experts without the management getting involved.

Practical Action appears to be very strong in terms of inventory management and IT capacity in terms of skills. Over 90% indicated that mission critical systems are secure. However this is negated by the fact the offline backups have not been tested well and no alternate sites have been identified in case of a major catastrophe occurring.

Antivirus management is a major source of risks in organisations. Practical Action appears to have satisfactorily managed to protect their systems from effects of virus infections (81.2%). The data also showed that 45.5% regarded IT risk management as ad hoc. This therefore means that there is need to put in place a coherent way of addressing risk management issues. Practical Action has put good systems to manage information systems but the extent of success is far below average on all of them.

5.2. Conclusion

The following conclusions can be drawn from the study.

a) There is great need to develop a comprehensive and all inclusive policy on the use of information systems to reduce the risks arising from insiders (employees).

b) There is generally low awareness among staff on information systems risks. The senior management have not dealt with the issues of information systems risks in an integrated manner and have considered other risks and left out what has turned out to be the backbone of the organisation - information systems.

c) There is need to develop the capacity of each country in terms of resources to ensure that they have alternate processing sites and equipment, testing equipment and real time backup systems to an offsite destination.

d) The general view from the results of the findings is that Practical Action has averagely performed well in terms of risk management with an average of 54.5% showing success in key preparedness indicators and 45.5% showing lack of success in key preparedness indicators used in the study.

5.3. Recommendations

The research findings show that:

a) Training on risk management is critical to success in risk management and that knowledge on disaster recovery and management would be key to reducing the information systems risk profile.

b) There is a need for alternative source of power for each of the country office as long term power failure would greatly affect information systems.

c) There is great need to evaluate the risk of fires in each country and the level of preparedness in each of the countries.

d) Contingency plans need to be put in place to ensure that each country is able to recover within a short period should any risk happen to occur. This includes allocation of funds for this purpose.

e) There is a need for involvement of senior IT staff in the senior management team (global) to help incorporate information systems issues in the decision making process.

5.4. Study limitations

The study was carried out in only one organisation and though it may provide typical information of an international NGO, it may not be possible to generalise the data as organisations differ in many ways as far as information systems implementations are concerned. In some countries, IT staff are not be very fluent in English (Arabic and Spanish speaking countries) though they may understand the language. Understanding the questionnaire may have been a challenge.

5.5. Suggestions for further research

There are key research areas that this study did not cover and form a good basis for further research. These include:

a) Why employees are the greatest information systems risk source within the organisation and the likely factors that could be contributing to this.

b) Management perception and role in IT risk management.

c) Challenges of integrating the senior management team in dealing with information systems management.

d) Developing a comprehensive and an integrated risk management model that can apply to any organisation.

e) Risks of global distributed systems.

f) Impact of information systems risks to organisations and their business continuity.

REFERENCES

Alberts, C. (2008), "Mission Diagnostic Protocol, Version 1.0: A Risk-Based Approach for Assessing the Potential for Success". Software Engineering Institute. Retrieved on 2008-05-26.

Alexander, C. (2005), The Professional Risk Managers' Handbook: A Comprehensive Guide to Current Theory and Best Practices. PRMIA Publications.

Aligning COBIT, ITIL and ISO 17799 for Business Benefit. (Rolling Meadows, IL: IT Governance Institute and Norwich,UK: Office of Government Commerce, 2005).

Aligning COBIT, ITIL and ISO 17799 for Business Benefit: Management Summary (2005), USA. Available at www.itgi.orR

Anyanje, S. (2005), Analysis of factors affecting information & communication technology development in Kenya. The case of network operators.

Baccarini, I. (2004). " Management of Risks in information Technology Projects : Industrial Management & Data Systems, Volume 104. Number 4 2004 pg 286-295

Benaroch, M. (2002)Managing investments in Information Technology based on real options theory, Journal of MIS, Fall 2002, pp. 43-84.

Anon, S. (2007), Business Roundtable. Growing Business Dependence on the Internet—New Risks Require CEO Action. (Washington DC: September, 2007).

Caldwell, F. (2006), Risk Management and Business Performance Are Compatible. (Stamford, CT: Gartner, Inc. October, 2006).

Caldwell, F. (2007), The 2007 Compliance and Risk Management Planning Guidance: Governance Becomes Central. (Stamford, CT: Gartner, Inc. April, 2007).

CIO Magazine. State of the CIO Survey, http://www.cio.com/state. (Boston: International Data Group, 2007).

Dorfman, G. (2007), Introduction to Risk Management and Insurance (9th Edition). Englewood Cliffs, N.J: Prentice Hall.

Dynes, S., Eva, A. and Johnson, M. (2007), "Cost to U.S Economy of information Infrastructure Failures", Http://www.ists.dartmouth.edu/library/207.pdf.

Emmett, J. Vaughan, P., Therese, M. and Vaughan, L. (1995). Essentials of Insurance: A Risk Management Perspective. John Wiley & Sons Inc, Pg 5-17.

Finley, I. (2007). IT Risk Comes Into Fashion. (Boston: AMR Research, August, 2007).
George (1989) Principles of Insurance, 3rd Edition, Pg 3-5

Gordon, B. (2006). CSI/ FBI Computer Crime and Security Survey. http://www.goCSI.com. (San Francisco: Computer Security Institute, 2008).

Graham, W.; (May 2007), "Refreshing Management of Risk: Guidance for Practitioners; Best Management Practice, USA pg 1-5

Gupta, R. (2006), "ITIL Adoption." E-Business Blog, http://www.line56.com. (Los Angeles: Line56.com, July 13, 2008).

Heisser, J. (2006), Choosing Risk Management Methods. (Stamford, CT: Gartner, Inc. June, **2006).**

Hughes, G. (2007) IT Risk Management Report, Trends Through December 2006; Symantec Corporation Volume 1 Pg 37-42, USA

Hughes, G. (2008), IT Risk Management Report: Myths and Realities, Trends through Dec 2007, Volume 2 pg 2-24

Infoconomy Ltd (2004). From Contingency to Continuity." Information Age, http://www.information-age.com. (London: Infoconomy Ltd. February 10, 2008)

Information Technology - Security Techniques - Code of Practice for Information Security Management. (ISO/IEC 17799:2005(E). (Geneva: International Organization for Standardization, 2005).

International Standard ISO/IEC 17799:2005, (2007). Information Technology - Security Techniques - Code of Practice for information security management: Switzerland

IT Governance Institute. "Framework Control Objectives, Management Guidelines, maturity Models (COBIT 4.1), US

IT Infrastructure Library, http://www.itil.co.uk. (Norwich, UK: Office of Government Commerce).

IT Policy Compliance Group. Taking Action to Protect Sensitive Data. (February, 2007).

Kapuria, (2006): Addressing IT Risks of Software Applications, USA, pg 2-5.

Kapuria, S. (2007), Addressing IT Risks of Software Applications: A Risk Management Strategy. USA, Pg 3-8.

Kark, K. (2007), Security Budgets Increase: The Transition to Information Risk Management. (Cambridge, MA: Forrester Research, Inc. January, 2007).

Kyama, S. (2006), Global Terrorism Analysis, Volume IV, Pages 6-8

Lamy, L. (2007), IT Risk Management: A Business Issue of Strategic Importance. (Framingham, MA: IDC, July, 2007).

Liautaud, K. and Hammond, P. (2001), E-business intelligence; turning information into knowledge into profit, McGraw-Hill, New York.

Munuki, D. (2006), Determinants of ICT application among small and medium enterprises in Nairobi.

Ngemu, A. (2005), A survey of computer forensic practices in litigation support. A case of the banking industry in Kenya.

Nzuki, C. (2006), A survey of ICT audit in commercial banks in Kenya.

O'Brien, J. (2000), Introduction to information systems; essentials for the internetworked enterprise (9th edition), Irwin McGraw-Hill, New York.

Porter, M. (1985), Competitive Advantage: Creating and Sustaining Superior Performance. (New York: The Free Press, 1985).

Practical Action (2007), Practical Action Annual Report

Rasmussen, M. and Michael, S. (2006), Business Drivers for Enterprise Risk Management. (Cambridge, MA: Forrester Research, Inc. February, 2007).

Risk and Insurance Management Society (July 2006). Risk management Magazine pgs 34-40, available at www.rmmag.com.

Risk Management Standard (2002), Published by AIRMIC, IRM, ALARM - pg 2-5, London.

Ritchie, K.(1998), Information systems in business, International Thomson Business Press, London.

Ropponen, J. (1999), Software Risk Management: Foundation, Principles and Empirical findings. University Printing House, Finland.

Steinberg, G. (2004), Enterprise Risk Management - Integrated Framework: Committee of sponsoring organisations of the Tradeway commission (COSO): USA

Sterling, P. (2006), ITIL Change Management Maturity Benchmark Study. (Sterling, VA: Evergreen Systems, Inc., July 2006).

Steve, P. (2006), An introduction to Information Risk Management; Information Security Reading Room (Sans Institute)

Stoneburner, G., Goguen, A. and Feliga, A. (2002), Risk Management guide for information Technology Systems: National Institute of Standards and Technology, USA.

Swanson. M„ Wohl, A. and Pope, L. (June 2002), Contingency Planning Guide for Information Technology Systems: National Institute of Standards and Technology Publication, USA

Symantec Corporation (2006), IT Risk Management, "An Essential Strategy for Success", Available at www.svmantec.com

The Boston Consulting Group. Innovation 2007: A BCG Senior Management Survey. (Boston: August, 2007).

Westerman, J. (2007), IT Risk: Turning Business Threats into Competitive Advantage. (Boston: Harvard Business School Publishing, 2007).

World Bank (May 2004), "Technology Risk Checklist Version 7.3. World Bank Integrator Unit and TRE Security Team Collaboration.

APPENDICES

Appendix I: Questionnaire

UNIVERSITY OF NAIROBI
SCHOOL OF BUSINESS

MBA PROGRAMME- LOWER KABETE CAMPUS

Telephone: 020-2059162
Telegrams: "Versify", Nairobi
Telex: 22095

P.O. Box 30197
Nairobi, Kenya

Date: 15th September 2008

TO WHOM IT MAY CONCERN

The bearer of this letter, SAMUEL WERU. Registration No: D61/P/7158/2003 is a Master of Business Administration (MBA) student of the University of Nairobi.

He is required to submit as part of his coursework assessment a research project report on a management problem. We would like the students to do their projects on real problems affecting organizations. We would therefore appreciate if you could assist him by allowing him to collect data in your organization for the research.

The results of the report will be used solely for academic purposes and a copy of the findings will be availed to the organization.

Thank you.

DR. W.N.IRAKI
CO-ORDINATOR, MBA PROGRAMME

Section I: Human Related Risks

A: The following are Human related risks/threats to information systems. Please indicate all that you have had to deal with in the one year and how often.

No.	Risk	Examples of risks/threats	Have you had to deal with any of the actions the last one year?	How often have you had to deal with this type of risk in the last one year? Please tick where applicable		
				Once	2 to 5 times	More than 5 times
1	Hacker, cracker	Hacking, Social engineering. System intrusion, break-ins, Unauthorized system access	●	●	●	●
2	Computer Criminal	Computer crime (e.g., cyber stalking). Fraudulent act (e.g., replay, impersonation, interception), Information bribery, Spoofing, System intrusion	●	●	●	●
3	Terrorist	Bomb/Terrorism, Information warfare. System attack (e.g., distributed denial of service), System penetration. System tampering	●	●	●	●
4	Industrial espionage (companies, other NGOs, foreign governments, other government interests)	Economic exploitation, Information theft, Intrusion on personal privacy. Social engineering, System penetration, Unauthorized system access (access to classified, proprietary, and/or technology-related information)	●	●	●	●
5	Insiders (poorly trained. disgruntled, malicious, negligent, dishonest, or terminated employees)	Assault on an employee. Blackmail, Browsing of proprietary Information, Computer abuse, Fraud and theft, Information bribery, Input of falsified, corrupted data, Interception, Malicious code (e.g., virus, logic bomb, Trojan horse), Sale of personal information, System bugs, System intrusion, System sabotage, Unauthorized system access	●	●	●	●

Others, Please specify

B: The human related categories of risks are listed below. Please indicate by ticking the appropriate box, which one between the pair is a bigger worry to you.

1.	Hacker or Cracker	●	and	Computer criminal	●
2.	Hacker or Cracker	●	and	Terrorist	●
3.	Hacker or Cracker	●	and	Industrial Espionage	●
4.	Hacker or Cracker	●	and	Insiders (employees)	●
5.	Computer criminal	●	and	Terrorists	●
6.	Computer criminal	●	and	Industrial Espionage	●
7.	Computer Criminal	●	and	Insiders (employees)	●
8.	Terrorist	●	and	Industrial espionage	●
9.	Terrorist	●	and	Insiders	●
10.	Industrial Espionage	●	and	Insiders (employees)	●

Section 2: Natural risks

A: The following are types of naturally occurring risks. Depending on your country office, please indicate your level of awareness which is dictated by the measures you have put in place in case it happens. Indicate in the space provided below the table.

	NO AWARENESS	LOW AWARENESS	MODERATE AWARENESS	HIGH LEVEL AWARENESS	CRITICAL AWARENESS
1. Floods	●	●	●	●	●
2. Earthquakes	●	●	●	●	●
3. Tornadoes	●	●	●	●	●
4. Landslides	●	●	●	●	●
5. Avalanches	●	●	●	●	●
6. Electrical storms	●	●	●	●	●
7. Heat/frost	●	●	●	●	●

Other information/Natural risk, Please specify

B: In case of the following types of naturally occurring risks, please select the best answer to the following statement.

"Our country office has put in place means and plans of continuing to operate without critical loss of data or information within ONE week from the time the incident occurs"

	NOT TRUE	SOMEWHAT TRUE	I DON'T KNOW	TRUE	EXTREMELY TRUE
1. Floods	●	●	●	●	●
2. Earthquakes	●	●	●	●	●
3. Tornadoes	●	●	●	●	●
4. Landslides	●	●	●	●	●
5. Avalanches	●	●	●	●	●
6. Electrical storms	●	●	●	●	●
7. Heat/frost	●	●	●	●	●

Section 3: Environmental Risks

In the event of the following environmental incidents occurring in your country, please indicate the effect they would have on your information systems and smooth running of the country office.

Nil= no effect and Critical = operation would stop for more than a week.

	Nil	LOW	MODERATE	HIGH	CRITICAL
1. Long-term power failure	●	●	●	●	●
2. Pollution	●	●	●	●	●
3. Avalanches	●	●	●	●	●
4. Chemicals	●	●	●	●	●
5. Liquid leakage	●	●	●	●	●
6. Fires	●	●	●	●	●

Section 4: Practical Action's preparedness in handling information systems risks

	YES	NO
1 • Does your country office have a person in charge of General Risk management?	●	●
2. Have you ever performed an initial Information Systems risk assessment?	●	●
3. Has Information Systems Risk been an agenda your country or Regional Management Team meeting (as far as you are aware)?	●	●
4. Has your country/regional office allocated resources to support Information systems risks/ IT contingency funds?	●	●
5. Have you ever conducted awareness building on Information systems risks to the staff within your country office?	●	●
6. In your view, do you consider that Practical Action has enough technical capacity to manage Information systems risks?	●	●
7. Do you have an organization-wide disaster recovery and business continuity programme in your country of operation in case of disaster?	●	●
8. Is disaster recovery and business continuity included in your risks assessment?	●	●
9. Do you have formal arrangements/agreements for an alternate processing site/equipment should the need arise to relocate your information systems operations?	●	●
10. Do you have policies / procedures for proper disposal of information assets? E.g. old computers	●	●
11. Are there measures already in place to ensure business continuity in case of a major catastrophe affecting your country office e.g remote backup sites (real time), Backed up data stored offsite, UK synchronised data in Sharepoint and Sun Systems	●	●
12. Are mission critical systems located in a locked location to which access is restricted to authorized personnel only?	●	●
13. Has physical security been reviewed over the last one year?	●	●
14. Are servers in environmentally controlled area with Smoke detectors, Water detectors, Fire suppression systems and Temperature sensors?	●	●
15. Is there an accurate inventory of all computing equipment and software?	●	●
16. Do you maintain offsite backups for critical information?	●	●
17. Do you have procedures for testing backup media at an offsite location?	●	●
18. Do you maintain topologies, diagrams, or schematics depicting your physical and logical operating environment(s)	●	●
19. Do you maintain an unmanaged Antivirus management program to protect systems from Malicious content?	●	●
20. Do you have an anti-spy ware management program to protect end-user systems?	●	●
21. Do you have formal intrusion program, other than basic logging, for monitoring host and/or network activity?	●	●
22. Does your country office have an inventory of each access point to your network (e.g. every connected device, wireless, remote etc.), both inside and outside of the firewall, in order to identify potential points of vulnerability?	U	●
23. Has penetration testing of your public or internet-facing connections been performed?	u	●
24. Does Practical Action in you view protect the intellectual property of individuals such as trade secrets and patentable ideas/concepts?	u	●
25. Does the IT department deactivate accounts for terminated or transferred employees in a timely manner (immediately)?	u	●

Please check in the box which most closely reflects your country office level of preparedness in dealing with Information Systems risks and avoiding such risks in future.					
	NO EXTENT	SMALL EXTENT	MODERATE EXTENT	GREAT EXTENT	*Greatest Extent*
1 - To what extent have you managed to set up a clear IT Unit Structure, Roles and Responsibilities and accountabilities for each IT staff? To what extent has this been realised?	●	●	●	●	●
2. To what extent have you maintained an IT asset Inventory, clearly classified and Managed within the organisation?	●	●	●	●	●
3. To what extent have you managed the physical environment to help preserve information confidentiality, integrity, and availability in compliance with appropriate local regulations and legislation? (e.g. Software copyright laws in your country)	●	●	●	●	●
4. To what extent have you complied with Configuration, Change, and Release Management policy within the organization (Ref: IIT meeting in 2007)?	●	●	●	●	●
5. How would you rate Practical Actions's level of realisation of Incident, Response, and Problem Management?: Includes effective IT incident response and problem management processes, effective escalation procedures, effective management of incident impact, effective management of day-to-day problems and issues.	●	●	●	●	●
6. To what extent have you managed to sign Service Level Agreements (SLA) with key service providers (e.g. ISP) in your country office in such a way that you can measure performance against defined SLAs?	●	●	●	●	●
7. To what extent have you implemented Service Continuity Management plans? This includes building and maintenance of effective, business-aligned IT recovery plans; and continuous testing and improvement of IT recovery plans?	●	●	●	●	●
8. How would you rate the extent of success of your country's Authentication, Authorization, and Access Management? (access to business critical data and IT systems; access to applications, systems, and effective and efficient maintenance and updating of user access authorization)	●	●	●	●	●
9. To what extent are you trained and made aware of results of incorrect, inappropriate, and insecure behaviour and a reduction in such behaviour; enhanced awareness and understanding of governance, legal, and regulatory requirements; and reduction of errors and omissions?	●	●	●	●	●

Section 5: General Awareness

10. in your own view, how would you describe the status of Practical Action's IT risk management

- Non-existent
- Ad hoc
- Well defined
- Managed and measured
- Optimized

11. How would you rate the need to establish a comprehensive IT risk management as a priority in your country office?

- Critical
- High Priority
- Moderate Priority
- Low Priority
- Not a priority

12. IT Risk management involve Technology, People, Processes and Information. Which one would you consider the most important ofall in ensuring that IT Risks are minimized, (choose one)

- Technology
- People
- Processes
- Information

13. What would you consider as the highest risk that could arise as a result of IT incidents and inefficiencies

- Lost Revenue /Donor funds
- Poor Project Implementation
- Poor reputation among communities
- Legal Suits
- Fraud

Please add any other information that you consider of importance in line with the questions above that would help in establishing Practical Actions risk profile.

^«ction 5: General Awareness

1O- **In your own view, how would you describe the status of Practical Action's IT risk management**

- **Non-existent**
- **Ad hoc**
- **Weil defined**
- **Managed and measured**
- Optimized

11. **How would you rate the need to establish a comprehensive IT risk management as a priority in your country office?**

- **Critical**
- **High Priority**
- **Moderate Priority**
- **Low Priority**
- **Not a priority**

12. **IT Risk management involve Technology, People, Processes and Information. Which one would you consider the most important of all in ensuring that IT Risks are minimized, (choose one)**

- **Technology**
- **People**
- **Processes**
- **Information**

13. **What would you consider as the highest risk that could arise as a result of IT incidents and inefficiencies**

- **Lost Revenue Donor funds**
- **Poor Project Implementation**
- **Poor reputation among communities**
- **Legal Suits**
- **Fraud**

14. **Please add any other information that you consider of importance in line with the questions above that would help in establishing Practical Actions risk profile.__**