The Cyber Citizen and Homeland Security

Freedoms versus Fears

Godfried B. Williams

CONTENTS

List of Contributors

Editing consultant:

Jamil Ampomah, Association of Chartered Accountants, UK

Forward by: Dr. Geoffery Writes,   Verizon

Preface:

The motivation to write this book and inspiration to complete it has been drawn from the memory of my dear wife and silver back Sylvia. The underlying ideas of this book commenced almost a decade ago after reflecting on my personal digital footprints accumulated from business and social trips. I enjoyed several economic and social freedoms while on business as a result of connectivity through the Internet and mobile devices. These enabled me to communicate to my family and friends in England and other parts of the world. These experiences made me to appreciate and value everyday technology that I sometimes took for granted. I also occasionally pondered over common security issues and concerns anytime I got connected to the Internet or used my mobile phone. These experiences created a vivid picture of my digitized footprints and brought to mind the cyber nature of my activities inland and overseas. I began thinking as a cybercitizen who was not limited by any form of communication boundaries. I saw opportunities that could be exploited for business and social advantage as well as threats due to the excessive exposure of my digital footprints to public networks. These background experiences have made me to believe that it is essential that the general public, policy makers, political leaders, educators, businesses and learners understand the evolving nature of citizenship within the context of the cyber world. The availability of technology and other mobile software packages allow many people to have access to information freely, enabling mobility globally across national jurisdictions without individuals and groups stepping a foot on the soil of these countries. It is important to educate ordinary citizens in local communities of the freedoms and opportunities that come along with technology as well as discuss the threats, fears and anxieties shared by many, including states, governments, families and individuals. The freedoms we enjoy due to these technologies in this decade also enable vulnerabilities that could be exploited by people and governments with malicious intent. It is plausible to argue that the cyber world brings along homeland and national security issues that States and Governments dread. Consequently they are anxious to address them without jeopardising the freedoms of citizens. Among most feared concerns are Cyber Attacks and Terrorism. In this book I discuss what these freedoms and fears are, and exploit strategies and models for managing them effectively. The book is made up of two parts. The first part explains identity of the Cyber Citizen, rights, expectations, economic freedoms and opportunities, whiles the second part discusses cyberattacks, terrorism and counterstrategies and models useful for citizens and states in responding to malicious intentions and attacks.

Chapter 1

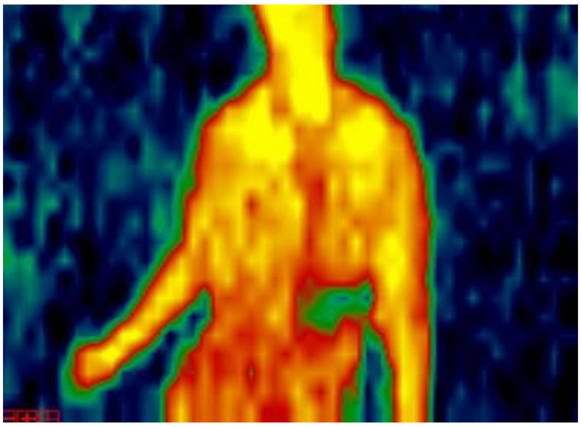
Cyber Citizenship

This book is the first to examine the impact of Cyber Citizenship on homeland and national security. The author asserts that digitization of human activities; business transactions and communications in social life are unavoidable, as such has changed the cultural landscape of many nations. In this respect digitized processes have become a part of human life, especially among technologically advanced economies. It is also fundamental to the comfort and pleasure to human life as well as efficient and effective for running businesses. This book argues that the digitized nature of human life has an impact on homeland and national security with respect to a community, people or nation. This implies that enhancing security and safety of citizens in a digitized era should be of pivotal importance to the security and defense apparatus of every nation and people. The lack of awareness among ordinary citizens, organizations and communities has made managing the relationships and coexistence among people or culture challenging. This is due to the lack of importance placed on the interrelationship between cyber citizenship, national and homeland security. This is also essential to causes of insecurity and safety issues among users of the Internet, and other critical infrastructure. There is also a paradox to this type of citizenship as it is not defined by a voluntary act or by law enacted by any Parliament. Cyber citizenship is rather defined by the globalized nature of digitized activities carried out by people that operate within different legal jurisdictions.

This book defines the cyber citizen as any inspired entity either human or artificial, capable of carrying out a set of cohesive processes, on the Internet, Mobile Phones and Computer Networks. It can also mean any entity or "Being" that has digitized existence and footprints on network and communication platforms. Any human or process that has the ability to interact socially, act economically and politically on digitized processes can be considered to be a cyber citizen. This book therefore does not limit the definition of cyber citizenship to humans.

A typical example is the numerous Apps deployed on social networks and mobile platforms that carry out human like functions in business and recreation. For instance an App may be entirely designed as an evolving autonomous intelligent software agent capable of carrying out surveillance operations, protecting critical infrastructure or launching cyber attacks. There are also Apps that support critical infrastructure such as water managements systems or the generation and production of electricity.

It can also be defined as an entity whose activities and operations cut across national boundaries and jurisdictions. Although citizenship by conventional reasoning is defined by law as a voluntary act as such a human vocation, this definition does not necessarily apply to the case of the Cyber World.



Courtesy of Scientific Development Branch Home Office –

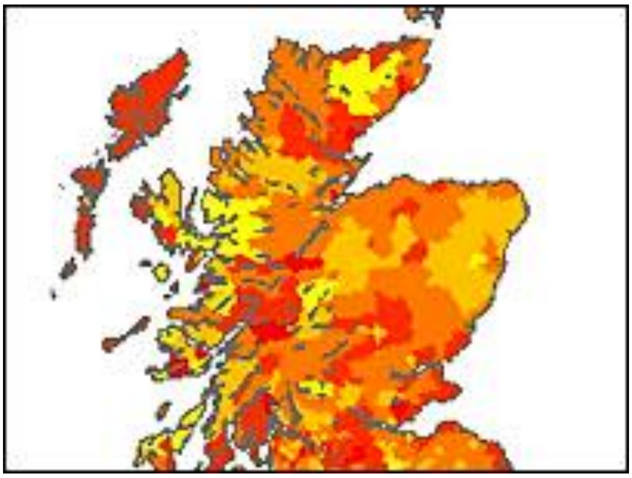
United Kingdom

This book discusses threats, vulnerabilities and personal responsibilities of the cyber citizen, economics, payments, social networking, cyber law, the continuous threat of terrorism, aviation security and safety, non terrorist threats and infrastructure and technology that drives critical services for the benefits and freedoms enjoyed by ordinary citizens.

Threats and Personal Responsibilities

The author described the Internet in previous works as an "ammunition depot" with no walls or security guards" Williams G (2007). Public users with malicious intentions could unleash lethal tools freely accessible on the Internet for destructive purposes, causing distress and occasionally significant losses of data among end users of computer systems and networks. It is therefore crucial that a cyber citizen become aware of essential systems that ensure basic safety and security. There are also guiding principles required to ensure that necessary safeguards and protection are properly implemented. This is due to common vulnerabilities and threats such as identity theft, email leaks, stolen passwords from users of online banking services, mobile voice mails, SIM and memory cards hacking, snooping tactics, wireless access points scanning for infrared, blue tooth and micro waves signals within the electromagnetic spectrum (EMS). Other forms of weaknesses are viruses, unsolicited emails, spam, malware, excessive download and use of online calling systems.

The next section of this book explores certain forms and sources of system vulnerabilities externally driven through social engineering and networking. One of such networks is the cyber tribe believed by the author as a key driver of the cyber world. This has been a growing phenomenon in recent times.



Households in Britain can be classified into 23 "e-types" depending on their access to technology, say researchers. (A research by UCL)

Cyber Tribes

Cyber activities may sometimes be carried out through organised groups also known as Cyber tribes (Williams G & Arreymbi J, 2008). Cyber Tribes is an alliance and association formed by organised network of people who have similar interest on the Internet. Whiles these groups in most cases operate with no malicious intent, there are others that have also capitalised on the nature of similar networks for malicious purposes by exploring virtual communities. The attributes of cyber tribes are a common language, similar belief systems, culture, traditions, practices and/or interest. Tribes are formed to: communicate, disseminate information and build relationships. However, no assurance of personal interest protection, control and, safeguards. There is also no hierarchy or ranking of such an organised group.

Cyber World

This comprises but not limited to online commercial activities, social platforms, such as chat rooms, bloggers, email, YouTube, MySpace, Facebook, Bebo etc. Entertainment – Music, distribution/download, game play etc, bullying, hatred and incitation (suicides), economical, Money scams, Money Laundering, Information Theft, Political radicalisation, Confrontation, Intimidation, Terrorism, Identity theft, Spoofing etc. spamming, and DOS attacks, Paedophilia, Cryptography Crime concealment etc. Spoofing, and spam attacks, malware trace, theft, sabotage, sale of critical business information and, more recently cyber terrorism.

Although there are several gadgets and aspects of the cyber world, this section explores what the author considers as the main categories that provide traceability of digital footprints of citizens in the cyber world. The main areas discussed are Online banking, marketing and sales, social networks, electronic discovery systems through emails, social, Internet telephony (VoIP) such as Skype and mobile base applications deployed by a number of carriers and providers. A fundamental aspect of the cyber world is that it is driven by ordinary people quite often with no technical know how about how these systems have been engineered and built.

Cyber Processes & Infrastructure

Figures 1 is a conceptual framework of the cyber citizen and associated activities, processes and the digital footprints essential to help in building a better understanding of the relationships between homeland security and the cyber world. This also depicts the traceability of personal data that characterises a digital footprint in a cyber world. The conceptual framework provides an abstraction of the interrelationship of essential processes that govern the cyber citizen and the boundaries of its world.

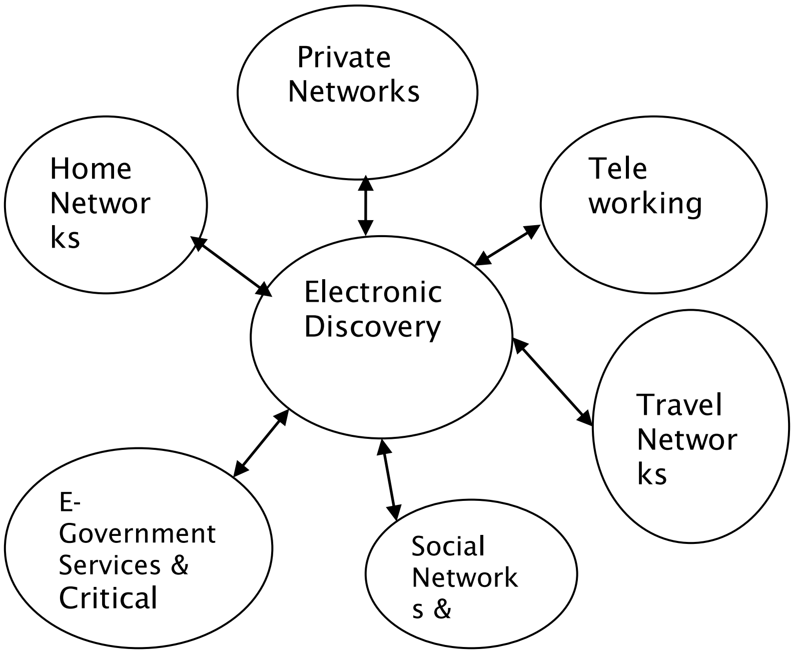


Figure 1 –Conceptual View of the Cyber Citizen

Common issues and challenges

The nature of the cyber world's daily activities and routines are driven by the use of online and mobile devices. This gives rise to a number of challenges and issues that need to be understood and at worst recognised. In this section the book explores some of the fundamental issues and factors that are likely to lead to isolation of users within the domain and confines of a security infrastructure. These issues may include poor education, lack of awareness among user community, right of access and privileges to information pools and systems that store and hold personal information of end users within the information chain. The safety and security implications of online services is due to a lack of defined purpose or set goals as well as difficulties in appreciating the actual value of information due to its intangible nature. Information usage in an operational and strategic setting within an organisation is also essential to our understanding of these issues. Using online information services just for the sake of recreation, pleasure and low cost to services and products may itself not constitute a weakness or a lack of awareness in respect of potential vulnerabilities to safety or security. There is however the general believe that greater awareness should be a part of strategic planning and leadership. This may serve as an effective tool for accelerating communities online and conventional methods leading to a better understanding of how all these technologies work and complement each player.

Cyber Citizen Programmes

There are a number of cyber citizen awareness programmes at the United Kingdom, United States and other parts of the advanced and developing worlds. This forms part of government policy designed to bring the general public in line with opportunities as well as issues associated with the use of digital devices and services. These programmes mainly attempt to create and raise awareness among ordinary citizens. The programme is usually government led and driven as part of its strategy to encourage security and safety awareness of Internet technology. They are also designed to encourage openness among users such as children, parents and teachers by discussing issues likely to affect them. Citizens are also assisted to understand that home computers can themselves be a target for malicious people by spreading computer viruses and other forms of malware. Citizens need to also appreciate that as much as computers and digital technologies enable easy access to information and interaction among people, it can also be a source of weaponry to committing crimes such as money laundering, identity theft and other fraudulent practices. Some of the organisations championing mitigating strategies in response to these threats include, The Department of Justice in Computer Crime and Intellectual Property www.cybercrime.gov, The Computer Emergency Response Team (CERT) at www.cert.org, and The National Infrastructure Protection Centre at the FBI found at www.infragard.net and the DHS (Department of Homeland Security) of the United States.

In the United Kingdom, cyber security strategy is underpinned by three main goals; safety, security and resilience in cyber space with the overriding aim that citizens, businesses and government can enjoy the full benefits of a joint responsibility by working together at home and overseas to understand and address risks, improve knowledge and awareness among citizens. There is also the need to ensure that the civil liberties of citizens are upheld with the highest regard, however ensuring that the same citizen's safety and security are not undermined.

Training Citizens

Part of the strategy for creating a robust cyber security environment should be the creation of pseudo training centres led by citizen bureaus or community centres. This does not refer to creating IT Centres, but rather a viral training strategy that mainly aims at raising the awareness of the opportunities, threats, safety and security issues associated with the use of digitised and mobile network systems. This should be a system that is capable of replicating itself across different parts of a nation. This is an essential component of cyber threat response. This is where governments in United Kingdom and United States are failing to achieve meaningful targets. There is an over emphasis on elite cyber forces.

Recently the GCHQ (Government Communication Head Quarters) in the United Kingdom launched a program to recruit eighteen year olds to train them as future elite cyber gurus. Although such initiatives are designed for all useful purposes, it fails to recognise that creating elite forces to protect critical infrastructure does not protect home computers used by citizens of the United Kingdom. This is because every home computer and mobile device hooked to the Internet is a potential cyber battleground and a war zone. This consequently suggests that inhabitants of such war zones should know how to employ tools critical for the defence of their personal information and IT assets without relying on some remote elite force.

Summary of Chapter 1

This chapter discussed training programmes for citizens, common issues and challenges, the phenomenon of cyber tribes, cyber world, threats, freedoms, cyber processes and critical infrastructure essential for deploying a robust cyber security system. Citizens in the United Kingdom, United States and other parts of the world need to have access to training programmes that build user awareness of issues on a daily basis. One of the common issues is identity theft. The proliferation of personal and private details on social networking sites can be sometimes astonishing. The simplicity and innocence to which ordinary users voluntarily submit information across social network channels such as Facebook, Kuntoo and Twitter need a much more detailed review and arrangements. In order for the role of security agencies to be effective and central to the activities of citizens, ordinary users should be encouraged to be a part of implementing a more cohesive and coordinated security process and structure. Chapter 2 examines life online and associated systems that support it.

Chapter 2

Life Online

Online social life is about how ordinary people and citizens take advantage of social networks to connect with people for entertainment, socialisation and keeping in touch with the daily lives of friends and family. The networks that support this form of life online are commonly described as social networks. On a broader perspective it is more a sociological and technological phenomena. Sociologists would define it as a network of people through friendship, work, family, interest and business activities. From a technological perspective these are communication network platforms that enable one to one and group communications for a wide range of purposes. The technology architecture that drive social networking platforms are distributed computer networks. This chapter discusses life online and the computer networking paradigms that power and enable group communications on these social networks and media.

A Cluster of Social Networks – Figure -2

Information sharing concepts and techniques

Social networking sites use file and data sharing techniques to share information among a group of people for entertainment, business, socialisation or work. The information shared is usually in the form of files or electronic folders. Data communication software may be effectively deployed to analyse the communication structure and multiple interactions that occur among users of these networks. Although there have been some developments in recent years with regards to analytics software, current law provision is inadequate when attempting to harmonise safety and security concerns with rights to privacy enjoyed by the citizens of many countries. Perhaps the west might be reluctantly drifting towards Internet models used by countries such China and Indonesia, where access to certain types of information on the Internet is restricted for homeland and national security purposes. Perhaps the “West” has failed to recognise the necessity of such a model or subsidiary model that entails such line of reasoning.

Social networks use “links” an information sharing technique to enable information required by users to establish a connection between the file to be shared and the directory entries of the users who want to have access to this file. Social networks such as Kuntoo photo sharing which connects people to places, Facebook, Linkedin and Twitter connect to profiles belonging to similar networks provided they have the appropriate permissions that allow them to connect and interact with other users.

This means when we say that a person with a single file has a number of links, we mean that the file of this person has or may have several number of electronic folder entries that allow them to interact with other people. These links help users by using different communication paths to information made available to be shared by a social network provider. The level of sharing is controlled by the access permissions on these files. Access permissions could be classified under “read or write only and execute”.

Implications of sharing

Sharing on social networks has enormous benefits to sharers as well as receivers. The value of any asset increases in value when it is shared. By increasing in value we mean getting many online users to acknowledge receipt of the shared information, there is an inherent multiplicity and a ripple effect of the information shared. This is applicable to sharing photos, play scripts, music and personal moments captured through writing, music or video. Notwithstanding these benefits, there are also negative consequences if the wrong item is shared on these platforms. These may be due to political or legal effects.

The nature of file sharing strategies on social networks platforms undoubtedly enables group communications. This facility comes along with a number of opportunities as well as risks and threats which when not managed effectively may lead to violations of privacy and confidentiality of individuals and the systems that drive them. Although these platforms have vulnerabilities and may experience potential threats, there is an overriding factor that seem to over rule or take precedence over any security threat or risks among these systems. The overriding factor is recreation or entertainment. Identity theft may lead to misrepresentation of users. This may be achieved through tagging or brain washing of the user.

The incident at Ramu in Bangledesh, some one got tagged with a photo on his facebook page, an example of misdirection and identity theft. This led to misrepresentation of the true image of the Prophet Mohammad, unfortunately since the boy was a Buddhist, he was thought and considered to be anti Muslim activist. This regrettably led to acts that destroyed Buddhist temples, houses and assault on any persons found to be associated with the Buddhist faith. This tragic incident could have been avoided provided that effective anti spoofing and identity theft strategies and controls were put in place.

There have been bullying and harassment case brought forward in the form of complaints to Twitter by many women including those in public office in the United Kingdom. These have caused members of the public office as well as parents sometimes in distress.

Mitigating with Intelligence

Intelligence is a product and a process that can be exploited for a variety of purposes. The objective of building or creating intelligence is to enable policy makers to formulate the right policies in organisations with the view of protecting their interest or pursuing a more strategic goal. It also enables executives to operate in a manner that protects the interests of the organisation as well as exploit new opportunities, which could facilitate processes that lead to accomplishing strategic corporate goals. Intelligence can be used in marketing, security, defence and business analysis, as such as important element of networking with people.

Connecting People

A profile analysis among young people shows that a vast majority of them are not aware of the extent of the dangers and risks on the Internet. Generally most young people that use online social networks fall within the age group 14 to 19 years old. The main networks comprise Snapchat, Instagram, and Clash Royale a game platform for younger children. A great way to be in contact with people they have lost contact with, as well as expand their current connections. The activities among teenagers and younger adults could comprise, profile viewing, listening to music and sharing contents among close friendship groups. Kids communicate to people they usually know or have known through a friend or a friendship group.

On the contrary adults tend to use Whatsapp, facebook and twitter for social or business reasons. Single Mums also use this as a means of talking to people, dating and building new relationships. It can be an effective way of introducing yourself to people. For instance new undergraduates use this medium as a way of introducing themselves to peers. Parents are less likely to comment on their child's profile. The main concerns online generally include bullying, leaving privacy settings open and sharing photos that could damage people's reputation. There is significant level of lack of awareness and understanding of how profiles could be exploited.

This is due to the low level of confidence in the ability to manage the settings on these platforms. This leads to the voluntary display of personal information.

It is however fair to state that although young people in most cases disregard safety and security concerns, they are still aware of some of the risks associated with online activities, however due to the fact that the benefits outweighs the risks less attention is paid to such issues.

Reconfiguring Access and Building Relationships

The primary role of the Internet is to reconfigure how we access information and do things such as getting to know people, understand their behaviour and how we can leverage this behaviour as part of developing useful relationships as cyber beings. Many people also use the social networks to kindle new relationships or rekindles past ones according to William Dutton, Professor at the Oxford Internet Institute. People usually meet on online dating sites, chat rooms and instant messaging platforms to facilitate this aspiration. Online dating sites have been prolific in the last decade in the UK and other parts of the world. For instance a couple that meet online are likely to have similar interest. A group of university students with similar interests will usually form online associations to further this interest, with the view of building stronger relationships to advance that group's programme. Many commercial opportunities can be created online, with very low capital. The barrier to entry in a business sense is very low for emerging entrepreneurs. There are however issues such as identity theft, bullying, exploitation of innocent people that requires effective response and strategy for mitigating these threats. A number of these tools have been discussed in chapter 6.

Summary of chapter 2

Chapter 2 presented an overview of information sharing concepts and techniques underpinning social networks. It also discussed the benefits, fears and implications of sharing data and files on social networks. Recent case of bullying on Twitter was also highlighted. Whiles chapter 3 reviews the economic freedoms that accompanies our access to cyber systems, chapter 6 further assesses the role and impact of cyber platforms on terrorism and how best these systems are used for building intelligence essential in protecting critical infrastructure.

Chapter 3

Economic Freedoms

Economics is fundamentally about the demand and supply of goods and services and how individuals and nations device strategies to manage the complexity that underpin the distribution and management of scarce resources. This is executed and carried out within the context of natural law, thus with the assumptions that all things are equal. This section provides an analysis based on the principles that govern micro and macroeconomics.

Microeconomics is the study of decisions made by individuals regarding daily economic activities, whiles macroeconomics deals with the dynamism within an economy as a whole from a nation's economic activity and standing, usually relating to all entities in that nation, country or region Williams G (2003). Although there are general economic principles, theories and models that apply to other countries and nations, these economic principles do not answer the problems of every country. It will be wrong for any economist to think that way. This is because factors such as financial power, culture Adams (1999), government policy, law, state of technology and manpower indirectly affect the economic standing and strategy of a nation. These factors in most cases drive an economy. If the manpower that sustains the dynamisms of growth is poor the growth of that economy might not be sustainable in the long term.

There is a paradigm shift and new thinking globally that suggests that introduction of social networking platforms for economics of information security is being leveraged. Although previous works by the OECD emphasise on the digital gap as driven by the internet as the main platform and driver, its coverage have been too broad as such lost its lustre on certain emerging issues. Web 2.0 platforms driven by social networking software is the new captain of the Internet ship. This has been mainly due to the cheap and affordable access to a range of different technologies enabling us to do things that in the past could have been considered as unimaginable.

The level of ICT education among developing economies has also become affordable among high school and university students. The notion that developing economies are stifled of digital information is certainly not true in the current cyber age. The penetration rate has increased dramatically for both rural and urban dwellers through the use of mobile technology. This has brought unprecedented freedoms to people in these economies urging them towards the developed world. The accelerated growth and access to mobile technology has given plenty freedoms to people as a result of mobility enabled through mass and affordable communications.

Recent developments and politically driven events and uprising in the Arab world is a testimony to these freedoms through penetration, galvanised by the ascendant use of social networking tools such as Facebook, Twitter and Linkedin, in the Arab world. This has forced certain leaders regarded as dictators to be removed from power and governments in an unprecedented manner. The factors that influence how other people gain access to information on the Internet have changed radically.

The economics indicate that there is a steady growth towards equilibrium between information demand and supply across the globe. This stability and progress is gradually enabling elimination of the digital gap. Most scholars and researchers place undue emphasis on the fiscal state of nations as such theorises the gap on the basis of the macroeconomic level of these nations. This has changed since technology use and development among cyber citizens is more at the micro level.

Governments and large corporations are now playing a defensive league of the cyber world. This is synonymous to IBM's business model in the 60's to late 70's where the company's structure was over rigid and lacked flexibility. Until nations and large corporations realised this paradigm shift, they would be left behind in understanding strategies necessary for governing the cyber world. It is this lack of understanding among major stakeholders of the cyber world that is impacting on the security and safety of nations and homelands.

This book asserts that the state of an economy and an understanding of micro level management of emerging and advanced economies are central to homeland and national security as well as the freedoms citizens enjoy. Organisations such as the OECD has over emphasised on poor infrastructure for developing and emerging economies. This is not the case according to emerging trends. The new trend suggests that the digital gap is slowly being eliminated through mobility and virtualisation.

Cyber economics is about the demand and supply of information and how this phenomena influence the wellbeing of citizens. There is enormous supply and information on social networks and the Internet as a whole. This is also met with almost an equal demand of information via the same social networking platforms. Social network users are driving the cyber world and economy. The bandwagon syndrome is still at work. Cyber users and hawks follow information, assimilate and share information through social networking platforms freely. The idea of information haves and have not's may be disappearing since demand and supply is almost at equilibrium. This equilibrium in cyber economics is not proportional to the rate of equilibrium in security. Although the digital gap may be disappearing, the cyber security gap is still widening, this is the paradox in the economics of security.

Takemura(2012) examine the interrelationship between information security, economics and also explores how technology provides us with a number of questions that require answers. For instance does policy makers cut corners when information security is expensive or do so when it has the likelihood of been expensive or unaffordable". What do we do under such circumstance? Is it prudent to adopt a cheaper workable security model as an alternative? According to the research results, there is strong evidence of the relationship between the expected effects and managing counter measures of information sharing and education. Most people in the public are willing to share information voluntarily if they understood its relevance and value. Unfortunately this is not the case as public and end user awareness is poor by government and industry. This kind of information is withheld among stakeholders and most institutions. The outcome of the research also indicates that human resources and information sharing are important two factors critical to information security. Workers awareness of information security is different in attributes of organisations and associated countermeasures.

A decade and a half ago Gordon and Loeb (2002) also evaluated the factors that were likely to get the best outcomes from security investments. The authors argued that it is not every case where security vulnerability might lead to a monetary loss. The authors questioned whether a breach should necessarily lead to increase in investments. Their arguments were that if the information set available to a stakeholder such as belonging to the public or an institution then one can confidently argue that the information is invulnerable therefore it remains perfectly protected for any amount if security investment being considered for rollout.

Security Spending

In November 2016, the UK government announced a 1.9bn spending on cyber security. This initiative by the British Government was announced as part of its national security strategy. The proposed budget allocation forms part of a wider landscape of the Government's interest in cyber security, defence, aviation, large data analysis using analytics and intelligence building tools.

Gartner the IT research organisation also asserts that security spending will grow by 7.9% to reach 81.6 billion by the end of 2016. The research also shows that until 2020, the highest growth is expected to come from security testing, IT outsourcing and data loss prevention. This analysis is consistent with many leading research trends.

A recent SANS institute survey (Silkins, 2016), suggests that security spending should be a core component of an organisation's budget. The research attempts to answer what, why, how and where security spending should go within the organisation. Security spending is on the ascendency with much of the funding going to staff development, analytics and data security. Although these are all important areas for an organisation to thrive strategically with respect to its business goals, there is a lack of emphasis with regards to skills and facilities fundamental to cyber intelligence.

The key aspects of security spending include, the protection of sensitive data, regulatory compliance, reducing incidents and breaches. Other anticipated growth spending from 2016 onwards is likely to be made up of training of staff, e-discovery and digital forensics. Compliance and audit forms a strong basis for justifying security spending among most organisations. The top spending areas according SANS research were skills with respect to application security, compliance and data security. Technology spending according to SANS covered areas such as access control, authentication, advanced malware protection and endpoint protection. The fundamental questions that require answers are; how security budget is justified, allocated, spent and accounted for. It is clear that security spending should be essential to a company's business strategy.

Economic sanctions

Afghanistan and other countries in the Middle East have experienced extreme government opposition to ICT. This has been a major factor in limiting Internet access. Many Middle Eastern leaders view the Internet as a Western-based agent of moral and political subversion. As a result, many countries strictly enforce limits on Internet connectivity. Whereas Egypt and Jordan have been relatively progressive in building Internet connections, countries such as Saudi Arabia have shown more resistance to allowing widespread access to the Net. Internet access is very limited in Syria, and Libya and Iraq prohibit any kind of Internet access. Bahrain and Tunisia openly monitor Internet traffic, and the United Arab Emirates and Yemen use proxy servers that can prevent users from accessing "undesirable" sites. Iran allows access, but the extent of the traffic monitoring in that country is uncertain. Although Countries such as China and Indonesia have invested heavily in Internet of Things technologies, there are still unbroken barriers with regards to what information could be accessed by its citizens.

It could be argued that these models are effective as a country like China has been enterprising and forward looking in the last decade, however employed effective controls in managing what it deems as irresponsible use of technology. Recent public knowledge sensitive information made available by Mr. Snowden a United States National Security Agency contractor known to have leaked classified documents may suggest that there is no much difference between countries like China, United Kingdom or United States when it comes to spying on citizens through cyber strategies or infringing on the basic rights of its citizens.

Chapter 4

Opportunities

Current and emerging technologies have led to the creation of innovative solutions for small as well as large businesses. This has dramatically shifted the way modern businesses operate, consequently leading to new opportunities for individuals, entrepreneurs and organisations. The nature of entertainment has also changed in many ways. The Internet and mobility based devices have enabled SMEs to be innovative in leveraging existing market share as well as exploiting new ones to meet strategic and long term goals.

Life without the Internet in the developed world will certainly be considered stifling and to the developing world a less adventurous world. This is due to the fact that almost 95% of home, work and social activities are carried out via the Internet and mobility enabled devices using strategies derived from the concept of "Internet of Things". This could range from working from home also known as teleworking, paying bills online, regulating the heating and temperature system and using washing machines and dishwashers at home. New businesses have been setup and resourced with less capital and infrastructure using lean models, however leading to high level of profitability and revenues, spiralling to the creation of new wealth. Other emerging technologies comprise driverless cars, unmanned vehicles, drones and aeroplanes deployed for security and defence operations.

Payment and Money Transfer Systems

This section describes the payment and money transfer systems that drive the freedom economy and how they enable secure funds transfer among individuals and businesses across the globe. These systems and technologies have given enormous freedoms and opportunities to people across different countries enabling them to play active roles take in cyber citizenship through use of payment systems and technology. Payment systems are designed to capture funds transfer from source to destination, authorise the funds and debit or credit a customer's account in real time. This real time phenomenon creates the efficiency and effectiveness required for a business to function successfully.

Certain payment systems are set up to authorise and not to debit or credit an account in real time, they do not necessarily authenticate a transaction, but rather enable payments between customers and merchants. Their primary function is to authorise a transaction received by a terminal. Examples of payment systems and gateways that have enhanced business operations and transactions include, PayPal, 2checkout, CyberSource, HSBC, BT SecPay, DataCash, WireCard, World Pay, eWay, FastCharge, Internet Secure, Secure Hosting Williams G(2007).

Payment systems and gateways generally use encryption software to secure money transferred online. Payment systems do not change how consumers and banks communicate or conduct a transaction. They only serve as man in the middle in online transactions. People use payment systems as a channel for communication and completing online transactions. A fee is usually charged for this online service.

Systems such as Paypal make money from transactions that go through its hub or tunnel; this is accrued in the form of an interest. There is a buffer or holding state of financial details of the buyer as well as the seller. These are trails that could be audited periodically for exceptional control purposes or as part of standards, regulatory or legal requirements.

Customer details such as credit and debit card numbers, bank account numbers and home or personal addresses are sources of information that link citizens to the wider cyber world. Some payment systems enable direct transfer of funds from buyer to seller. It is however vital to note that, their operations are based on different models.

A key security feature adopted by most payment systems and web services is the "Gausebeck Levchin" test. This technique forces account holders to type in a word found in a small image file on a web page when creating a new account. The technique prevents local or remote execution of scripts that comprise a text. It is suggested that only humans could read the text on websites if the technique is adopted Williams GB (2007).

Payment technology is essential to electronic and mobile commerce. Technology Gadgets and artefacts that drive such payments comprise credit cards, telephone and the Internet. Underlying these end user and frontline facilities are SSL, SET, and IPSEC that serve as security systems for securing transactions. These security technologies are central to the success of cyber payments. The other forms of cyber payment systems mentioned include digital cash, electronic checks, debit cards, smart cards, store and loyalty cards, prepaid and micro payments money transfer systems.

SET, a standard drawn from contributions made from VISA and Master card. Three security protocols deployed as part of the TCP/IP protocol suite. These are IPsec, SSL and SET. IPsec is implemented at the network layer. Although contents are usually protected, there are issues with traceability of source and destination data. This could be a form of vulnerability. IPsec can also encrypt a standard message and subsequently place this message in a disguised header. This technique is known as tunnel mode. This permits users to set up private groups over networks, usually in the form of VPNs (Virtual Private Networks). There are also difficulties in authenticating individual users, since IP addresses could be shared on a network.

Even though SSL has its strengths, recent developments reveal key vulnerabilities. This is because it provides only transport level security. Most security vulnerabilities originate from the network layer. Also see Synchronizing E-Security for more information on vulnerability spots on networks Williams GB (2003). This might serve as a loophole if there is no robust security at the network layer.

SET is also described as a standard that relies more on digital certificates. Certificates sometimes have trust issues with them. Robustness is a key strength however has performance related problems. When it comes to SSL there is a lack of mutual authentication critical to security of electronic commerce transactions.

PSP (Payment Service Providers) have challenges that must be conquered in micro payment systems. The operational models of these systems are not always transparent. In a cyber payment environment one may need to understand how the various transactions between a merchant, customer and PSP take place. The major categories of cost are also not clear when it comes to PSP. The information is necessary because it enables traceability and auditing of transactions, resolves disputes, charge backs, customer support, equipment, processing and communication cost, bookkeeping, point of sale and management of credit risk needs critical evaluation.

It is emphatic that most discussions and research published or unpublished have mainly emphasised on the security aspects of electronic transactions and not to the extent which such transactions and cyber payments affect homeland security. The one strap approach usually adopted by governments to identify a suspected terrorist group account and freeze it, is perceived as short cut, and fails to address the underlying and fundamental factors that facilitate cyber terrorism. This approach does not also expose communications associated with organised groups involved in cyber payments that may be linked to terrorism or fraud. Mobile payments and wireless systems fall within current and the on-going technological trends in academia and industry. This was also predicted over a decade ago by Keen and Mackintosh (2001).

The role of software agents in modern payment systems cannot be understated. Software agents literally perform useful services on behalf of citizens of the cyber world who browse and conduct business in both a friendly as well as a hostile environment. Cyber citizens use tools such as search engines and social network platforms to interact and communicate across to individuals and groups alike. Efficient and intelligent techniques in data search and retrieval tailored to customers and client needs are adopted in these instances (Arnolds S, 2008).

There are many categories of commercial activities driven by the Cyber world comprising B2B, B2C and B2G. These usually make up a significant form of cyber payment transactions. However the exponential growth of users of social networking platforms seems to have outpaced such commercial activities. There is some exponential growth in interest with regards to mobile communication that need considerable attention, especially the commercial activities it drives, which remains on the ascendancy as a result of fourth generation mobile networks (4G).

Mobile communication, social network platforms, B2B, B2C and B2G are all competing drivers of the mobile economy in an age of cyber citizenship. There is significance place on the common algorithms applied in business and cyber world to ensure the security and traceability of both financial and social interactions.

This intricacy is relevant for understanding the issues associated with confidentiality and integrity of data that traverse across networks that support electronic commerce and business. Algorithms such as DES, 3DES, AES, RSA, Diffie-Hellman public key distribution scheme, ECC, HCC form the basis of the security of cyber payments. These form a caucus of technologies required for ensuring privacy and protection of data. There is also the need to further explore the subject of authentication.

Citizens of the cyber world may need to understand how processes that drives these technological systems, without worrying about the underlying technology. Basic concepts and principles such as confidentiality, integrity, availability, nonrepudiation, authentication and auditing of third party systems should be understood. According to Zhang and Wang (2008) the history and background of the science and art of cryptography dates back as far as 1900 BC in the days of circa, where it was mainly used for military purposes.

Trust is also an essential component of cyber payment systems, access control and corporate security. Recent developments and end user needs also show that it also ensures some level of integrity, although that was not the original purpose of the science and art. Attackers of cyber platforms usually embark techniques such as plaintext attacks known as man in the middle attack. This may be a correlation or corroborated attack against hardware. Emerging techniques emphasise on quantum computing, a research area related to polynomials and discrete logarithms, DNA computing with highlights on limitations in real world. Other algorithms such as hash functions, SHA-1, and MD5 should be further explored especially when complemented with random number generators.

PKI or the publishing of public key cryptographs is an effective system that combines software, encryption technologies and services that enable enterprises to protect communication infrastructure, business forecasting and the Internet. PKI uses a holistic approach by integrating digital certificates, public key crypto graph, certification, enterprise wide area network architecture. This is cherished from a theoretical point of view. There is however problems associated with certification authorities and bodies, which sometimes cause the foundations of PKI to shake, as a result of excessive structuring of processes. There are issues related to trust, law and inconsistencies with existing regulatory frameworks that require further analysis and consideration.

Biometric systems are gaining prominence in the cyber world. Although there is reasonable evidence to suggest that biometric is growing in popularity, there is also scepticism with regards to its effectiveness within industry and the research community. Biometrics a security paradigm based on the study of physiological and behavioural characteristics of a person is yet to be implemented widely across the financial world.

It is assumed that the vivid pictorial representation of the physical features usually captured for deploying biometric security systems ensure a high level security. Although this assertion may be true, it is also highly debatable, due to the scepticism associated to its accuracy and the associated probable error. Attributes such as finger-scan, hand scan, hand geometry, retina scan, iris scan, facial scan, facial geometry, signature scan, dynamic signature verification, voice scan, or speaker verification are essential however may be considered not critical to the security of cyber payment systems.

The technology however may be usefully applied in areas such as physical access to buildings (physical access control), authenticating of exclusive financial transactions such as withdrawal of gold or large deposits. For instance finger printing is seen as a means of improving online banking transactions and fraud protection. It is also perceived as a method that boosts confidence amongst customers. Scanning technology also need adequate lighting to improve the data set required to be stored in a database for drawing probabilities required for estimating accuracy.

Smart card technology although another credible means of providing secured financial payment its operating systems are not as robust as that of the operating systems supporting desktops. The usefulness of these cards is that they serve as a rich source of security intelligence for homeland security.

Smart cards such as Octopus smart card in the transport system in Hong Kong introduced almost 16 years ago and the Oyster transport card introduced a few years back for Londoners are examples of this technology. These cards serve as useful sources of information for homeland security provided the appropriate analytics tools are employed to classify and interpret datasets.

Wireless technology provides useful and relevant information on the communication systems that support the cyber infrastructure. This information may relate to IP numbers for routers, PCs, port numbers and MAC (Media Access Control) addresses. Other useful information such as addresses on data packets showing sources and destinations of data on networks can be used for counterintelligence operations. Wireless technology could support a wide range of applications including local area networks for corporate buildings, customer service applications and email services. For readers and researchers interested in scripting languages that drive these systems, the C languages is effective for deploying all kinds of network communications.

Agents serve as tools for making payments on behalf of clients. They however migration and mobility challenges and safety threats on communication networks if not robustly protected. Agents serve as an excellent foundation for developers who want to branch into mobile application development with intelligent capabilities and functions. There is a differential analysis of the agents that facilitate transactions, and mobile agents who migrate autonomously from one computer network to another. The main phases of a secured payment protocol is also essential in agent communications on networks. Common functions of software agents are withdrawal, distribution, payment, verification and transfer phases on financial platforms and systems. The importance of agents with respect to digital evidence is further discussed in chapter 4.

Digital cash, fair digital and Brand's digital cash all consist of four phases, thus opening an account withdrawal payment and deposit. The last decade have seen the reporting of security issues raised by ordinary citizens and law enforcement agencies alike. It sometimes serves as a haven for criminal activities due to the nature of the system and accompanied policy for processing transactions. This system makes large Scale deployment a nightmare. This is form part of issues that throw lots of challenges to security auditors, and researchers with keen interest in information systems auditing. There is clear notational representation of concepts for the setup, the process of opening an account, the withdrawal protocol, payment protocol and the deposit protocol. This chapter is appropriate for developers who want to explore the different digital schemes, design concepts and associated protocols. It is also suitable for final year undergraduate students and postgraduate students alike. Concerning digital checks, there is emphasis on authentication processes.

ATM footprints are captured when a consumer enters their personal identification number (PIN) at an Automatic Teller Machine (ATM), the PIN is verified for authenticity, followed by authorisation of the financial transaction. The implication is that a consumer leaves a digital footprint on the account after carrying out the said transaction.

The digital footprint of the consumer as a result of the electronic fund transfer may show a balance transfer to another account, payment of a bill, printing of a statement or the balance on that account.

These tasks and digital interactions by a consumer comprise some of the frequent tasks performed on an ATM. The financial statement may reflect movement of funds indicating sources and destinations of the transfer. This may be reconciled with other accounts held by the consumer or by associated beneficiaries.

Most banks provide ATM facilities to their customers on different communication networks, regardless of the customer's geographical location with the VISA being an example of such a network. Customers whose banks and financial service providers belong to this network could use the facility anywhere. This comes along with a number of distributed communication challenges, such as synchronisation of data and processes across these communication networks. This sometimes has security implications. A poorly synchronised network is a ladder and an escape route for electronic criminals. These criminals may not be as simplistic perceived on the face value. They may also have terrorist links. Although electronic intelligence services such as the GCHQ and SOCA agencies may be capable of analysing the interrelationships of such transactions and communications the disincentive and downside of this is that a longer time could be taken to build a full picture of what might be taking place. Their operations might also be frustrated by geographical boundaries as a result of jurisdictions.

The reader may carry out a personal experiment. Withdraw funds from any ATM, display or print your balance. Repeat the task of printing the balance at another service provider's ATM you may notice that the balances at both ATMs are not quite the same. This is an indication of a poorly synchronised system that has security implications.

Electronic Point of Sale (EPOS) footprints

A customer usually enters transaction details to a checkout machine or swipes a debit or credit card after items have been selected and scanned for purchase. The Personal Identification Number (PIN) of the customer is verified. At this stage it is the PIN which is verified for authenticity and not the consumer or customer. Authorisation is then granted to the consumer. The consumer's account is then debited or deducted, followed by a reconciliation of the consumer's account via the service provider's third party's payment system such as a bank or PayPAL.

Banking footprints

A consumer or customer usually provides a security code to a Bank's Customer Service Personnel. The code is verified and authenticated. The transaction requested by the consumer is authorised. The transaction is confirmed while the consumer's account is reconciled. Some of the security problems associated with telephone banking include the lack of encryption facility on most home telephones, eavesdropping by third parties, diversion and interception to fraudulent providers.

The use of debit or credit card on the internet, telephone, mobile devices such as dongles or through any other data transfer device forms the basis of the incubation of the cyber citizen built from digital footprints. This sets the boundaries for defining cyber citizenship. Personal details captured during an electronic transaction are verified for authenticity. For instance a payment system may authorise as well as authenticate a cardholder. The card holder's personal bank or card details could be associated with databases of service providers accessible by public agencies for homeland security purposes as prescribed by law.

Contactless Payments

Contactless payments are generally used to make petty payments from electronic cards. These payments are usually carried out using cash. Although designed to facilitate small payments, the technology and its implementation comes with its own security risks. There are key questions that need answers, such as; What happens when the authorised limit for payment is altered? How do we authenticate a user? How secure is the contactless access point from a user's perspective? Clearly there are not yet satisfactory answers to these questions.

Summary of Chapter 4

This chapter discussed security technologies and processes usually put in place to enable secure online payments. One of such technologies is SET, a standard designed by VISA to support all transactions carried out on its network. Although these systems are designed to provide high level of security, users are in a better and stronger position if they receive the appropriate guidance from service providers to assist them in understanding the best way to secure personal data and resource. Security spending trends were also discussed among governments and corporations. Technology also played a vital role in addressing sanctions and exploiting strategies required in doing so. The freedoms and opportunities that we have with respect to the applications of cyber technology to social networking and business also comes with the understanding of our rights and obligations. The next chapter discusses the role of governance and the rights of citizens.

Chapter 5

Governance and Rights of Citizens

This section examines governance, freedoms and rights of the cyber citizen in the context of the law and legal requirements that affect cyber activities internationally. The author makes specific reference to Internet law and legal requirements in respect of homeland security and intelligence activities. Some of the laws covered in the chapter includes, Fraud and Abuse Act of 1986, Computer Misuse Act of 1990, Copyright, Electronic Communication Privacy Act 2000 and the data protection Act of UK 2000, the patriot act after 9/11 in 2001 in the United States. Email and Privacy Laws usually covering email policy, email privacy, monitoring employees, Right of Privacy in Online applications, Crypto-systems, Online Games and Gambling, and most importantly the Telephone consumer Act of 1991. Refer to details of the laws in appendix 1.

The global reach of the Internet and prolific growth of social networking platforms have changed the face and nature of Internet activities. This emergence does not only accelerate business activities, it has also accentuated the manner in which people of all nations and countries interact and share information for business purposes as well as for entertainment. This has enabled communication and organisation of social events beyond geographical boundaries and traditional business channels.

The rapid deployment of commercial web activities and sites globally shows the importance of this cost-effective possibility for businesses to present themselves in a global market place, Bernard Glasson et al (30, 31, and 34). In view of this new marketing and business age, using sophisticated technology in online business activities have become more complex than the years before. The law regulating the behaviour of individuals and businesses with the advent of advance technology in this regard is not as effective as one will expect it to be, within the broader context of international law.

Jurisdiction boundaries

Each time someone misuses a computer by either infecting a computer, with a virus or any sort of malware, is liable. On the other hand you have to look at the jurisdiction point of view. For instance, if someone is based in New York, and affects a computer in London, the person in New York could be prosecuted in the United States because of the jurisdiction boundaries…"

These Jurisdiction boundaries are not always clear and it is far from easy to delimit them precisely while browsing on the web. That's why James Bridle, who is a writer, artist and publisher based in London, created Citizen Ex.

Citizen Ex is a plug-in for web browsers that tracks your online behavior and finds where websites are legally registered. All this information is compiled thanks to the 'algorithmic citizenship' and then creates a flag to identify the jurisdictions under which you browse on the Internet.

Citizen Ex algorithm

The algorithm mostly browses the Internet under US laws. This causes discourse, as the US as a country has different laws and legal framework among its numerous states. You still have to know which law applies, if any, in theses different states or countries.

International Law

The simplest definition of international law believed ever defined is “a system of rules governing the relations between sovereign states”. Let us take a particular interest in the word sovereign or sovereignty Dixon M (306,138,276). According to the oxford dictionary, it means supremacy, self Government or a self Governing State. It is important for us to note that for the sovereignty of a state to be recognised in the purview of law, its jurisdiction must be clearly defined.
Jurisdiction is the extent of a nation’s legal or territorial authority. In other words where it can administer justice, play a crucial role in the contribution to information security management of Online Business. This is because globalisation of information transfer cuts across the boundaries of nations.

Limitations of Law

There are limits to what the law can do. Cyber activities are analogous to an ammunition depot that has no locks. The activities cannot be policed effectively as the set of processes that govern its functions cut across legal boundaries. Although there are indications of safety and security issues that impact on homelands, it is not simplistic to arrest people when the crime committed is outside one’s jurisdiction. The nature of networks is turning a number of western countries such as the US and Britain into virtual police states. Interestingly policing is not only carried out by State but also through investigative journalism as a result of public interest.

Although some part of the law empowers nations to arrest and prosecute individuals who might have committed a crime against any of its institutions, this only works where the criminal's country of origin or citizenship cooperates in the arrest and prosecution. It must be noted that this aspect of the law mostly applies exclusively outside the scope of information technology, due to the fact that laws covering computer crime needs further development and enforcement globally. In order for us to get a better picture concerning this aspect of the law, let us examine the Harvard research convention on jurisdiction with respect to crime (1935). "A state has jurisdiction with respect to any crime committed outside it's territory by an alien against the security, territorial integrity or political independence of that state, provided that the act or omission which constitutes the crime was not committed in exercise of a liberty guaranteed the alien by law of the place where it was committed".

Social order and the coexistence of states make it important for boundaries between their sovereignties and jurisdictions. This is because contradiction of every state's power is inevitably involved. The American law institute defines jurisdiction as "the capacity of a state under international law to prescribe or enforce a rule of law". The institute's definition draws attention to the distinction between a State's jurisdiction to prescribe and to enforce law. A state cannot enforce a law it has no right to prescribe. However a state may prescribe a law it may be unable to enforce. For instance if a criminal commits a crime and escapes into another states jurisdiction, and that state has no good international relations with state that the crime was committed against, the affected state has no right to extend it's judicial powers in that State Levi W(107).

Poor international relations grossly contribute to the ineffectiveness of the law. It is a real unforeseen menace that lies ahead in the new Cyber World. Within the context of enforcement of the law consumers of products of information technology and cyber services have obligations that must be observed.

Consumer's obligations

There are independent organisations that provide advice to consumers with respect to these Acts. These organisations include; The Online Privacy Alliance, (AUCE) European coalition for unsolicited emails, Crypto Law Society and Australian Privacy Foundation. Section 1.6 presents the Electronic Communication Privacy Act as applied in the USA. This is designed to provide relevant information regarding the legal implications in case of violation or an incident of abuse with respect to privacy in places where similar Acts of Law exist. You may skip this section if you are already familiar with this particular Act.

Privacy and the Law

Although society abhors fraud and accepts that it is wrong and should be prevented. The methods that are used to detect or prevent fraud sometimes conflict with the law and also violate the right of the individual's privacy. This section examines certain factors that restrain the effective application of methods developed and devised to detect or prevent crime. **Privacy** is one of such factors. A method such as data marching of personal records compiled for unrelated purposes actually violates the data processing act 1984 that have subsequently been reviewed since 1992, 1998 and 2000. Despite that this is supported by the Act, end users have the right to control personal information and prevent its use without consent for purposes unrelated to those for which it was collected. **The way the law is applied** could also make it difficult for an individual not to be notified in a particular situation where data protection is likely to be violated.

There is a conflict between notifying the individual and maintaining the integrity of any on going investigation. The person's right for justice in most instances could be curtailed. Although it might affect the course of the investigation, apprehending or arresting people on the grounds of data marching on possibly an insecure computer system mounted somewhere is wrong in any form of natural justice. This understanding of a basic freedom and right is not limited to computer nerds, but clearly understood by ordinary citizens who use and share vast amount of information on a daily basis. This line of action is certainly seen as a humiliation and a miscarriage of justice in any form. Any improvement in the security management of information may require a power balance to reflect the needs of that particular environment. Internal controls must be highly improved and co-ordinated through all banking institutions. Companies are marketing their products at the expense of information security; in view of this, Government must review policies that control the operations of businesses.

Regulating Businesses

The role of regulatory frameworks has become an important aspect of modern business. This forms part of the running of any business, whether small or large. The nature of a business is likely to dictate what sought of regulatory framework should be adopted. Cyber Technology has become an important aspect of running a business and addressing the operational framework necessary to support the day to day running of that business.

The use of cyber platforms in business operations is an evolving phenomenon according to (Piper J 2016). Historically computers have served as tools for supporting main line business operations, whiles on the contrary it has been used more as the main driving force among businesses in recent times working towards strategic goals in organizations.

One of the fundamental strategies of running a business, is the ability to develop know how from existing experience and skills. Some of the skills required for running a modern business, form an essential aspect of making a business successful.

Summary of Chapter 5

This chapter highlighted the importance of governance, international law, right of citizens, associated freedoms and the balance between the law, its enforcement and personal responsibilities. Internet law was also discussed with respect to limitations and issues regarding privacy. Chapter 6 describes and reviews some common attacks and strategies on cyber systems and what end users and organisations should be aware of.

Chapter 6

Attacks

This chapter discusses common cyberattack methods and strategies used for exploiting and compromising infrastructure designed to support homeland and national security. The methods of attack may include a wide range of common techniques derived from penetration testing strategies, usually adopted to facilitate vulnerability investigations or expose risk access spots on electronic based and online systems. The methods of attack may be classified as soft and hard. Soft methods focus on social engineering strategies, whiles hard methods relate more to technology led strategies.

Soft Methods?

Hard Methods

Hard methods are attacks on online platforms, Service Access Points (SAP), Routing Table & IP address systems for domestic and corporate networks, Ports and Port number, MAC address, Server, User Profiles, encrypted messages, operating Systems. The defence and management strategies for handling these attacks on online systems have been presented in the subsequent sections.

The attacks have been classified into methods and software tools. The methods of attacks cover the us of Brute Force, Masquerading, Traffic Analysis, Profiling, Scavenging, Roaming and Scouting, Spoofing (Web, DNS, IP), Stealth Attacks, Denial of Service (DOS) (SYN Flood, Smurf, TCP ACK Flooding etc), Distributed Denial of Service (DDOS), Malware propagation (Worms, Viruses, Bots, Spyware) Man in the Middle, Replay, TCP Session Hijacking, ARP (Address Resolution Protocol) pollution, IP Fragmentation, Replay, TCP Session Hijacking, Password conjecture and guesswork, Backdoor, Mobile codes and electronic bombs, Ping, Permutation Analysis, Software tools and utility computer programs used by hackers to exploit vulnerabilities on these networks.

Denial of Service (DOS) and Distributed DOS attack

Service request of applications are usually made via ports on the host computer of a Service Provider. For example, most web services are provided via port 80. Vulnerability could lie within the program code of the application providing the service, which can be exploited by a remote user attempting to look for a service. This section illustrates the process of launching a DOS or DDOS attack by disrupting the services provided by an application using a port as its communication channel. Buffer overflows could be a risk access spot that could be generated by corrupting the source or executable code of the application. An attacker could dump several lines of code in different syntax or programming language as a way of disrupting the functionality of the application. An application could also be exploited to consume system resources. An attacker could also compel an application to misbehave or malfunction. This is possible although ports are usually closed as a routine measure; applications do not have that form of self defence. This is common to most applications. A client or user that aims to attack using a DOS attack could sometimes succeed by simply sending several ping messages or request to a server, making it unable to cope eventually.

SYN Flooding

This is a form of attack that is usually launched during TCP client server interaction. A client or user makes a request to a server, for a service such as video streaming or directory search. This is preceded by a TCP handshake in the form of TCP SYN and ACK packet exchange. Below is a flowchart and diagram illustrating this process.

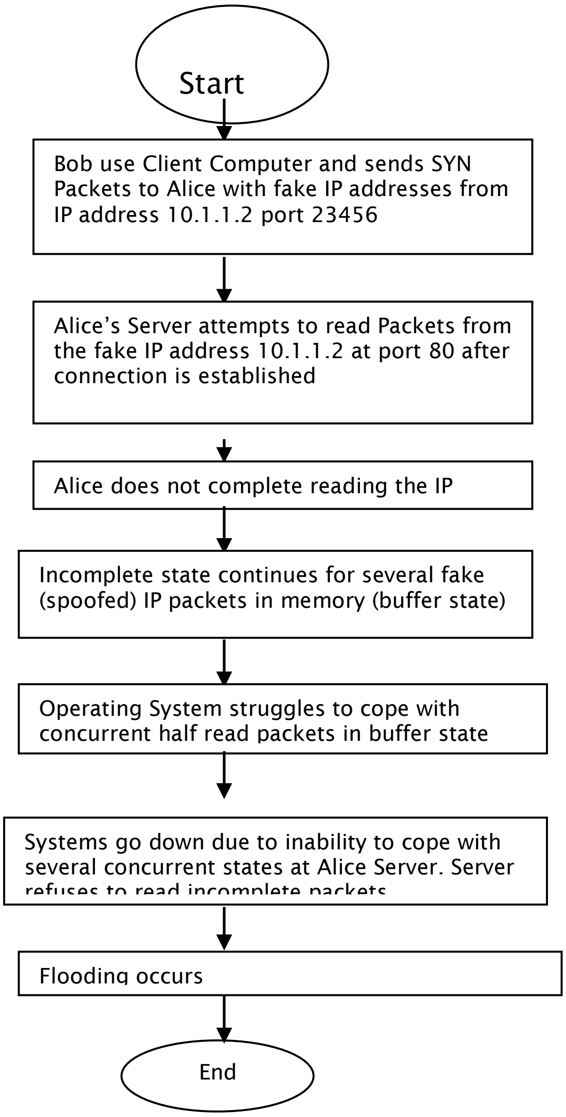

Start
Bob use Client Computer and sends SYN Packets to Alice with fake IP addresses from IP address 10.1.1.2 port 23456
Alice's Server attempts to read Packets from the fake IP address 10.1.1.2 at port 80 after connection is established
Alice does not complete reading the IP
Incomplete state continues for several fake (spoofed) IP packets in memory (buffer state)
Operating System struggles to cope with concurrent half read packets in buffer state
Systems go down due to inability to cope with several concurrent states at Alice Server. Server refuses to read incomplete packets
Flooding occurs
End

Figure 12 – Flowchart showing the process of interaction of SYN flooding

Description of figure 12 simulating SYN Flooding Attack

Figure 12 is a simulated flowchart illustrating how a client machine could launch a denial of service attack via SYN Flooding. In this attack there are two persons involved. They are Bob and Alice. Bob use Client Computer and sends SYN Packets to Alice with fake IP addresses from IP address 10.1.1.2 port 23456. Alice's Server attempts to read Packets from the fake IP address 10.1.1.2 at port 80 after connection is established. Alice "reads" but does not complete the process of reading the IP addresses sent by Bob. The incomplete state continues for spoofed (fake) IP packets in memory (buffer state). Operating System struggles to cope with concurrent half read packets (data) in buffer state. The system fails and becomes intolerant due to inability to cope with several concurrent states at Alice's Server machine. The server refuses to read incomplete packets. Flooding occurs resulting to a Denial of Service (DOS) attack.

SYN vulnerability is primarily revealed during the establishment of a connection between a client and server using TCP. The SYN and ACK 3 way exchange could be blocked or made unsuccessful when a client's IP address is spoofed, a terminology used to represent a form of deception or counterfeit service request made by a client. This compels the server to be in an indefinite response loop in an attempt to send an ACK to the genuine client that established the handshake with the server. This misdirection indicates a successful spoofing strategy resulting in a DOS attack.

6.1.3 Simulated Attack

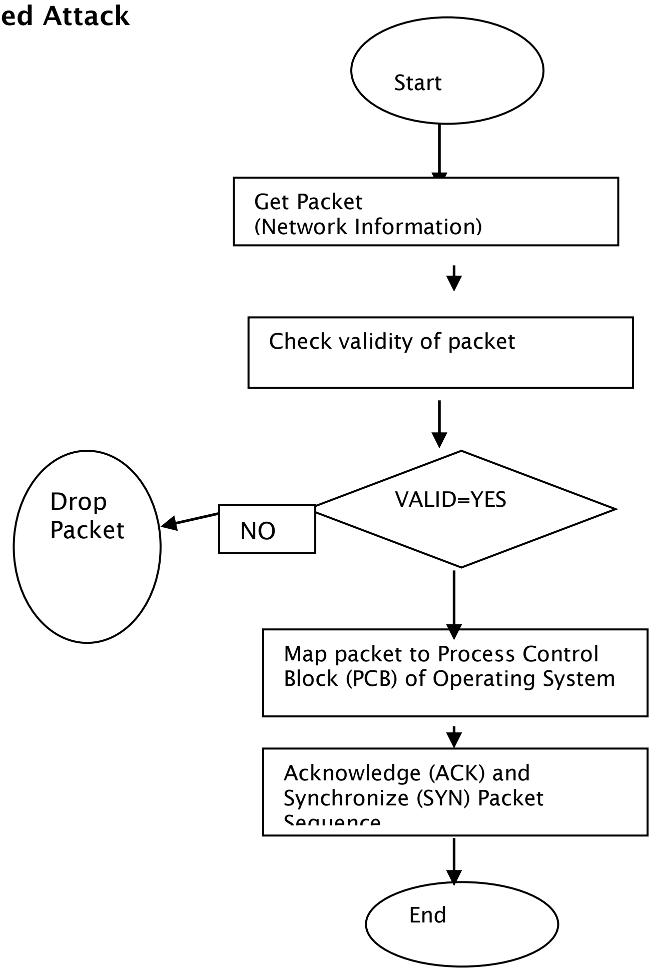


Figure 13– Flowchart showing the process of interaction of ACK Flooding

Description of Figure 13

The attack starts with a packet sent to a network node through a network or socket address using a “ping” command. The packet is checked for credibility by verifying the IP address. If the packet is valid it is likely to be left through to the network node under attack. This is sent to the process control block (PCB). The PCB is that part of the operating system responsible for scheduling data being processed. .

Attacks on Service Providers

A hostname is the name allocated to a computer that provides services to other computers. It can also represent a user's computer that serves other computers. For example a home computer can serve as a local host when it provides remote services to other computers on a public network such as the Internet. It can also be referred to as the computer that serves users usually called the server.

Displaying network information and hostnames from a Linux system using "Ifconfig" command:

Ifconfig

- $: Ifconfig – Command views the IP address and other information about hosts's interface to the network.

    - Eg: ifconfig –a

Comments: The above command leads to the results below:

- 1o0: flags=849<UP, LOOPBACK, RUNNING, MULTICAST> mtu 8232

```
    inet 127.0.0.1 netmask ff000000
    1e0: flags=863<UP BROADAST, NOTRALLERS, RUNNING,
MLTICAST >mtu 1500
   inet 192.102.10.89 netmask ffffff00 broadcast 192.102.10.255
```

NB: 127:0.0.1 is destination address for (local host), whereas 192.102.10.89 is your host's actual IP address, by which it is known to the outside world

NB: The "Ifconfig" is usually located at /sbin directory on UNIX operating system platform. The "ifconfig" command and utility is used by the systems manager to modify the configuration of a network interface. Network managers usually use that for allocating an address to a network interface during configuration. Given this network information an attacker can use it to change the network interface address from local and remote positions. The command can also be used to manipulate the DHCP (Dynamic Host Configuration Protocol). DHCP is a protocol for automatically assigning IP addresses to network devices. It keeps track of both static and dynamic IP addresses. This means that intervention of its function with "ifconfig" command is likely to destabilize its role of dynamic address allocation.
This command can be executed remotely using a script written in Java or Visual Basic.

Attacking Servers

Displaying domain names and IP addresses of the hosts on your network using “cat /etc/hosts” command.

The “hosts” file is a local database for matching hosts and internet protocol addresses. Another database for holding addresses of domains and resolving names when clients make a request to a host known as DNS(Domain Naming Service) can be combined with the host file by an attacker to launch an attack that can terminated network functions. A host can have many IP addresses. The database of the host has the following format.

Host	IP-address	Hostname	Alias

Using “Finger” command

“Finger” command displays and captures information about a user’s computer on a network. The command can display information about a user on a specified host running the “finger” command. It can also provide information on the user you want information about on the specified computer host or server. Figure 15 is a screen dump of the “finger” command. The command “finger Godfried Williams” has displayed the user ids and details associated with other people with “Williams” as a last on the network. It has also showed the path that stores the user ids.

Password Attacks

Cain and Abel

It is a password recovery tool for Microsoft Operating Systems used by network administrators to test their system. Hackers exploit this tool for cracking encrypted passwords using dictionary attacks or crypt-analysis. The application of the tool can render systems vulnerable by taking advantage of weaknesses in protocols, cache memory and authentication granting systems. It has the capability of breaking into VoIP conversations, breaking open scrambled passwords as well as tracking the routes of IP packets on a network. On a positive note it can be used for digital investigation or computer forensics. More recent development of the tools enables users to poison router table information.

John the ripper

John the ripper is a password breaker effective on UNIX and Windows operating systems. The following command is based on a dictionary attack using a word list in a password file. The words listed in the dictionary covers a common set of words likely to be used for a password attack. John the Ripper comes with a number of command line options.

```
Session = name
Stdout =length
Status=name
```

The above option is sent through a UNIX pipe, which simply handles input output data. JRP comes with a utility for bruteforce attacks, which can crack encrypted passwords with OpenBSD, DES, MD5 and Blowfish. The command below is can detect a password weakness and attend to crack it.

```
# Godfried – wordlist = password.password.
```

Snort

Snort works as a packet analyser and sniffer. A packet sniifer is a program that reads packets of data in transmission on a network. Packets read may include passwords, credit and debit card details. The packets are in the form of plaintext. Remember that there are some password systems that do not encrypt. A packet sniffer can be installed on a network without permission from an administrator.

Mobile Codes

A mobile code is a code that can suspend execution on one system and migrate onto another to restart the execution. It is also a code that can be executed remotely to a victim's machine.

Design goal

It is primarily designed to optimise performance of distributed systems and networks. It can however be exploited for malicious gains. Examples of mobile code programming tools are Javascripts and ActiveX.

Architecture of a mobile code system

The simplest mobility system model comprises a program code, dynamic states or instances of the code and a code execution platform. The different types of attacks launched by mobile codes take the form of mobile code to mobile platform, mobile platform to mobile code or mobile code to mobile code attacks.

Architecture of malicious mobile code

Example 1 – Malicious message to *Godfried Williams*

```
# Message
<Script> malicious code </script>
#End of message
```

The code can be embedded as a malicious html tag intended for *Godfried Williams.*

Example 2 – Malicious web link

```
# Web link
<A HREF="http://Godfried.com/news.cgi?
   news = <script> malicious remote code </script>"> Please click
this for latest channel 1 news </A>
```

This could be launched as Phishing, Trojan or Worm attacks. Clicking this link can trigger remote execution of a code**.**

Worm and DOS (Denial of Service)

Worms use remote code execution by targeting buffer spaces in running programs as well as exploring vulnerabilities such as; 1. Format string errors due to human errors 2. Buffer overflows 3. Syntax and grammar violation due to missing arguments or wrong data type violation in system programs 4. Character mismanagement 5. Character mismanagement 6. Poor references to program variables and data types 7. Information gathered from a host on a network not intended to be distributed across the network 8. Multiple operation errors due to poor synchronization and poor handling of deadlocks in computer memory 9 A process that consumes more resource than other processes in memory.

It is also known as "asymmetric" resource consumption 10 Operating system configuration errors. Refer to chapter 5 for details on vulnerabilities.

Brute force

Dictionary attack for cracking password on computer systems or networks. It uses an exhaustive key search to crack a Ciphertext by referencing to a comprehensive dictionary. It is however computationally demanding.

Backdoors

Backdoors are used for gaining remote entry to networks. They are tools used by network administrators. Examples of such tools are Back Orifice, Subseven and Netbus. These tools can allow remote control and management of a computer.

Stealth – This attack exploits vulnerabilities on router tables and network information.

Phishing – A social intelligence tool deceiving users in Online Business. It adopts techniques such as profiling and identity theft. This type of attack capitalizes on human vulnerability RAS.

Summary

This section presented a pedagogical view of methods used by hackers and crackers to exploit risk access spots and network vulnerabilities in Online Business Systems. The attacks exploited on vulnerabilities such as transmission media (Wired and Wireless spectrum, Service Access Points (SAP), Routing Table & IP address, Port and Port number, MAC address, Server, User Profiles, Cyphertext and Crypto-systems and Operating Systems. The defence and management strategies for handling these attacks on a communication network supporting Online systems. The methods of attacks cover methods and tools such as Brute Force, Traffic Analysis using tools such as Snort, Profiling, Scavenging, Roaming and Scouting, Spoofing (Web, DNS, IP), Stealth Attacks, Denial of Service (DOS) (SYN Flood, Smurf, TCP ACK Flooding etc), Distributed Denial of Service (DDOS), Malware propagation (Worms, Viruses, Bots, Spyware), Man in the Middle, Replay, TCP Session Hijacking, ARP (Address Resolution Protocol) pollution, IP Fragmentation, Replay, TCP Session Hijacking, Password conjecture and guesswork, Backdoor, Ping, Permutation analysis and exhaustive key search. Software tools and utility computer programs used by hackers to exploit vulnerabilities were discussed. In chapter 7 we examine and discuss countermeasures that could be put in place to address the common attacks presented in chapter 6.

Chapter 7

Counter Measures

Counter measures are systems, strategies and models put in place to mitigate or respond to any cyber threats or attacks on an infrastructure. This chapter evaluates and discusses the application of security and risk models essential to responding and addressing the attacks discussed in chapter 6. These constitute a suite of counter measures necessary in mitigating threats and any potential attacks on critical infrastructure.

Risk Security Models (RSM) generally map out security and risk requirements in an information system or the process of developing such a system. It is also used to determine and simulate the behaviour of such systems, as a means of understanding details of changes, vulnerability and noise likely to occur when the system is functioning.

This chapter is an assessment of existing security risk models and how they compare and contrast with a more robust model known as SSTM (Service Server Transmission Model) discussed in chapter 8. The analysis covers common and widely deployed models such as CRAMM, OCTAVE, ASSET, JAVA SECURITY MODEL and HOLISTIC SECURITY and ISMM. These models constitute the tools that could be employed by corporations, SMEs, defence and security agencies for mitigating the cyber attacks discussed in the previous chapter.

OCTAVE

OCTAVE (Operationally Critically Threat, Asset and Vulnerability Evaluation is a method for evaluating security risk. Its proponents and advocates deem it to be comprehensive, systematic and context driven. In OCTAVE, confidentiality, integrity and availability are evaluated in conjunction with the IT infrastructure of the organisation under investigation. OCTAVE applies a three phase methodology. The phases are; Build Asset Based Threat Profiles, Identify Infrastructure Vulnerabilities and Develop Security Strategy and Plans.

Phase 1: This is an assessment of an organisation's key assets, threats associated with these assets and the security needs of the assets identified. The risk and security management team identifies strategies adopted by the organisation to secure its ICT infrastructure.

Phase 2: Build Asset – Based Threat Profiles - An organisation's ICT Infrastructure is assessed. An audit is performed to identify operational elements of the ICT infrastructure. This is based on the information gathered by compiling notes on existing infrastructure.

Phase 3: Develop Security Strategy and plans - A risk assessment is carried out at this phase. Infrastructure gathered from phase 1 and 2 are analysed to identify risks to the organisation, and subsequently assessed to determine the impact of risk to the organisation's mission or goals. A strategy for protecting and mitigating risk are developed.

Pictorial representation of OCTAVE

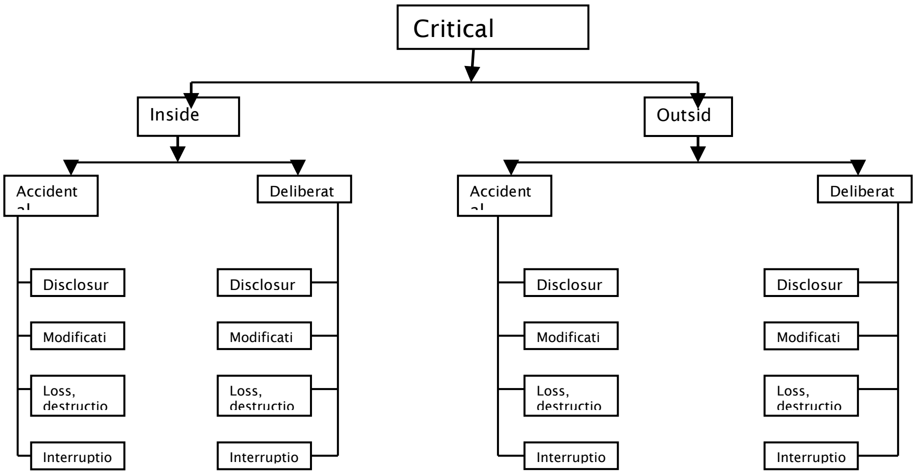


Figure 17 - Human actors using network access

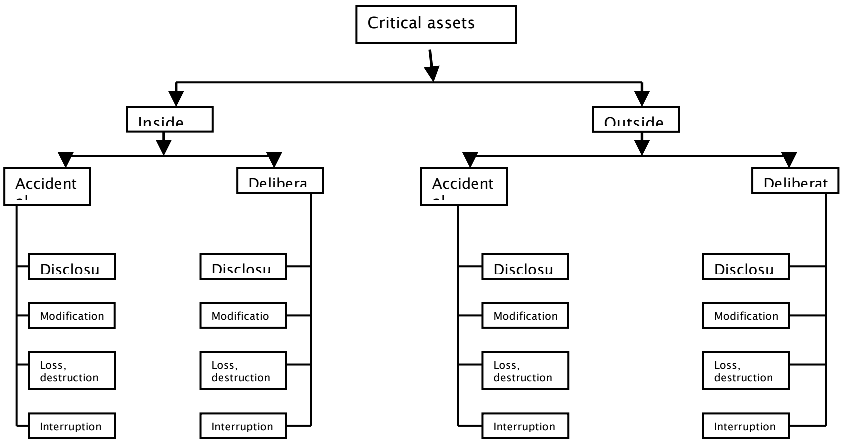


Figure 18 - Human actors using physical access

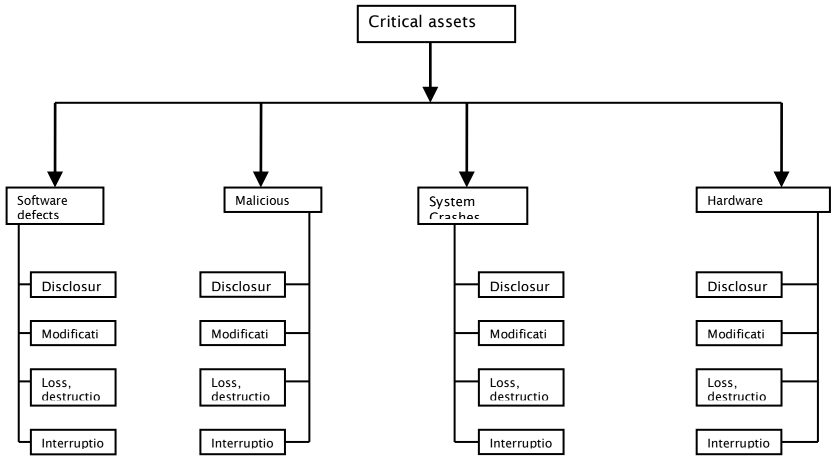


Figure 19- Systems Problems

7.1.2 OCTAVE & Threats

OCTAVE perceives or defines threat as an indication of a potential undesirable danger. An example is an attacker initiating a DOS (Denial of Service) attack against an organisation's file server.

Table 7 - Properties of threat in OCTAVE

Property	**Description**
Asset	Anything with a value in an organisation
Actor	Anything be it a person, an item or a process that can compromise the confidentiality, integrity and availability of an organisation.
Motive	An indication whether the actors actions were deliberate or accidental
Outcome	Effects or results of post confidentiality, integrity and availability violation.

The general threat profiles according to the developers could be customised to meet the needs of different organisations, by inserting and deleting threat based profiles not applicable to a particular organisation. Whiles some organisations might apply the standard threat profiles, others may choose to tailor it to their security needs and requirements.

7.1.3 Threat Profiles

Workshops and seminars are conducted with the particular organisation's employees. This is done to elicit information requirements associated with the threats that could compromise the confidentiality, integrity and availability of that organisation. This information is used to create threat profiles for critical assets of the organisation's systems and information assets.

Different scenarios are built based on the areas of concern highlighted by employees at operational, tactical and strategic levels of the organisation. The main objective of the workshops is to identify important assets, concerns with specific areas and processes, (this could be perceived risk linked to the assets). It is also designed to understand strategies used by the organisation and associated vulnerabilities. At the end of phase 1, areas of concerns are matched to threat properties identified. Areas of concern are mapped unto users using the network access tree. In summary OCTAVE allows security risk evaluation that assist organisations to determine risks associated with confidentiality, integrity and availability of critical information assets.

7.2 Overview of CRAMM

CRAMM is an acronym for United Kingdom's Risk Analysis and Management Method. It applies a structured approach to risk analysis. It is designed to enable reviewers conduct detail security audit on information systems. According to government and practitioners, it is a tool that should be used by experienced or certified practitioners. The concept underlying CRAMM is that risk is dependent on asset values, threats and vulnerabilities. The risk analysis interview is conducted with owners of the assets, users of the system being analysed, technical support team and the security department where appropriate.

The outcome of CRAMM is usually to depict countermeasures necessary to mitigate risk identified during risk analysis. The need to mainly recruit trained practitioners in using CRAMM can be viewed as a weakness of the tool. This is based on factors such as cost for SMEs, flexibility, adaptation and adoption by other risk analysts who may not be familiar with the tool. Although it is sensible and important that the users of the tool are experienced with the application of CRAMM, it lacks the openness that permits professionals to transfer their skills to the CRAMM environment or organisation.

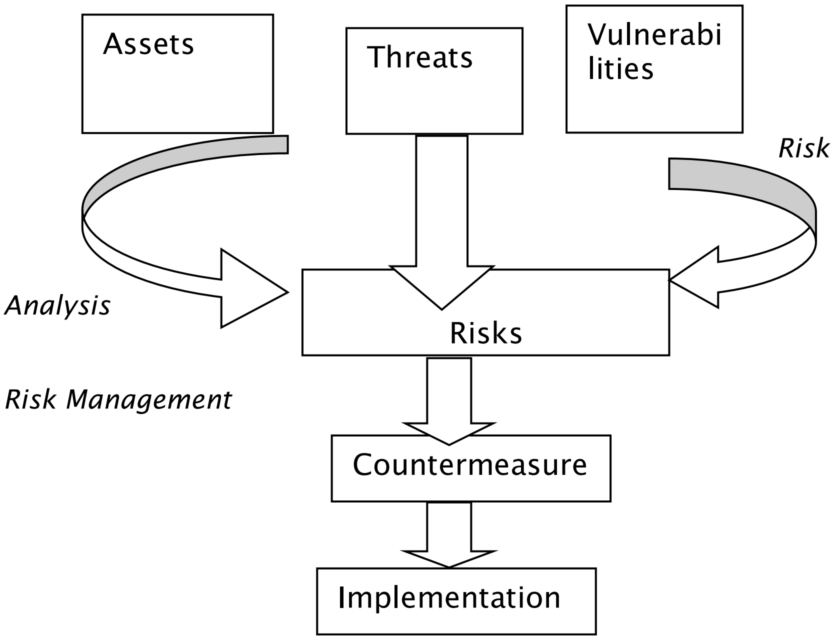


Figure 20 - Conceptual diagram of CRAMM

The key stages in CRAMM are as follows; measure your risk, understand your risk, set a target for your risk, manage your risk, adopt standards.

Key stages in CRAMM

Measuring your risk

Determining the scope of this risk and the extent to which it could be quantified is not an easy task. This is because risk is very qualitative as such could effectively be measured indirectly by assessing the cost associated with threat .According to proponents of CRAMM, it has the toolset that enables risk analyst to measure risk. Whether it does that effectively or not is not something that could be solely judged in this book. The view taken with regards to this is simply based on the notion that risk is highly subjective and qualitative therefore risk measurement should be assessed in different contexts in the same application environment.

Understand

An understanding of the risk and the level of the danger associated with it, is highly dependent on factors, such as the experience of the analyst, training, background and an understanding of the system being examined.

Set a target

The risk target relates to potential areas likely to have elements of danger. This also suggests there should be an understanding of the information system and the environment within which it is deployed.

Manage

This is the stage where vulnerabilities, threats and potential dangers are analysed together. Countermeasures are recommended as a means of mitigating the threats that might result in potential danger.

Adopt standards

Adopting the appropriate standards is a way of certifying your information system. It is basically to ensure that basic security requirements are put in place. There is a range of standards that one could adopt and tailor to a particular information system. The obvious one is the ISO17799, which was derived from the BS7799 for security management implementation, a defacto standard for the UK Government.

ASSET (Automatic security self evaluation tool) – *Nist (2002).*

ASSET is designed with the primary objective of identifying a standard way of performing self assessment. This is done by using a guide which highlights questions directed at the system specific control objectives measured against a benchmark. It is designed to help system managers gather system data. The assessment process involves data collection, reporting and analysis. It speeds up the data collection and reporting processes, as a result supporting the assessment process. There are roles or processes actively played by actors. These actors are the manager or Chief Information Officer (CIO), collector, reporter and expert of the subject being considered.

JAVA Security Model

JAVA is a programming language. Its design is based on the object oriented paradigm and for meeting challenges in application development of heterogeneous and distributed network systems. JAVA security model is based on what is known as the sand box model.

Sandbox Model

The sandbox model has a dedicated area that allows untrusted code to run or execute on a system. This is not a familiar feature common to traditional operating systems. Its proponents argue in the literature that JAVA security model allows an applet to solely execute in the sandbox region and similar regions within the JAVA virtual machine (JVM). In other words malicious code could be protected. This however does not apply JAVA applications, since they are mostly bought off the shelf and installed on individual's or an organisation's PC. Within the perimeters of the sandbox is JAVA security manager. Its role is to ensure that borders of the sandbox is respected and observed. In the event of an applet performing maliciously, JAVA's virtual machine checks with the security manager if the running of an applet goes ahead. If the feedback is positive the code is allowed to run or else terminated. Common issues regarding this security model relates to authentication and encryption of data. It is also vulnerable to the "man in the middle attack". This attack is a description given to the interception of data by an agent on a network usually observing the communication between client/servers of a network. JAVA usually adopts a technique known as

"digital shrinkwrapping" to counteract this form of attack. This is achieved by exposing tampering of responses sent from a server. It checks the integrity of the server's response. JAVA security model is effective and useful within the confines of the operating systems platform. The main weakness of the security model is that it does not take into account embedded and inherent risk within a communication network. Whiles the network platform promotes mobility it also exposes itself to numerous attacks on the network. Although development of the sandbox model extended to the entire JVM based on the thinking of "no built in notion of untrusted code to networks", the key risk highlighted which is common to networks, still hangs like a "debacle sword" on the JAVA security model Fritzinger S.J, Mueller M (1997).

New Trends in security management

Holistic Security

The concept of holistic approach to information security was introduced by Williams (2003) within the context of both risk and security management on global communication platforms. This has been a prominent area of research with industry playing significant role, although within domains of advanced economies. Musaj (2006) proposes design steps believed to be key to creating holistic security. The enterprise architecture serves as the foundation of holistic security. Four layers are identified as components of the architecture. These are, Business Architecture (BA), Information Architecture (IA), Application Architecture (AA) and Technical Architecture (TA). The model seems to be based on non functional requirements. These are requirements which when satisfied support the business processes of an organisation. The paper discusses technology requirements, which cut across different application environments and boundaries. The checklist comprises approximately 86 items related to security architecture design specification. Musaj (2006) argues that security is not a technological issue but a management one. Although this is true to some extent, we cannot understate the fact that technology plays a vital role in the successful management of security.

ISMM – Information Security Maturity Model

According to Symantec, although information security is sometimes not the heart of most organisations competence, it is a central requirement of most organisations. ERP (Enterprise Resource Planning), TQM (Total Quality Management) and CMMI (Capability Maturity Model Integration) are frameworks, when implemented could serve as a base for serving a corporate information system Alaboodi Saad Saleh(2006). Alaboodi Saad Saleh(2006) place emphasis on the implementation of standards as a means of supporting technical security. There is importance placed on proactive rather than reactive approach. The author introduces a new Information security maturity model (ISMM) that incorporates different schools of thought in the security industry.

ISMM covers 3 main areas. These are layering dimension, process dimension and people dimension. The layering dimension describes five main areas. These are, 1 physical and environmental security, 2 front end system security, 3. backend system security, 4 comprehensive security awareness and 5 definite security. Each of these layers has strengths with regards to specific problem areas, covered within requirements of holistic security. The general notion of ISMM is that visibility decreases across the layer from physical and environment security to the last layer known as definite security. Although the model attempts to integrate security requirements and systems, there is no evidence and importance placed on risks captured during the application of the security models. The models solution areas map onto domains outlined by ISO17799 for security standards AlAboodi S.S (.2006).

Summary

This section reviewed classical and contemporary security risk models for governments and businesses. The feature common to these Models was that none of them addressed risk inherent and associated with heterogeneous and hetero-standard systems as mentioned in chapter 3. Models proposed are usually based on the premise that network infrastructure supporting business processes were homo-standard. There is also too much emphasis on hardware and software. Security risks associated with soft issues such as skills and vulnerabilities with consumers have not been addressed satisfactorily.

The chapter provided an insight into the risk spots and security vulnerabilities of information systems that support Online Business and electronic based transactions. The methodology proposed highlights the fact that there are risk access spots that need to be identified in the development process of such systems. It also suggests the need to determine perceived risk and actual risk. Although the risks identified are of critical importance to such systems, the risk areas could evolve or change. The underlying mathematical model is applied to electronic business cases with regards to on-line banking and results presented in chapter 9.

The chapter also described details of concepts and notations underpinning SSTM. The Concepts and notations described comprised, risk,(r) , RAS (Risk Access Spots), Zones, which represents Locations on a network. Zones can be local or global. They are graded as 1, 2 and 3 meaning low, medium and high levels. RIG (Risk Identification Grid) for integrating risk .extracted during risk assessment. Factors essential to synchronization process were outlined. These include time, event and attack, as well as the Zone. RISG (Risk Identification and Solutions Grid) a tabulation of recommended solutions for the security risk problem identified in RIG was also presented. A subsection of the chapter recaptured guidelines for implementing SSTM. Chapter 8 is a critical analysis of the prevalent phenomena of terrorism, its origin and impact on the freedoms of ordinary people, corporations, governments and states.

Chapter 8

Terrorism

This chapter evaluates threats to our personal freedoms as a people, especially among economically advanced countries. Terrorism has become a predominant phenomenon that should be addressed as a central part of government and a nations development and advancement strategic and economic goal. The chapter explores how the cyber world serves as a potential tool for bondage through terrorism rather than a means to the freedoms of civil society. This chapter discusses other forms of terrorism tools with the view of drawing similarities and contrasts of the different scenarios and circumstances that are likely to be considered a threat.

The chapter argues that possession of chemical, biological and nuclear materials themselves should not necessarily constitute a terrorist threat. It is rather the transportation, poor management, use and disposal of them that should be seen as a threat to the US and allies. The chapter also assesses the extent to which these threats affect human life and homeland security. Additional challenges relate to climate changes, natural disasters and negligence associated with disposal of chemical, nuclear, and biological waste.

This chapter also assesses the history and evolution of terrorism globally, by examining perceptions, strategies, and countermeasures, both past and present, for addressing terrorist threats and acts. The chapter also assesses how such past events affect our thinking in dealing with currents threats as well as effect on present world and global climate. In order for us to appreciate its history, it is necessary to place it in a context by providing definitions that guide our understanding and what we deem as terrorism.

Definitions of Terrorism

Reid (1997) stipulates that terrorism is defined from a Western perspective, rather than global, as its' definition is driven by government and the media of the US. The definition can be subjective as academics, government, businesses, and ordinary citizens can sometimes have different interpretations (Hashim, 2006).

(Fletcher, 2006, p.899) propounds that terrorism is a super crime that is driven by eight variables, which comprise p.899"the violence factor, intention, victims, wrongdoers, drama, theatre, a justice cause, organisation and absence of guilt", and therefore cannot be categorised under other criminal activities such as murder. According to Fletcher, "It shows characteristics similar to war".

Title 22 of the US code defines it as a "politically motivated violence perpetrated in a clandestine manner against non combatants" (Ruby, 2002, p.9). It is an act orchestrated to create fear among people other than the victims, which are affected by the acts of violence (Ruby, 2002). The FBI defines terrorism as "a violent act or an act dangerous to human life, and subsequently violates criminal laws of the United States or any state, to intimidate or coerce a Government" (Ruby, 2002).

Origins of Terrorism

The word terrorism was first used during the Jacobin reign after the French revolution between 1789 to 1794, referred to as the reign of terror (Laqueur, 2001; Banks, Nevers & Wallerstein, 2008). It also derives its roots partly in the public execution of approximately 18,000 people, which the French legislature considered as "enemies" in its newly formed Government (Hashim, 2006). The assassination of the Russian Tsar, Alexander II, in 1881, the assassinations of the French President Marie - Francois in 1894, US President William Mckinley in 1901, and the bombing of the Greenwich Observatory in London in 1894 all constitute acts of terrorism. These are carried out by what is described as anarchist terrorist (Laqueur, 2001).

The killing of the Austrian Crown Prince in Sarajevo in 1914 precipitated the First World War. The 1917 revolution in Russia also signalled the end to the Russian empire in 19th century Europe. Other forms of armed confrontations in other parts of the world such as Colombia, Northern Ireland, and the Middle East all contributed to international terrorism (Gasser, 2002).

Terrorism can also be associated with religious movements and political uprisings (Bullock, Haddow, Coppola, & Yeletaysi, 2009). Movements such as the "Sicarri" in Palestine in (A.D. 66-73), an extremist Jewish group, used a short sword known as the sica for assassinating opponents such as the Romans and some Jews during the Roman occupation of Palestine (Laqueur, 2001; Banks, Nevers, & Wallerstein, 2008).

Another terrorist group which was an Islamic sect, the "Assassins" in the 11th century, strived to change Islam by killing Sunnis and Christians based in Persia, communities in Syria and Palestine, as well as statesmen and government officials. They mostly used daggers as the weapon of attack. Other groups comprised the Ku Klux Klan dating back as far as 1865, 1915 and 1944, where they attacked, terrorized, and killed Black ethnic minority people (Laqueur, 2001; Banks et al., 2008). Other groups comprised the Provisional Irish Republican Army in Ireland and England between 1969 to 2005, which targeted economic assets and state buildings in Britain, and Hamas, which used suicide bombs and attacks (Banks et al., 2008). Terrorist attacks also evolved and originated from hubs, camps, and networks located in the Middle East and South Asia. There have been attacks from non- noticeable sources, such as Guyana, where "Russell Defreitas", a native from Guyana based in the USA, was linked with a planned attack from the radical Islamic group Jamaat al Muslimeen. The Pakistani born, US citizen recently planned an attack which was foiled at Times Square in New York, Barron & Schmidt (2010).

The Nigerian Terrorist and extremist convert also planned to carry out an attack on Christmas Eve on-board a plane via Amsterdam to the US. This perhaps gives a broader picture of the continuous threat al Quaeda poses to state and national security. These cases suggest that terrorists may emerge anywhere in the world so far as that community has elements of radical and Islamic extremism (Hashim, 2006; Bullock et al., 2009). Past and present cases show connections with religious extremism; however, terrorist attacks historically have been carried out with much more focus on prominent people as well as people in leadership (Laqueur, 2001).

Current and Emerging Threats

The role of organized networks and recruitment camps in recent times, especially among European Countries such as Germany, Spain and Britain serve as incubators for terrorism. These networks show characteristics similar to terrorists groups in the 19th century (Caudill, 2008).

Significant activities and communication networks by al Qaeda on the Internet, as well as insufficient border control within the US, facilitates activities of terrorist networks and groups (Heyman and Ethan, 2008). According to Lewitt and Jacobson (2008), the new terrorist threat facing the US involves growing popular networks motivated by Osama Bin Laden's doctrine and ideology. These include al Qaeda in Iraq, Lybia Islamic fighting group, al Qaeda in Islamic Maghreb, and groups such as Hizballah, an Iranian sponsored group based in Lebanon with global reach and influence.

According to a 2007 US State Department report, Hizballah remains then most technically capable terrorist group in the World (Caudill, 2008). Some of the terror acts attributed to Hizballah include 36 suicide bombings between 1982 and 1986, thus the bombing of the US embassy in Beirut taking the life of 63 people, bombing of US embassy in Kuwait Airways flight 221 enroute to Pakistan and the hijacking of TWA flight 847 (Caudill, 2008). The new face of the enemy changes from a stable form to an elusive and evasive stature (Raufer, 2006). The enemy and threat facing US and Allies is unidentifiable, undefined and unexpected (Raufer, 2006). The enemy evolves from hybrid groups capable of transforming and mutating itself in a short space of time. These terrorists' networks are usually made up of militias, guerrilla groups, fanatics, warlords, lunatics and criminals (Raufer, 2006).

A strong emerging threat is the lone actors also known as lone wolfs. The Boston bombers who set explosives on the day of the Boston marathon is an example of lone Wolves although at the time of completing this book, it has not been fully established whether they acted by their own intentions or were drawn into these acts by acting on instructions from a more experienced group. In any case it is clear that these young men have been influenced and inspired by a false sense and interpretation of Islam.

Chronology of recent cases

The shootings in a gay night Club in Florida in 2016 by an Islamic extremist sent ripples of shock waves among civil society. The intelligence required to profile and track such a person was inadequately applied in this instance.

On the 23rd May 2013 the south of London experienced a horrendous and brutal murder of an army officer in broad day light that sent shock waves across the United Kingdom, by two British citizens motivated by extreme ideology and allegedly shown evidence of radicalisation. It can be argued that this may not be the central reason behind such attacks, but rather people with very troubled past, sucked into this extreme ideology. To paraphrase the British Prime Minister Mr Cameron, it seemed they were rooted and prepared to jump onto some sought of an already made conveyer built for radicalisation, the outcome being homeland mentored murderers.

I believe a forensic analysis and examination of the background of these young men might have revealed some important facts. In the aftermath of that incident it seemed paradoxical the way these men were described by past and present friends as "the normal boy or man" next door. This revelation, the least is astonishing. This is also consistent with comments made by most people that new the background of the Boston bombers. The acts resembled most peopled usually dubbed as falls extremist and also motivated or driven by such ideology despised by most people of the Islamic faith.

One of the fundamental reasoning which underpin religious groupings is that it provides a strong sense of belonging and acceptance, which might not be experienced at home, school or at a work place. This is central to all religions. Nonreligious persons may not be in the position to understand this phenomenon and ethos. This sense of belonging to a community may be driven and encouraged by communities where such beliefs are practiced.

The White Islamic convert Richard Dart came from a middle class English background whose parents were teachers in the town of Dorset, however was successfully radicalised from a normal young man to becoming an extreme Islamist ideologist (Independent, 2013).

It is too early however to suggest that there is any indications of a pattern among these cases. It can however not be disputed that most attacks in Britain has been carried out by home bread and grown citizens. This suggests that there is the need for a paradigm shift and a counter narration of how terrorism is addressed and prevented.

One of the failings of policy and lawmakers is that, the central leadership is quite often devoid of adequate understanding of matters associated with religion. Every religion operates within a wide spectrum of dogma. There are those on the left of that spectrum for which we may consider more liberal whiles others may fall within the centre and be considered as moderate. The third may be on the right of the spectrum and may be viewed as extremist or hard liners.

It is a fundamental mistake to suggest that such views do not coexist as part of the widely accepted teachings. Religion could be analogous to the Internet. It is the only system that transcends geographical boundaries apart from the Internet. It has its own language. On the contrary citizenship is boundary specific and restricted by geography and jurisdiction. This enables any form of extreme view to reach a global audience catapulted by the Internet.

On 27th of May the Telegraph had a headline “The hunt for the white widow”. This article referred to Samantha Lewthwaite, a white muslim convert from Aylesbury who allegedly detonated an explosive in Kenya. She is currently on the run and was married to one of the 7/7 bombers. The three dangerous British citizens who planned to cause catastrophes bigger than the 7/7 suicide bombings is also another case that substantiates some of the views in this book. The questioned still unanswered is why British citizens still target their home soil? Is there something that serves as a trigger or stimuli to hatred to the Land. This book will argue the need to critically evaluate these factors.

Lessons for the future

According to UK government response to intelligence and security committee’s report into London’s terrorist attacks, key factors attributed to failure in preventing the 7/7 2005 bombings in London were due to intelligence gaps, poor surveillance and inadequate resources (HM Government, 2006). There were also lack of cooperation between Britain and Pakistan over visits of two of the 7/7 bombers, Mohammed Sidique Khan and Shehzad Tanweer, who were in contact with extremist groups. This is evidence of failure in information sharing, coordinated response and counterintelligence. It also supports the notion that government has not been able to invest adequate resources in fighting and mitigating terrorist attacks. One will believe that after 9/11, Allies of US, such as UK would have learnt certain key lessons regarding intelligence failure. Other failed preventions include the night Club bombings in Soho.

Although there have been some failures, there are also successes, for the US and Allies. British Intelligence MI5's counterterrorist operations and police, foiled a major terrorist attack on a night Club and theatre bombings at park lane in London, where two Mercedes Benz were spotted with parked nails and fuel gas canisters. According to the police this would have been disastrous, if it had been successful (Night Club bombing, n.d).

The national terror alert of US, reported an incident a few years ago in Nevada, Las Vegas, where a high way patrol pulled over a car. One of the men in the car, by name "Faarax", of Somalia origin was flagged by the (National Crime Information Centre) as positive after an enquiry by the patrol. The patrol was instructed by local agents to let him go, as there was no active warrant to arrest him. Although one of the men in the car "Abdow" was later apprehended by agents in Minnesota, it is not clear whether one can attribute the failings of not making any arrest to one particular entity or unit. It could be argued that there was systems failure and , where the directives in place for intelligence and law enforcement are not positioned adequately to coordinate and interpret the threat potentially posed by these men at that time. This case is indicative of lack of comprehensive and coordinated response to what might be a potential terrorist plot and attack (National Terror Alert, 2009).

Conflicting interest among interagency collaboration and co-operation among different stakeholders operating under the umbrella of the DHS (Department of Homeland Security) can be a setback (Knezo, 2006). This is especially profound in the area of R&D funding where most of the portfolio managers will return to Laboratories that are also bidding for funding. Conflict of interest can create sub optimality, as some agencies lack the necessary resources to operate efficiently whiles others may be more resourced than necessary.

Emergency response managers face difficulties in dealing with uncoordinated messages and information (Bean, 2007). Uncoordinated electronic bulletins can lead to information getting into the wrong hands, where there are poorly unsecured communication networks. This is a limitation that needs significant improvements to build the necessary counterterrorism intelligence operational framework, if governments were to succeed. The lack of effective information sharing and emergency response system can cause counterterrorism and intelligence operations to be ineffective.

Conditions such as local government administrative capabilities, different levels of commitment and strengths among city governments, are challenging factors required in determining how funding should be disbursed (Brian J Gerber, 2007). Uneven distribution of resources required to support counterterrorism operations is an "Achilles heel" that can be exploited by the enemy. Lack of emphasis on risk assessment, performance and capability models serves as major weaknesses in determining fund disbursement priorities. This is an area where government needs to do more in developing robust and competent predictive models for formulating funding policies.

Alliances, information sharing and intelligence need to serve as key to cooperation among local communities. This can be sometimes ineffective as, there are underling communication difficulties between ordinary citizens, law enforcement agencies and intelligent services, (Eberhart R.E, 2003). Lack of effective collaboration among stakeholders in information sharing and intelligence is a cause of failure in provision of robust and comprehensive homeland security.

According to (GAO, 2004), Homeland Security Strategy partially addresses resource investments, risk management issues, performance measure issues, when integrating various stakeholders as well as carrying out set objectives and responsibilities. These findings show the need for more efficient performance Metrics, Capability and Risk models for assessing how, where and when should government invest. Constant change of intelligence data among varied number of communities needs to be managed more effectively, through coordination.

Summary of Chapter 8

This chapter discussed threats, historical insights and origins of terrorism. Emerging and current threats were also reviewed using a chronology of recent cases. Lessons for the future were also highlighted. The author believes that the nature of Terrorism and the drive behind this phenomenon has not been fully understood by policy makers of both developing and advanced countries. This view is backed by recent events where suggestion of a dialogue between the Taliban, United States and the ruling government in Kabul was flagged up as a potential route to resolving the conflict in the region. This approach to conflict resolution is likely to be imitated by many countries experiencing similar challenges. It may be also considered as one of the worst turns in foreign policy. The position of this book is that there is no winning outcome, except great lessons could be learnt for future adventures. The next chapter presents systems that could be employed as a part of critical response in case of a potential attack or natural disaster.

Chapter 9

Critical Systems Response

This chapter explains cyber technology and systems that drive both public and private sector services technologies and how they are applied in combating natural and manmade threats and disasters. The comparative analysis explores the different types of technologies used for disaster management. It also compares and contrasts how technology affects the effectiveness of government and private agencies in preventing and responding to current manmade and natural disasters and draws conclusions from the analysis. The chapter compares and contrasts requirements for problem areas that need technology based applications and solutions. The chapter also covers challenges associated with the need for application of technology and the consequences of technology failure.

Problems that require Technological Solutions

Problems that require technology base solutions include the detection of chemical, biological, nuclear and radiological weapons. There are other problems associated with vulnerabilities on computer networks that could be exploited to sabotage businesses through the acts of denial of service, release of malware, evading intelligence and capture and working towards the efficient dissemination and sharing of information among stakeholders. An example of such an attack is a DOS (Denial of Service) or a DDOS (Distributed Denial of Service) attack on network data transmission and communication points known as Ports as well as Protocols that govern data communication rules (Williams, 2007;Wright, 2008).

For example several web applications provide services from a transmission point known as port 80 on computer networks. This port can be vulnerable to attacks by an experienced hacker who may also be a terrorist. A denial of service attack could be launched disrupting the services from the port 80 communication channel. An attacker could dump several lines of code in different syntax or programming languages as a way of disrupting the services provided by the software. An application could also be exploited to consume system resources. An attacker could also compel an application to malfunction. This is possible even though communication ports are meant to close when dormant (Williams, 2007; Wright, 2008). A Terrorist that intends to launch a DOS attack is likely to succeed if computer servers are left unguarded effectively by system administrators.

The need for warning systems is also essential as they predict changes associated with the weather and the environment. Such systems could anticipate events such as, Tsunami, Katrina and manmade disasters such as the Gulf of Mexico Oil Spill. The application of technology is also essential in analysing behavioural patterns of people in crowded areas such as airports, ground transportation terminals and market areas. Areas such as recreational venues including cinemas, restaurants and bars are equally important.

Overview of Technology Based Solutions

The main technologies that support homeland security operations are surveillance technologies, data mining, pattern recognition tools, biometric systems for access control, authentication, authorisation, approval of access, anti-spoofing software, unmanned vehicles, ultra-violet, infra-red detectors, chemical, radioactive, biological and nuclear detectors, port and border security systems and anti malware software (Kaplan, 2007; Masters, 1999).

These technologies are usually developed in private sector, but also on a number of occasions with the collaboration of government agencies. Some of the technologies that have become effective in deploying emergency management and disaster response systems in recent times include real time data collection and information generation using airborne sensors, satellite remote sensing for near real time geospatial data collection from different regions and locations and the use of terrestrial mobile mapping Zlatanova and Li (2008).

Data communications and networks are also additional essential tools critical for terrorism prevention. Communication software technologies capable of mapping data shared or communicated between person to person or among a group of people is useful. The lack of use of such technologies leaves several gaps within any security apparatus or infrastructure. In some countries the use of such software may be deployed in a limited fashion due to legal requirements and the need to comply with privacy laws. The difficulty is whether the state and its citizens will be prepared to trade off a few freedoms for safety and security. Lawmakers and citizens should jointly examine what factors should determine safety and security? And what sacrifices will citizens be prepared to make?

Technology based solutions can enhance homeland security in many ways by supporting efficient information sharing, emergency response activities, building intelligence for counterterrorism operations as well as serving as a road map for digital evidence recovery (Berry, 1998). It can also assist in the analysis of large and complex data sets, which humans are incapable of analysing or find it difficult to interpret. Cyber security and defence are examples of counterterrorism strategic areas that are experiencing exponential growth of new tool development useful for intelligence data gathering (Thuraisingham, 2003).

Private and Public Sector Technology

Intelligence Building & Analytics

Large data analytics is the ability for systems to derive new knowledge and reasoning using machine learning strategies and algorithms. The complex nature of large data requires tools, strategies and algorithms that enable systems to build intelligence critical for defending and securing national infrastructure. In order for counter terrorism to have an impact on homeland and national security, intelligence building should be at the forefront of strategic thinking. One of the main challenges that security and intelligent agencies face, is the capability required to derive new knowledge and intelligence from large data. This might require Internet surveillance.

Several government agencies suggest that data mining tools enhance safety and security. It is a tool that can be effective in the airline industry. Existing technologies can be applied to passenger profiling and pre-screening. There are securities enhancing verification systems that help airlines to quickly validate personal information supplied by their passengers. There are also software packages for customer recognition and data integration that verify information from a variety of sources associated with purchases of airline tickets in real time (Wright, 2008).

Pattern analysis software tools such as neural networks and genetic algorithms can provide trends on operational activities associated with counterintelligence (Berry, 1998; Masters, 1999). An example of such an application of a software tool for pattern analysis is to be able to predict attacks as well as determine the level of potential destruction of an attack (Koh, 2002). These trends provide a lead to stakeholders regarding investment opportunities and possible saboteur, as well as putting in place mitigating strategies at local and community levels (DeRosa, 2004).

Profiling

Profiling can be integrated as part of a software tool using artificial intelligence techniques. Although the technique can be useful for recognizing unusual behaviour, there have been concerns raised in the past by the American Civil Liberties Union and Arab-American groups, such as the sub committee that held a hearing on the issues of aviation security with a focus on passenger profiling on May 14, 1998.

The hearing focused on issues related to computer-assisted passenger pre-screening system (CAPPS), an automated screening system designed to separate a small percentage of passengers that required additional security measures based on factors such as passenger's religion, race or national origin (Turley, 2002; Williams, 2004). There has been a shift from profiling using discriminatory techniques to profiling that takes into consideration of generalization of patterns gathered from the data (Turley, 2002).

Critics assert that this form of technology is invasive and violates privacy laws. They argue that Terrorists do not usually operate under patterns that are easily recognizable, and therefore it is likely that the technology is used in targeting innocent people (Carlson, 2003).

Information sharing & emergency response systems

Information sharing and emergency response systems are technologies that are used and driven by the public sector. The technology uses multi casting messaging techniques to disseminate information to specific persons on a computer network. In other words not all persons on that network will receive the message being sent across, unless it is relevant to them. One can also use broadcasting systems to disseminate information where there is the need for mass evacuation, in case of a disaster or adverse incident. Emails and electronic bulletins can also be disseminated using a multicasting strategy in case of emergency and disaster management operations (Bean, 2007). These are technology systems championed by public services, usually first respondents in an emergency incident.

Case Studies

Northwest Airlines, Jet Blue Airways, and Delta Air Lines all came under scrutiny at one point for sharing passenger data with the government without getting the consent of customers. The USA started Airline Background Checks after September 2001 (Swartz, 2004). Northwest acknowledged that it had provided three months of data, which included credit card numbers, addresses, and phone numbers, on millions of passengers soon after September 11, 2001, to the National Aeronautics and Space Administration (NASA) for a secret government air-security project. NASA said it used the information to investigate whether data mining of the records could improve assessments of threats posed by passengers. Jet Blue conceded it had violated its privacy policy by turning over records on 1.1 million customers to a defence contractor. Both airlines were criticized for voluntarily sharing customer data and were being sued by angry passengers in class-action lawsuits.

The White House's Office of Management and Budget (OMB) put the brakes on the Transportation Security Administration's new scheme to find the bad guys among airline passengers the second-generation Computer-Assisted Passenger Pre-screening System (Capps 2). OMB wants TSA to show that the computer "data mining" project is effective in reducing risk. Civil liberties groups have raised red flags on the program, which would search commercial databases on credit cards and other personal information to determine which individuals pose the greatest security risks. TSA chief James Loy suggests that screeners will never see or retain the commercial data used to conduct the analysis and the data will be discarded after using the data. HNC Software, a San Diego-based firm that develops risk-detection software led a team of companies to build one of the two main prototypes. HNC is working with Houston-based PROS Revenue Management Inc., which already supplies customer analytic software to 17 of the top 25 USA airlines, and Acxiom Corp., a data marketing firm in Little Rock to collect information on land records, car ownership, magazine subscriptions and telephone numbers (Verton, 2002).

“The CAPP 2 systems will use extensive data mining of credit and criminal records as well as travel patterns collected by the airlines. NASA has proposed developing “non-invasive” neuroelectric sensors or brain scans for use at the screening points to see if people are having “suspicious thoughts”. (Capt.R.J.Cox). It is not the scope of this book to discuss the operations of CAPP 2 Systems in detail.

HNC's ProfitMax is one example of this type of proactive neural network technology ProfitMax records the-details of each customer's interactions. The data is updated with every financial transaction, every call placed and at any other interaction point. Using neural network, pattern-recognition technology, ProfitMax predicts if a customer is unlikely to pay his bill or if he may change to another carrier. It can also predict the best time to take advantage of sales opportunities. (Hanna Hurley, 1999)

HNC Software, a San Diego-based firm that develops risk-detection software, is leading a team of companies to build one of the two main prototypes. HNC is working with Houston-based PROS Revenue Management Inc., which already supplies customer analytic software to 17 of the top 25 U.S. airlines, and Acxiom Corp., a data marketing firm in Little Rock, Ark., that collects information on land records, car ownership, magazine subscriptions and telephone numbers (Dan verton, 2002)

Joseph Sirosh, executive director for research and development at HNC, said his company's technology is currently used to detect credit card fraud in the private sector. It is based on neural network technology that can pick out vague relationships between data that may indicate the potential for terrorist activity, "The data will have to come from the airlines, "It will have to be pooled, and we will have to have a way to get the analysis to the various checkpoints around the airports". He said, HNC is currently talking to both the TSA and Atlanta-based Delta Air Lines Inc. about the feasibility of deploying the technology throughout airports (Dan verton, 2002)

Consequence of Technology Failure

Technology failure may lead to data loss, financial loss, and a negative impact on the confidence of the people using disaster management systems. This might lead such persons leading to sources of support that could eventually result in further weaknesses and vulnerabilities of existing systems. In case of incident first respondents may not be effective as the systems they rely on for communication and coordination could be rendered redundant.

Technological and Socio-Cultural Solutions

Technological and socio cultural solutions should work hand in hand by encouraging suppliers of new technology, governments and end users whether being customers or enthusiast. The continuous absence of such harmonisation will not redress the current situation where mass consumption of technology is misguided due to poor awareness of individual rights to data protection and misuse. The existence and enforcement of law in itself is inadequate and cannot substitute human rationality. In other words better understanding by consumers in respect of sources and destination of data, in the cyber world is much more superior to the application of law and technical know how.

Challenges

The main limitations according to this review can be summarized as human error, interoperability issues, shortage of expertise manning existing systems and privacy laws affecting aspects of homeland security. Although the most sophisticated technology system can be installed, there are potential human errors that must be taken into account when deploying as well as running the system for homeland security. The lack of efficient human management support system serves as a potential cause for technology failure (Kaplan, 2007). There are potential interoperability and heterogeneity issues anytime devices operate on different platforms, for information sharing and emergency response purposes. Getting the right kind of expertise (Kaplan, 2007), can also be a challenge given the ubiquitous nature of communication devices, and wide range of free access frequencies. Privacy laws, lack of interagency collaboration and cooperation can hinder hinders the effective use of any form of technology for counterintelligence operations (Metz, 2005).

Summary of Chapter 9

The conclusions drawn from this analysis is that although private and public sectors seem to have unique technologies for public safety and security, the systems are inextricably linked. The fundamental difference is that the private sectors spearhead the development of these applications with sometimes funding support from government. This funding occasionally leads to collaborative research and development initiatives between public and the private sector. The difference is that most technology applications developed by the private sector supports public services. The effectiveness of the deployment of such systems should usually be backed up with robust counter strategies. Chapter 10 presents such strategies and how to effectively use them for terrorist related incidents as well as cyber attacks of critical infrastructure.

Chapter 10

Counter Strategies

This book reviewed the history, origins of terrorism, its emergence and current threats. It cites a chronology of recent cases. It is the hope of the author that we learn the lessons for the future and better strategies for mitigating the threats we face today.

The nature of Terrorism and the drive behind this phenomenon has not been fully understood by policy makers of advanced countries such as United Kingdom and United States. This view is backed by recent events where suggestion of a dialogue between the Taliban, United States and the ruling government in Kabul was flagged up as a potential route to resolving the conflict in the region.

This approach to conflict resolution is likely to be imitated by many countries experiencing similar challenges if it turns to be successful. Conversely it may be considered as one of the worst turns in foreign policy in solution formulation if it fails. The position of this book is that adopting a synchronised and holistic approach to conflict resolution is more likely to lead to significant results. This simply means getting all parties involved whether considered weak or strong. This model works very well with families experiencing conflict or corporate bodies that pride in their reputation.

This approach should have commenced from the onset in Kabul as part of the strategy for the deployment of troops. In hindsight, it is easy to assert this line of reasoning, however wisdom dictates that there is no amount of violence that can substitute diplomacy.

The principle of no negotiation is contrary to human instincts and reasoning, and can only be effective if interested parties on any side of the negotiation table are considered irrelevant. Such an approach is primitive and only generates results in the short term.

There is no winning outcome, except hash lessons could be learnt for future scenarios. There are other forms of threats faced by the US, UK, its Allies and the world at large apart from terrorism. Some of the threats are climate changes, natural disasters as a result of environmental changes, unexplained natural occurrences, poor use of materials, management and disposal of nuclear, biological and chemical waste. This usually results from an initial legitimate industrial and economic use among countries, however the continuous management of the disposal of the waste is poor.

This book also argues that possessing of these materials themselves does not necessarily constitute a threat or association with terrorism, except that poor controls and lack of leadership may result to such an outcome. It is rather the waste resulting from processing these materials that constitute the threat, as this may lead to the hands of persons of malicious intent.

This book brings to light the emergence of a new type of citizenship driven by large volumes of data captured from digital footprints of ordinary citizens. It argues that our actual identities may not necessarily be defined by who we think we are, but rather by our online activities.
The zeal to protect a nation and its citizens may lead to people relinquishing certain freedoms. Some of these freedoms may relate to privacy in homes and lives, as well as the inability to express and experience our freedoms the way we intend to do in every day. Most ordinary people know that any act of terrorism is dooming and evil.

Although our cyber citizenship has enabled us to express who we are at different places, times and among different people, we often fail to appreciate what it takes to protect such opportunities, rights and freedoms. There seem to be a strong correlation between cyber activities and vulnerability of systems. Communications and information on the Internet has become a source of inspiration for radicalisation.

One of the critical tools weak in its use is counterintelligence and response to anti-radicalisation and extremist Ideology, highlighted initially. This is where the battle should be won, or at worst driven and led by policy makers, intelligent and security agencies. There is overemphasis on shire force and technology and the lack of will to apply sophisticated diplomacy tools.

The mitigation strategies outlined are not necessarily novel, however they are innovative ways of applying them and also serve as the basis of a novel model that could be emulated. The innovative strategies and tools are to *“Use sophisticated analytics and computational intelligence tools, Fight Ideology, Train and educate ordinary citizens, Avoid unnecessary legal jargons, Use ordinary citizens as driving force and engine and Establish a close strategic alignment with goals of emerging economies”*.

Deploy analytics and computational intelligence tools

Sophisticated intelligence and analytics tools such as KAIF Analytics used by large corporate bodies, businesses and governments can also empower ordinary citizens to have a transparent view of who is behind their networks at a micro level.

Fight Ideology

The battle against terrorism cannot be won over by solely employing the most sophisticated technology, military might, force and expert minds. If this were the case the United Kingdom may not be dubbed as loosing the cyber war. This is a lesson that has to be learnt very quickly. A war against Ideology is more likely to play a significant role in diminishing terror threats and the propaganda apparatus that drives it. Other effective strategies should involve the involvement of countries in regions where technology and expert knowledge is not as sophisticated as most advanced economies.

At the beginning of the Afghanistan war, I asked myself why United States and Allies would not sit and talk to the Taliban? I am of the school of thought and persuasion that no matter how extreme a person or group of persons view, beliefs and convictions, they are subject to persuasion, especially if your most credible alternative leads to violence. I am not making a moral statement, but rather a strategic one. The cyber world is a haven for the good, the bad and ugly.

Train and educate ordinary citizens

Training programmes for citizens in the United Kingdom, United States and other parts of the world should lead to awareness among citizens on a daily basis. One of the common issues is identity theft. The proliferation of personal and private details on social networking sites can be sometimes astonishing.

The simplicity and innocence to which ordinary users voluntarily submit information across social network channels such as Facebook and Twitter need a much more detailed review and understanding. Social networking sites should provide simplistic briefs of rights and obligations to users without using unnecessary legal jargons. In order for the role of security agencies to be effective, the activities of citizens, ordinary users should be encouraged as part of implementing a more cohesive and coordinated security process and infrastructure.

Avoid unnecessary legal jargons

The role of the law in protecting the rights of citizens and associated freedoms should not be undermined, although there is the need to avoid the use of unnecessary legal jargons. There should also be a balance between the law, its enforcement, rights to privacy and personal responsibilities. There is strong evidence to suggest that, the freedoms that come with the use of advanced technology in everyday life and enjoyed by ordinary citizens also come with potential threats which when not mitigated and safeguarded could be exploited for malicious purposes. A simplistic explanation of rights and obligations should be the way forward, if we were to approach a more inclusive cyber security strategy.

Use ordinary citizens as driving force and engine

Ordinary citizens should be guided and involved as the driving force for policy and strategy formulation in counterintelligence and response. Mitigation strategies need to be driven by experts and users alike. The author believes that the experiences of ordinary citizens with regards to everyday attacks serve as a valuable asset in deepening our understanding of what to do in order to protect personal freedoms as well as put in place countermeasures for dealing with the fears that may exist or arise as a result of excessive use of public networks.

On the contrary this is not what happens, rather citizens are placed at the end of the supply chain of information and knowledge acquisition and transfer. For instance the commonest security technologies and processes that facilitate most of our daily online transactions comprise SET, a standard designed by VISA to support all transactions carried out on its network.

Although these systems are designed to provide high level of security, users are in a better and stronger position if they receive the appropriate guidance from service providers to assist the public understanding of some of the best ways to secure personal data and resource. Information sharing concepts and techniques underpinning social networks show the benefits as well as fears. Recent case of bullying on Twitter of a prominent politician in the United Kingdom also made a major social network company like Twitter to consider putting in place more robust systems to protect user online.

Establish a close strategic alliance with emerging economies

Most foreign policies of advanced economies have the stain of selfish strategic interest, mostly accused of having no due regards to other stakeholders, unless parties involved are considered friends. I have heard these accusations from people from the international community as well as fellow citizens. There are times in war where there is the need to join hands with unfamiliar parties to fight a greater enemy. Developing a strategic alliance with only familiar parties of similar military might and cyber force will not necessarily work in every circumstance.

Adopt the KAIF System and Model

The continuous increase in growth of data on the Internet, public databases and distributed mobile systems as a result exponential growth of social networks calls for robust software capable of handling and understanding complex data set as well as making sense out of meaningless data. KAIF (Knowledgebase for Artificial Intelligence Forensics) designed by Intellas UK, is a digital Security, forensics, and incidence response software platform apply techniques capable of harnessing intelligent data analysis capabilities essential for digital security and forensic analysis for electronic crime attacks, investigation and case analysis on social networks. This could range from day to day network security breach, anti-terrorism surveillance on Internet, mobility based systems, Online Fraud, Online Masking for impersonation and digital evidence recovery, collection and forensic analysis.

KAIF captures vulnerable data likely to be relevant in a digital forensic application from both temporal and resident memories of computer networks. Data Packets are captured from routers and software applications running at operating system level or workstations of clients. KAIF captures packets transferred between local and external networks. The software also has learning capabilities. The data is captured in iterative mode through memory dumps. It also creates patterns that can provide leads to security and forensic investigators or analysts.

KAIF robustness enables it to perform the following tasks as part of its intelligent processing system. Reads data in packet form analyze data in packet form and suggest leads to a black box secured for future forensic analysis in case of network crash or malware attack.

KAIF captures vulnerable data likely to be relevant in a digital forensic application from both temporal and resident memories of computer networks. Data Packets are captured from routers and software applications running at operating system level or workstations of clients. KAIF captures packets transferred between local and external networks. The software also has learning capabilities. The data is captured in iterative mode through memory dumps. It also creates patterns that can provide leads to security and forensic investigators or analysts. Chapter 11 presents a novel based security model that could be adopted and adapted to manage the threats, risk, attacks and preparedness required for implementing a reliable and robust security response.

Chapter 11

SSTM Security Model

11.0 Introduction

This chapter presents the theoretical, philosophical and empirical foundations of a more robust and effective security risk model known as SSTM (Service Server Transmission Model) for managing security risk in Online Business. It also describes details of concepts and notations underpinning SSTM. The key concepts and notations described in this chapter comprise risk (r), RAS (Risk Access Spots), RIG (Risk Identification Grid), RISG (Risk Identification Solutions Grid), and Zones. This chapter provides the reader with justifications and reasoning behind SSTM of synchronising e-security methodology.

11.1 Theory

The concept of synchronization in distributed systems has been primarily applied to problem areas associated with time and events on communication networks across different geographical locations.

Synchronization is mainly to ensure that, times associated and recorded with respect to the occurrence of network events are valid. The event could either be a financial transaction involving the purchasing of an airline ticket or credit transfer to a particular bank account. This usually involves the synchronization of physical and logical clocks. The primary objective of this type of synchronization is to ensure consistency, avoid discrepancies and duplication during and after the transaction. Algorithms supporting these types of transactions have been discussed and proposed by Christian and Berkeley Coulouris (2001).Other algorithms for synchronizing distributed processes include interactive convergence algorithm (ICA) of Lamport and Melliar-Smith, fault tolerant midpoint algorithm of Lundelius-Lynch, Schneider's generalised protocol of clock synchronization and generalised clock synchronization protocol in isabelle/HOL. BV(2005).

Whiles previous works on synchronization focused on times and events, this work extends previous works by applying synchronization to security of global heterogeneous and hetero-standard systems by modelling the relationship of risk access spots(RAS) between advanced and developing economic platforms. It is hypothesised that this modelling will help secure the security gap between these economies in real life applications. The mathematical model synchronizes the risk and probable type of attacks associated with electronic security on distributed platforms across the globe. It forms the foundation of a new design approach for securing systems deployed on developing and advanced economies computer and communication network platforms. Arguments for the model and accompanied graphical representations have been published in the book synchronizing E-Security Williams (2004). The book also reviews the graphical models and associated descriptions as background information to the reader as discussed in Williams (2004). Experiments have been conducted using simulation techniques such as monte carlo technique to proof the validity and credibility of the mathematical model.

Global and Local Zones are identified using a location based algorithm engineered from the model. The model defines parameters and criteria for the location based algorithm of the mathematical model.

The modelling of the relationships has been based on essential variables derived from results of empirical studies published in previous work of Williams (2003). The framework below highlights the main sources of risk from studies on electronic banking on communication networks.

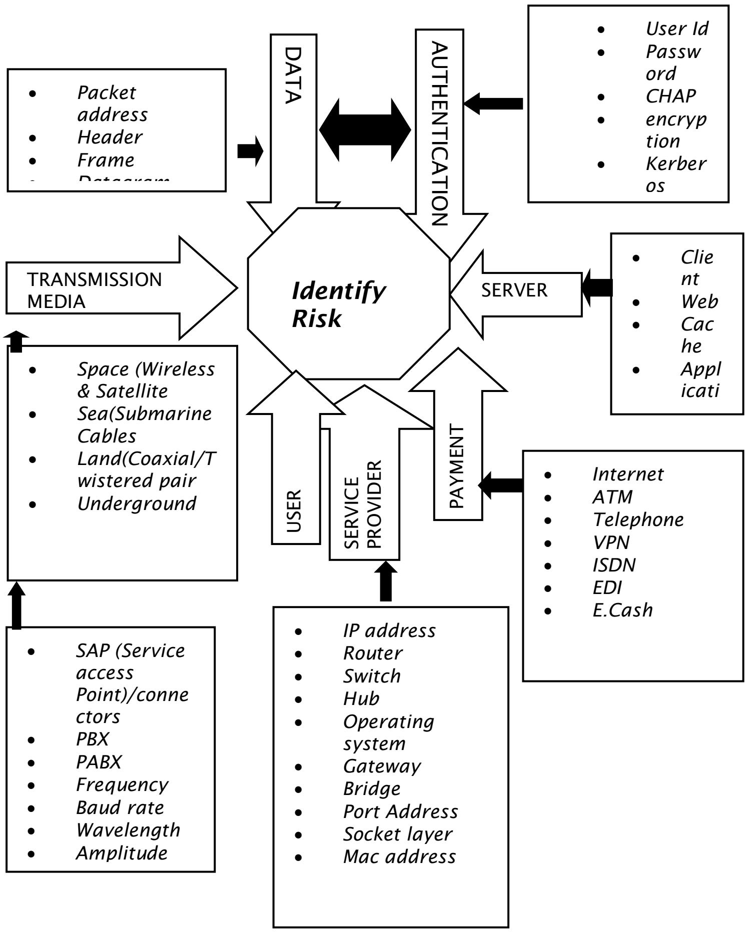


Figure 21 – Framework

The mathematical model uses basic set theory in conjunction with the Risk Identification Grid and Risk Identification and Solutions Grid in the synchronization process. The model is demonstrated as a simulation. The sources of risk identified are tabulated in the framework known as the RISG (Risk Identification and Solutions Grid. The Grid comprise risk identified an mapped unto appropriate solutions. The content of the risk identification framework may change depending on the application environment and the risk associated with that environment.

11.2 SSTM

SSTM is an integral part of the Synchronizing E-Security methodology based on the findings of empirical studies from the examination of communications infrastructure across the globe Williams (2004).

Previous models proposed by PMBOK (1996), Higuera and Haines(1996), Chapman and Ward(1997), Buchman(1994) and the integrated approach for risk response development in project planning by Ben-David and T. Raz (2001), OCTAVE, CRAMM, ASSET, JAVA security model and SCERT do not address security as an integral part of risk assessment, as SSTM adopts a holistic approach to risk and security management. This is the fundamental difference between Synchronisation E-Methodology using SSTM and previous Models.

This work presents the mathematical model as proof of concept and practical demonstration of the Service Server Transmission Model SSTM as a tool for synchronizing electronic risk and security methods. It is central to Synchronising E-Security Methodology originally published in the book Synchronising E-Security Williams (2003) mentioned in the background.

The analysis, evaluations and experimentations are based on seven risk areas within the selected risk access spots (RAS) identified in the SSTM of Synchronising E-Security Toolkit Williams (2003).

11.3 Reasons for SSTM

1. **Technologies that support electronic transactions are globally available to both advanced and developing economies Williams (2004).**

The global economy has technologies, which are available and accessible by both developing and advanced economies. There are also electronic commerce activities in both types of economies. The current technological age makes risk assessment of security in a global context a critical programme. There are Internet Users across the globe regardless of economic strength. Although the percentage of user participation of the Internet is not similar everywhere across the globe, there is evidence that developing economies have technologies that enable them to engage in electronic transactions similar to that of advanced economies. The author thinks that when it comes to the application of technology, mass or size does not matter much. A small mass of a certain type of technology can depict vulnerability that could be used as a means of attack.

2. Security Gap always a concern.

This suggests that it is important to synchronise the communications infrastructure available to both developing and advanced economies. It has been advocated strongly in this text that synchronising security among economies is critical. The lack of synchronisation of these security platforms leaves a security gap. Hackers and intruders could exploit the gaps in security. The present gap can be harmonised by encouraging the appropriate standards and policies. Policies and standards should fit the economic structure of developing economies. Risk is relative and subjective. The risks associated with technologies in advanced economies are not the same as those in developing economies. These are important factors that every risk analyst, systems manager and information systems management consultant should be aware of.

3. Assessment of authentication methods

The rules that constitute the design of security policies and algorithms do not integrate risk factors that evolve from developing economies. This means those security software designs do not anticipate risks and vulnerability that might evolve from the Internet platforms of developing economies. It is time for designers and developers to investigate risk factors that might cause harm as a result of such weaknesses. Supposing we assume that the mindsets and profiles of electronic criminals are the same, it could be argued that, electronic crime in advanced economies are similar to ones in developing economies. Perhaps that is the rationale behind the design of existing security systems and methods. Although that might be true in some instances, in Synchronizing the platforms and means of access to vulnerable elements of communication technologies are very different as evidenced by empirical studies in synchronizing e-security Williams(2004). This means that the avenues of attack as a result of present risk related to the communication technologies of developing economies are more compared to that of advanced economies.

4. Growth of Online business

Current global electronic business trends show that e-trade is still on the rise although there have been instances of Dot Com failures. There is enthusiastic participation from developing economies. The arms of central governments, banks and private companies are being encouraged to take opportunity of the competitive advantage that comes with the participation in such ventures. In advanced economies at least 60 to 70% of the population participate in some form of Tele-banking or Internet banking. Customers check their current account balances via telephone or Internet. Similar percentages of people use their credit cards to purchase items on the Internet. All these activities form part of e-trading.

5. E-trade regulations

Although regulations governing trade in advanced economies are not mandatory, it suggests that there are risk factors, which could only be borne by companies who choose to violate these regulations. E-trading will continue as technology becomes more sophisticated. For instance there are new mobile communication technologies that currently work in conjunction with the Internet using protocols such as (WAP) Wireless Application Protocol Keen.,Mackintosh, (2001), WiFi, WiMAX and WLAN. These communication devices could be employed to outpace current risk prevention technologies. For instance mobile communication devices could be disabled at street market places and transferred to any part of the world. The software for carrying this task is readily available at street markets. Replacing electronic chips in these mobile devices with custom built electronic chips could be highly dangerous and risky to electronic security.

6. Human vulnerabilities

The regional imbalance between developing and advanced economies needs to be addressed by channelling standards through organised bodies and structures such as governmental agencies, leading IT firms in these economies and interested academics. This could be achieved by both advanced and developing economies taking initiatives, which will be embraced by both economic communities. Such initiatives could be achieved through international conferences and forums with the participation of governments. Developing economies should be encouraged to contribute to discussions that lead to formulation of new ISO standards. For example how many representatives from Africa are in the committee for drafting the new ISO/IEC 24744 standard for software engineering meta-model for development methodologies? This is an area which western leaders in technology and associated governments including lobby groups of professional bodies have been quite inward looking with respect to standard development.

7. **Rise and growth of global electronic risk**

It is also likely that risk will increase due to a relative increase in capital expenditure in communication technologies in developing economies. The pace at which technologies are permanently distributed across the globe needs to be investigated and addressed with urgency. Lack of similar pace in the advancement of standards in information security management will cause a relative increase in security spending in advanced economies. The alternative means of solving the e-trade ban and regulations is by closing the gap in risk between advanced and developing economies.

Findings from empirical studies originally published in Williams (2004) depict that developing economies have placed less importance on risk spending. Although there are existing risks from the gap analysis conducted, there is still an increase in capital expenditure rather than risk mitigation technologies. The contrast shows that advanced economies over estimate risk.

Each of the steps discussed above will go a long way to help developing economies gain the credibility necessary for e-trading which will eventually reduced risk globally. It may also increase investment drive in developing economies in the medium term. This will ultimately have an effect on global economic productivity.

Current risk methodologies in information systems do not address this gap that exists which needs synchronisation.

A methodology has been proposed for synchronising e-security methods in global electronic transactions in the next section.

11.4 Descriptions of SSTM

This section is a description of Synchronising E-Security Methodology. There are six levels in the implementation process of the Methodology. These are usually accompanied by a set of models, known as SSTM (Service Server Transmission Model) presented below.

Level 1

Risk identification is the process of randomly listing areas considered to be risk access spots within the information system or network communication platform. Risk identification could span from areas as generically represented at levels 1 and 2 of the methodology.

This is the first step in the e-synchronisation process. Identifying the risk from risk access spots is the approach adopted by this methodology. Risk spots in italics might not necessarily be risk access spots in every environment although the view taken by this book has been derived from findings of field studies. This might vary from one environment to the other. It is however recommended that these risk access spots are used as a basic guide when accessing risk spots in any online business environment application environment.

Level 2

The objective of this level is to build a trail of perceived risk in the application environment. This could range from online banking, gaming, electronic payment system, general practitioner information system, online video service or online stock and inventory systems for a wholesale or delivery service. The risk identified should be extracted and well documented.

Level 3

(RIG) Risk Identification Grid extracted from **levels 1 and 2**. The grid shows recommended risk access spots on a network. The RIG was based on risk spots common to both developing and advanced economies operating and networks platforms identified in empirical studies by Williams (2004). The security analyst could make changes to the RIG by editing risks that are particularly associated with specific problems or application environments.

Level 4

This is risk integration. The process of identifying common and uncommon risk across all network platforms. This step is critical to the success of the synchronisation process. It involves the process of identifying common and uncommon risk across all network platforms. This step is critical to the success of the synchronisation process.

Level 5

This is the process of auditing the risk. This stage subjects the risks to an assessment, which determines whether risk is perceived or actual.

A perceived risk is a risk which is judged as potential threat. An actual risk is a risk judged to be a threat. The auditing at this level is meant to make the type of risk clear. This can be derived using the SSTM mathematical model for calculating risk.

Level 6

This is (RISG) Risk Identification and Solution Grid. This grid shows recommended RAS on a network with suggested solutions from a software simulator. The RISG is based on recommended solutions provided by a security expert or the simulator. Synchronizing E-Security Toolkit comes with a set of solutions.

Fundamental Concepts of (SSTM) Service Server Transmission Model of Synchronising E-Security Methodology

The ideas central to Synchronising E-security Methodology are based SSTM comprising risk identification, extraction, integration, audit and a risk identification solution grid derived from risk access spots on network and operating system platforms.

11.5 Pictorial representation of SSTM

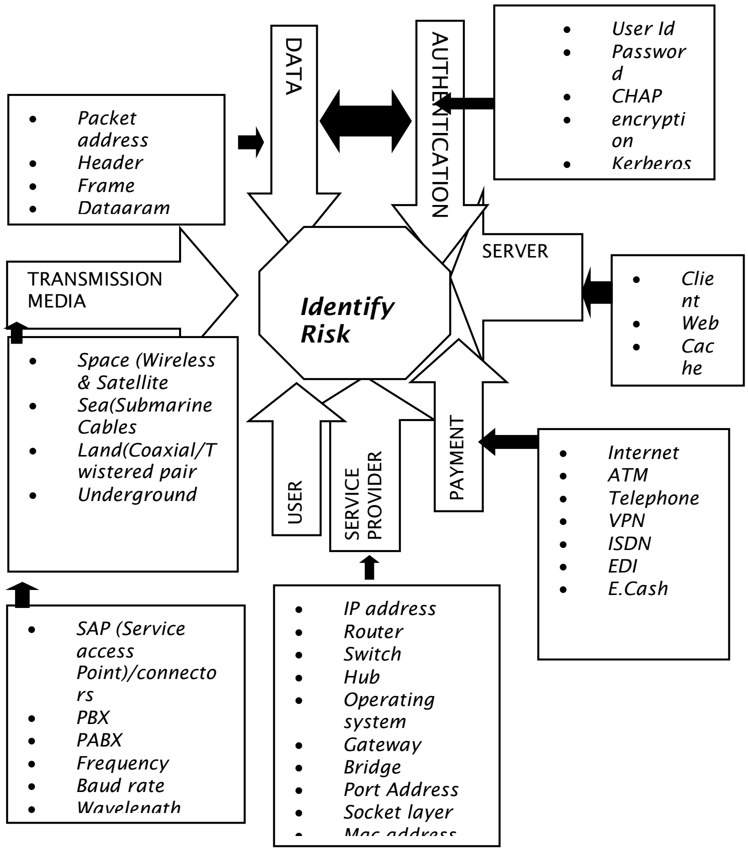


Figure 22 - LEVEL 1 - SSTM – (SERVICE SERVER TRANSMISSION MODEL) of Synchronizing E-Security

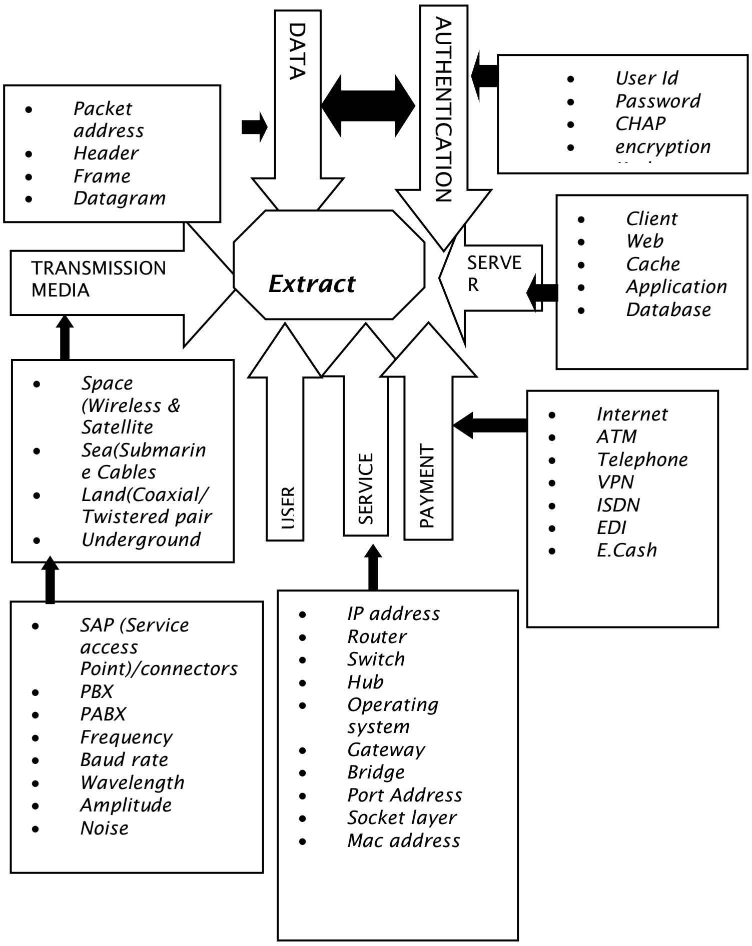


Figure 23 - LEVEL 2- SSTM – (SERVICE SERVER TRANSMISSION MODEL) OF Synchronizing E-Security

Z7	Z6	Z5	Z4	Z3	Z2	Z1	
IP-Address	Bandwith	Baudrate	Switch	Hub	Location	Skill	Z1
Router	Packet address	ATM	E-cash	EDI	VPN	Satellite	Z2
Wavelength	Earth station	VPN	OSS	E-Chip	Terminator	Gateway	Z3
USER	SAP	PBX	Cyphertext	Password	Socket layer	Repeater	Z4
Sec. Provider	Amplitude	Application	Profile	Cable/Wire	Connectors	Frame	Z5
Noise	ISP	Web Server	Dbase Server	Cache Server	Frequency	Router	Z6
Circuit	Protocol	Datagram	MAC address	Port address	SAP (Service Access Provider)	Client Server	Z7

Figure 24 - LEVEL 3 - (RIG) Risk Identification Grid

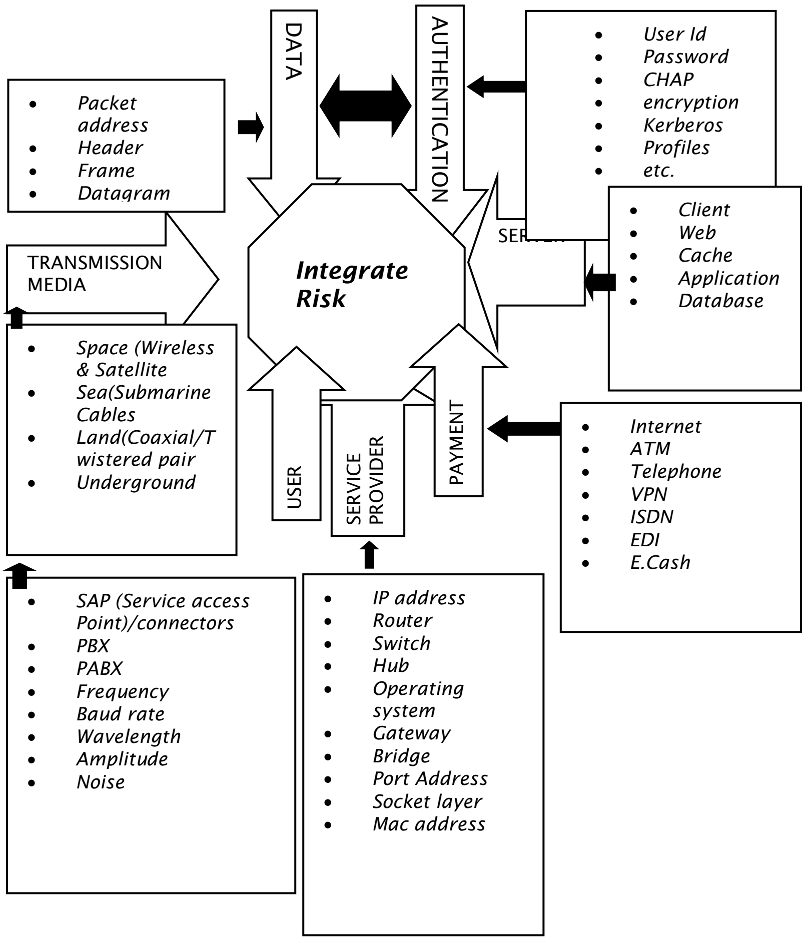


Figure 25 - LEVEL 4 – SSTM – (SERVICE SERVER TRANSMISSION MODEL) of Synchronizing E-Security

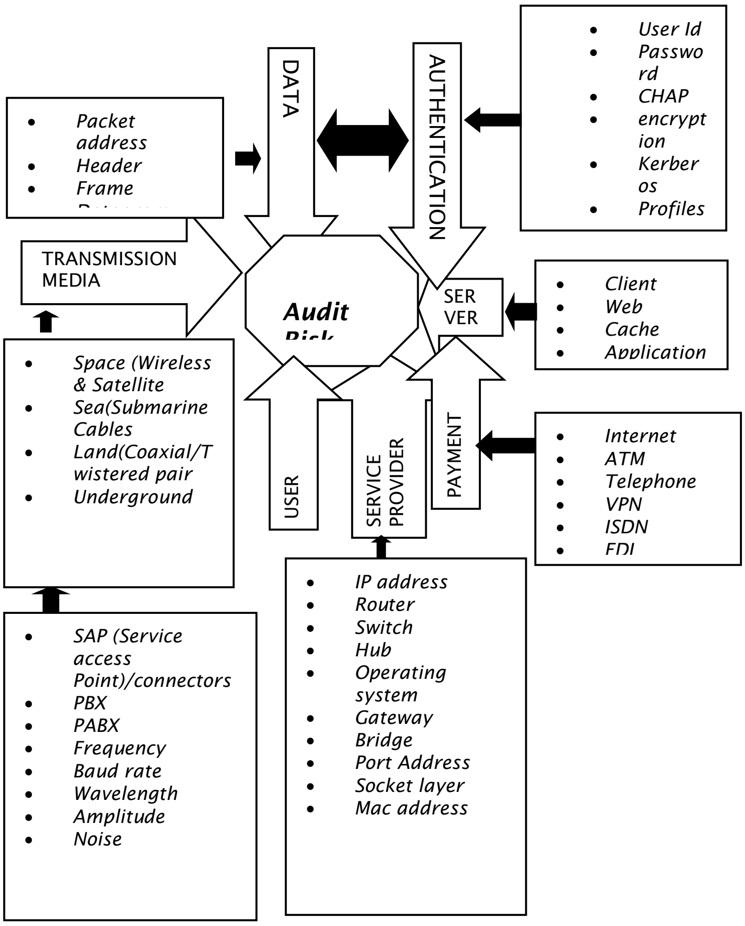


Figure 26 - LEVEL 5 – SSTM – (SERVICE SERVER TRANSMISSION MODEL) of Synchronizing E-Security

Z7	Z6	Z5	Z4	Z3	Z2	Z1	
IP-Address	Bandwith	Baudrate	Switch	Hub	Location	Skill	Z1
Router	Packet address	ATM	E-cash	EDI	VPN	Satellite	Z2
Wavelength	Earth station	VPN	OSS	E-Chip	Terminator	Gateway	Z3
USER	SAP	PBX	Cyphertext	Password	Socket layer	Repeater	Z4
Sec. Provider	Amplitude	Application	Profile	Cable/ Wire	Connectors	Frame	Z5
Noise	ISP	Web Server	Dbase Server	Cache Server	Frequency	Router	Z6
Circuit	Protocol	Datagram	MAC address	Port address	SAP (Service Access Provider)	Client Server	Z7

⬍

SOLUTIONS

Figure 27 - LEVEL 6 - (RISG) Risk Identification Solution Grid

11.6 Guidelines for using the model

- **Integrate risk preventive technologies**

It is essential that current technologies available for risk prevention should be available to both advanced and developing economies. There should be a clear understanding of importance associated with risk preventive technologies. The design aspects should also integrate characteristics that foresee risk from both developing and advanced economies perspectives. Software designed for risk prevention should have the capability to analyse risk factors that take into account socio cultural elements in developing economies. There is the need to adopt a context based approach to risk, by integrating such factors.

- **Prioritise global technology scheme**

Newly developed technologies should be based on schemes that address fundamental bottlenecks of risk preventive technologies. For instance examine whether training schemes that support technology take a holistic approach, by putting into perspective training needs of developing economies vis-à-vis advance economies.

- **Prioritise national and international funding for technologies**

Funding that support any form of technological development should be properly prioritised. The scale of preference of such prioritisation should be based on an understanding of the risk requirements in specific economies. The need for a context based approach is paramount and a critical success factor.

- **Verify premature distribution of hardware and software across the globe**

Manufacturing and distribution of hardware and software should not be executed prematurely. Vendors of hardware and software should verify whether products being marketed meet minimum security requirements such as the C2 classification of the orange books. The buyers of these technologies should revalidate and reassess whether the products being sold to them meet security requirements that are globally acceptable. A thorough examination of security features should be beta tested by the user.

- **Ensure that certification of software and hardware is satisfactory**

Certification should be managed and delivered thorough the appropriate set of controls or framework recommended and well understood by users. Certification should provide the assurance and trust that organisations need to forge ahead business security. Addressing and predicting uncertainties that might evolve in different environments should be embodied in security model implementation. The integrity of the certifier for information assurance should be verified.

- **Reconcile the disparities in skills of human ware within the environment the technology will be implemented.**

Train technical and non technical manpower that interact or communicate with the technology. Training is the engine to growth and sustainability. Most developing economies lack the necessary infrastructure to support in house training within organisations. There is also a lack of appreciation regarding the role that training play in developing personnel whether at operational, tactical or strategic level. Training schemes adopted within developing economies are more structured compared with advanced economies. Advanced economies therefore have the flexibility to easily adopt different trading models.

- **Refuse to be misdirected by the "Bandwagon syndrome"**

Do not be led. Take the lead in the introduction of any technology or information system. Before an introduction of new technology in your environment or organisation, a thorough assessment should be made to establish whether such a technology is required. The assessment can also determine the best strategy for optimising technical and non technical resources.

11.7 General concepts

This section introduces a number of concepts that explains the techniques and notations adopted by the models of the methodology. The following are concepts central to the methodology: (RAS) Risk Access Spots introduced as a footnote in section (RIG) Risk Identification Grid, (RISG) Risk Identification Solutions Grid and (Z) Zones.

11.7.1 Risk

An event that poses a threat or danger to a system. It is also the value or importance attached to a network vulnerability. Ben-David and T.Raz (2001) also define it as the exposure to the probability that an event with adverse consequences might occur.

11.7.2 (RAS) Risk Access Spots

RAS are areas of risk that could be perceived, actual or emerge as a hoax and may be vulnerable to threat or attack. Identifying RAS is the first level of the methodology. RAS are not permanent, although certain areas could be recommended as risk prone than others. RAS are dynamic and might not necessarily follow any particular pattern. The identification of RAS should be followed by risk extraction. Extracting the risk and documenting the risk is essential to providing solutions. The risk extracts are documented using the (RIG) Risk Identification Grid.

11.7.3 Zones

Zones are demarcated areas where risk could be perceived or emerge. Synchronising E-Security methodology proposes seven Zones as hypothetical risk regions. The proposition is based on the notion that RAS emerge at different levels of network and operating systems, which support international, national, city, town, company or organisation's electronic activity. The least divisible part of a zone is a node (n) on a communication network. A node has parameters or variables which are synchronized during synchronization. These include time, risk, event and attack history.

A zone can also comprise many processes. This could be represented as, $Z=(P_1.......P_n)$, where P is a process in a zone and P_n. is infinite number of processes. Every zone (z) is associated with both physical and logical clock, which is a characteristic of most synchronization primitives and algorithms. The logical clock is a derivative of physical clock in any geographical location. The physical clocks are adjusted due to drift times and rates associated with physical clocks. Each process in a zone is responsible for reading risks® associated with that process. In order words, there is one to one, one to many, or many to many relationships between zones (z) and processes

11.7.4 RIG) Risk Identification Grid

RIG is a two-dimensional array grid comprising RAS and (Z) Zones. The risk access spots identified on RIG is integrated. The purpose of the integration is to determine common and non-common risk amongst the seven Zones in the RIG which represent network and operating system platforms in any geographical region. The process of risk integration is followed by a risk audit, which creates a synthesis of perceived and actual risk. Solutions are then provided for the actual risk whiles contingencies are put in place to monitor the perceived risk using the RISG. An expert or the proposed simulator in this text could be consulted to deal with the RAS documented in the RIG. The concepts that drive Synchronising E-Security Methodology have been modelled using (SSTM) Service Server Transmission Model.

Z7	Z6	Z5	Z4	Z3	Z2	Z1	
IP-Address	Bandwith	Baudrate	Switch	Hub	Location	Skill	Z1
Router	Packet address	ATM	E-cash	EDI	VPN	Satellite	Z2
Wavelength	Earth station	VPN	OSS	E-Chip	Terminator	Gateway	Z3
USER	SAP	PBX	Cyphertext	Password	Socket layer	Repeater	Z4
Sec. Provider	Amplitude	Application	Profile	Cable/Wire	Connectors	Frame	Z5
Noise	ISP	Web Server	Dbase Server	Cache Server	Frequency	Router	Z6
Circuit	Protocol	Datagram	MAC address	Port address	SAP (Service Access Provider)	Client Server	Z7

Figure 28: RIG- Risk Identification Grid – Level 3 of SSTM

11.7.5 Local zone

The location refers to a network area within a radius of 100meters. It is location where an event or attack takes place within the 100meters radius.

11.7.6 Global zone

A network area or radius which is outside 100 meters demarcation
This covers all locations affected due to an event or attack on a local zone.

11.7.8 Zone Grading

A zone is graded at different threat or risk levels as a result of an association with a RAS within a zone. For example networks deployed in developing economies within the larger context of global network infrastructure, such as the Internet suffer a higher risk. This make such networks pose more danger to global networks. Risks associated with RAS are graded as 1,2,3 where 1 is Low, 2 is medium and 3 is High. It is important to note that a RAS graded as 1 in a particular zone could be graded as 3 in another zone. This primarily depends on location, although there are other factors that come to play.

11.7.9 Sync

Sync represents α (alpha) as the synchronisation primitive that manages the asynchronous nature of risks and attacks on computer networks located at different zones.

11.7.10 Time

The time an attack or event took place. This is important since time zones vary globally, as such capturing the time of such an attack or event is essential to profiling when such attacks and events are likely to take place. Whiles a physical time is derived from a physical clock in a geographical location. A logical time is derived from a logical clock.

11.7.11 Event

An event is any system activity that is likely to generate a system response, although not all responses from the system is visible or measurable by a computer security management system. It is also an anomaly to system activities. This book takes the view that events can be generated accidentally or deliberately. An event also triggers a computer network or system response, visible and non visible to a network administration and management system and associated with a **RAS**.

11.7.12 Attack

Any activity that exploits risk access spots with the goal of breaching security. An attack is an event with catastrophic consequences, whether deliberate or accidental. Its source may be known or concealed. The nature of a network attack is analogous to an act of war. It has no pre-defined rules like a road traffic system. Its demographic relationship is not correlated. However there are functional variables when captured could serve as a guide to expected attacks, based on risks whether known or unknown.

11.7.13 (RISG) – Risk Identification Solutions Grid

Risk Identification Solutions Grid denotes mapping between risk access spots identified within the zones and recommended solutions, which in some cases could be described as countermeasures prescribed to mitigate the risk flagged to be a threat or danger. The RISG is the point where the outcome of the risk assessment is integrated with appropriate security solutions embedded within the RISG Simulator. The countermeasures or solutions drawn can also originate from a human expert as part of the solutions that the RISG simulator provides.

Risk Identification Solution Grid Level 6

	Z1	Z2	Z3	Z4	Z5	Z6	Z7
Z1	Skill	Satellite	Gateway	Repeater	Frame	Router	Client Server
Z2	Location	VPN	Terminator	Socket layer	Connectors	Frequency	SAP (Service Access Provider)
Z3	Hub	EDI	E-Chip	Password	Cable/ Wire	Cache Server	Port address
Z4	Switch	E-cash	OSS	Cyphertext	Profile	Dbase Server	MAC address
Z5	Baudrate	ATM	VPN	PBX	Application	Web Server	Datagram
Z6	Bandwith	Packet address	Earth station	SAP	Amplitude	ISP	Protocol
Z7	IP-Address	Router	Wavelength	USER	Sec. Provider	Noise	Circuit

SOLUTIONS

Figure 29: Level 6 of SSTM- (RISG) Risk Identification and Solution Grid

11.8 Symbolic and mathematical notations

This section presents a mathematical model and notations underlying SSTM (Service Server Transmission Model) as well as general description of the model. There are six levels which form the implementation section and process of the models linked to the methodology.

1. Lest Risk notations be represented as:

r = risk

Ir = risk identification

Er = risk extraction

Ir → Er = RIG (Risk Identification Grid)

Int = risk integration (common & uncommon risk)

2. Let Synchronisation primitive be represented as Sync = α

3. Let Time & Event Notations be represented as:

t = time
e = event
z =local zone
Z = Global zone
γ= attack

4. Generic relational notations

We present the relationship between r, x, y, z, Z, γ ***as***

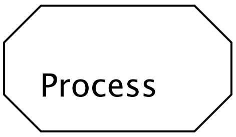
$\alpha = r \rightarrow t \rightarrow e \rightarrow z \rightarrow Z \rightarrow \gamma$ or $r \cap t \cap e \cap z$

5. We represent $z \rightarrow Z$ ***as*** $z \subseteq Z$ (z is a subset Z) and $z \subset Z$ (not a proper subset of Z)

6. According to SSTM Probability of risk r is calculated as
$P_B = ((Z^n) + \text{time } t + \text{event } e) \times \text{sync } \boldsymbol{\alpha}$ **/ cost**
Global and Local Zones are identified using a location and profile based algorithm engineered from the model. The model defines parameters and criteria for locating risk, threat and possible attack.

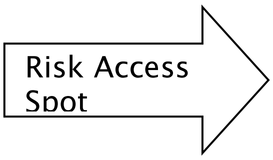
11.9 Graphical notations

1.



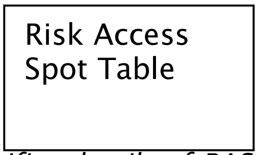
Security risk analyser and processor

2.



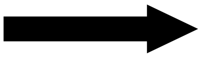
Security risk access spot indicator

3.



Specifies details of RAS (Risk Access Spots) indicated by risk access spot flow diagram

4.



Risk Access Spot flow

11.10 Summary

This chapter provided an insight into the risk spots and security vulnerabilities of information systems that support Online Business and electronic based transactions. The methodology proposed highlights the fact that there are risk access spots that need to be identified in the development process of such systems. It also suggests the need to determine perceived risk and actual risk. Although the risks identified are of critical importance to such systems, the risk areas could evolve or change. The underlying mathematical model is applied to electronic business cases with regards to on-line banking and results presented in chapter 9.

The chapter also described details of concepts and notations underpinning SSTM. The Concepts and notations described comprised, risk,(r) , RAS (Risk Access Spots), Zones, which represents Locations on a network. Zones can be local or global.

They are graded as 1, 2 and 3 meaning low, medium and high levels. RIG (Risk Identification Grid) for integrating risk .extracted during risk assessment. Factors essential to synchronization process were outlined. These include time, event and attack, as well as the Zone. RISG (Risk Identification and Solutions Grid) a tabulation of recommended solutions for the security risk problem identified in RIG was also presented. A subsection of the chapter recaptured guidelines for implementing SSTM.

Chapter 12

Simulation using Monte Carlo

12.1 Introduction

This chapter provides a simulation of SSTM Security Model with respect to **TRAP** (*Threats, Risks, Attacks and Preparedness)* of online systems using the concept of Monte Carlo with respect to case scenarios. The purpose of the simulations is to assess the reliability and trustworthiness of the model in assessing security risk on online systems and the range of infrastructure that support them for Business Security for heterogeneous and hetero-standard systems with respect to communication networks using Monte Carlo method.

12.2 General problem scenario

In this scenario we will attempt to predict possible events likely to occur using SSTM and verify them by Monte Carlo method.

The general problem scenario is based on the following set of questions:

1. How is the security of an organisation with a local and global network
infrastructure assessed?

2. How do such risks threaten the confidentiality, integrity and availability of its information services?

3. Supposing an activity on a network with parameters x_1 to x_n is identified in a particular geographical location of the network platform, what will be the probability of risk?

The need to model and simulate security risks across such network platforms strengthens our understanding of sources and nature of risks faced by organisations which have local, metropolitan and global business presence.

12.3 Overview of Monte Carlo

Monte Carlo is a method for risk analysis and uncertainty. It simulates real life systems. Monte Carlo uses random numbers and probability to evaluate structured and non structured problems. Monte Carlo method has been used extensively for modelling and simulating problems similar to the model being tested, due to its ability to randomise set of activities. In general, the steps involved in Monte Carlo simulation are as follows:

1. Create a parameter based model

   - A model is created comprising parameters or attributes of the model being built. This can be represented in mathematical form as security risk = f(x), where f(x) is a function with elements
     x_1 to x_n

2. Create a set of random inputs (x_i1, x_i2, x_i3 x_i4 x_i n)

   - Different security risk scenarios are generated for input into the model being simulated

3. Test the model

   - Model is tested using input variables

4. Save the results from the testing

   - Results from the test is saved for comparative analysis

5. Analyse the results to establish confidence in the solution model

   - Results are compared to other solutions models to establish significance of model

6. Repeat test for model

1000 security risk scenarios have been randomly generated as part of an experiment to evaluate SSTM. A random number in the series represents a security risk scenario.

12.4 Methodology for testing SSTM

12.4.1 Research method

The method applied in simulating the model is Monte Carlo.

12.4.2 Sources of Data

Initial sources of data for simulation have been extracted from the following sources:

Risk Identification Grid (RIG) based on empirical studies Williams (2004).

Analysis of RAS generated using SSTM from case studies

(Reliable sources)

12.4.3 Factors likely to affect outcome of analysis on risk access spot.

12.4.3.1 Types of data variables

- Time (local, global)
- Event (local, global)
- Attack (local, remote)
- Zone - Geographical location

12.4.4 Sensitivity Analysis

A method for refining data gathered through the fact finding exercise identifying factors critical to network security.

12.4.5 Fact finding methods applied

Observation
Document sampling (independent records)
Interviews
Case studies
Empirical studies

12.4.6 Factors considered in determining accuracy of data collected

Pessimistic and optimistic views expressed by personnel providing information about existing network infrastructure. Security policy of governments is a useful source of data if available.

12.5 Application of SSTM in Case studies

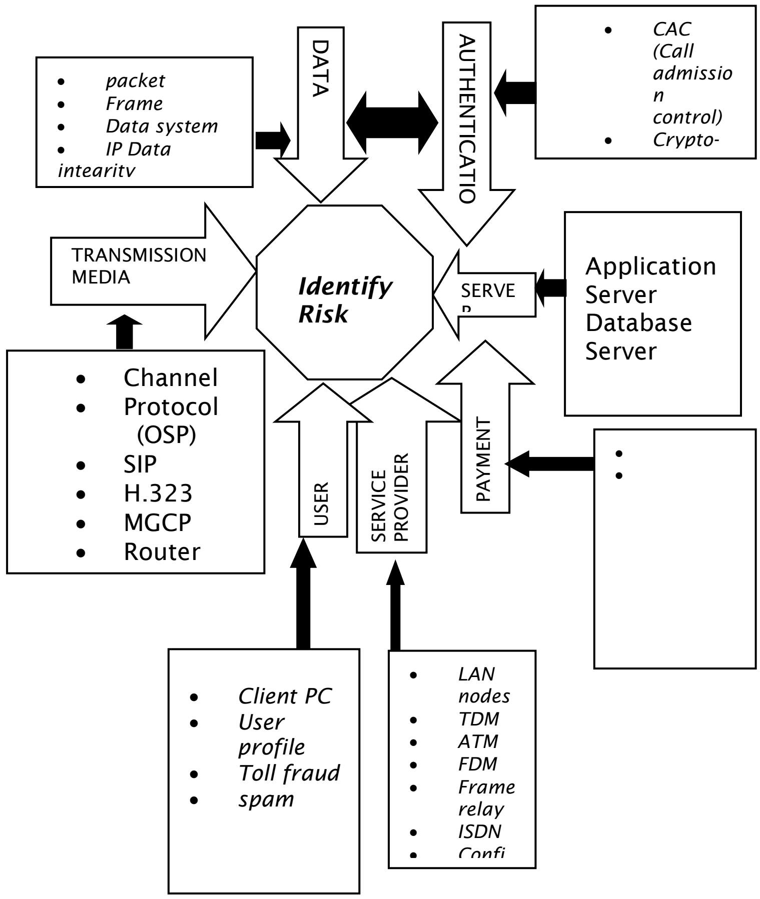
This section is a description of case scenarios where SSTM has been applied in real life environments. The section illustrates the application of the model in security risk assessment. Due to data protection and security requirements of the companies which volunteered for this study, some companies' names have been changed.

(CASE 1) - **Joint Logic Ltd VoIP**

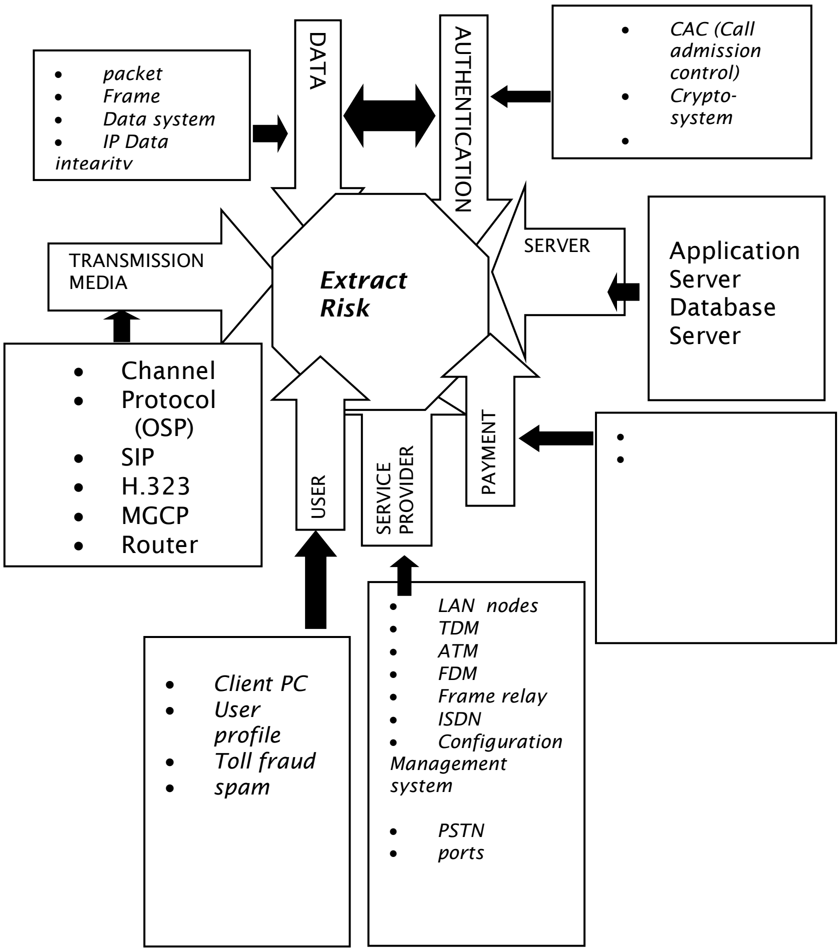
Joint Logic Ltd introduced Voice over IP(VoIP). There have been concerns with regards to security. In a more general sense this is how the company's VoIP work. Voice over Internet Protocol (VoIP) is a technology that enables phone calls using the Internet. It virtually costs nothing. The Internet transfers information in the form of packets. In other words it is a packet switching system. Supposing there are two points of communication on the Internet called points A and B, the data sent from A to B is broken down into packets. The address of B is then added to the start of each packet. The packet-switching network despatches the packets to B by any route accessible on the network. Since each packet has the identifier of the intended destination, a single communication channel can carry packets from different sources to different destinations. VoIP converts the sound which is analogue to digital data. This digital signal (DATA) is placed into packets for subsequent transmission on the Internet.

Although this technology is cheaper and is likely to be more efficient in the future, there are a number of issues and challenges that have not yet been overcome. Some of these issues are: Sound quality (The effect of noise and attenuation), Jitter (The variation in the time between packets arriving), Latency (The delay on a phone line) and Security. The company showed concerns with regards to confidentiality, integrity and availability of data. The company desires that such fears are alleviated before it gets out of hand. The company requires a risk assessment of this technology. The VoiP architecture formed the bedrock of this assessment.

LEVEL 1 – Identify Risk



LEVEL 2- Extract Risk

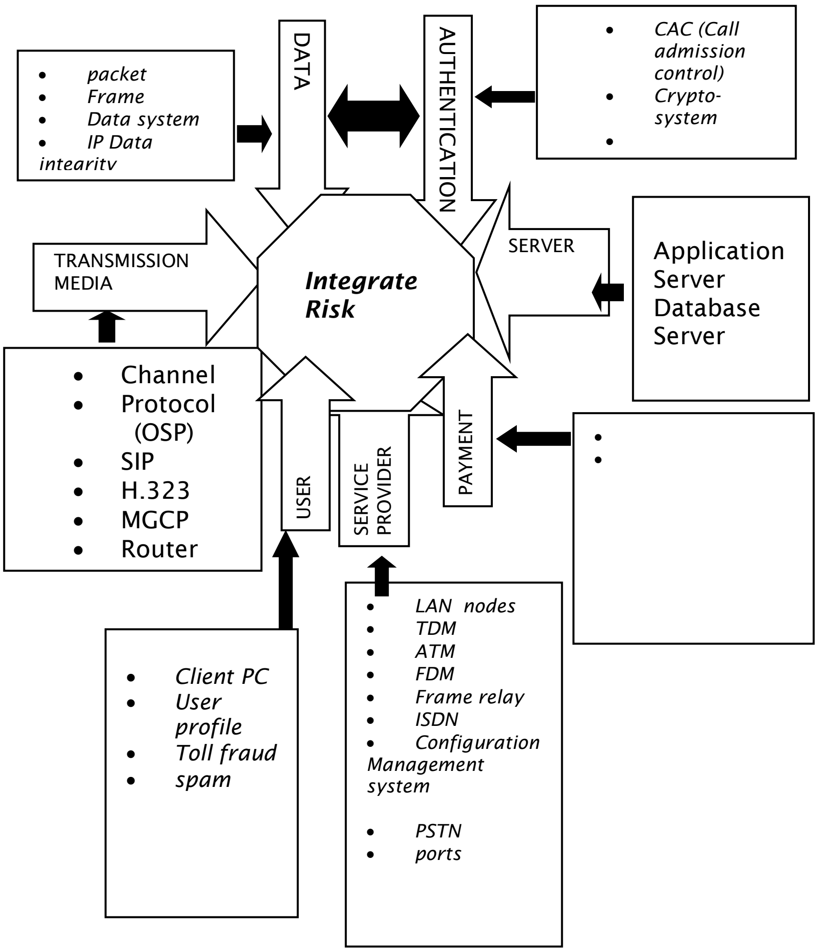


LEVEL 3 - (RIG) Risk Identification Grid

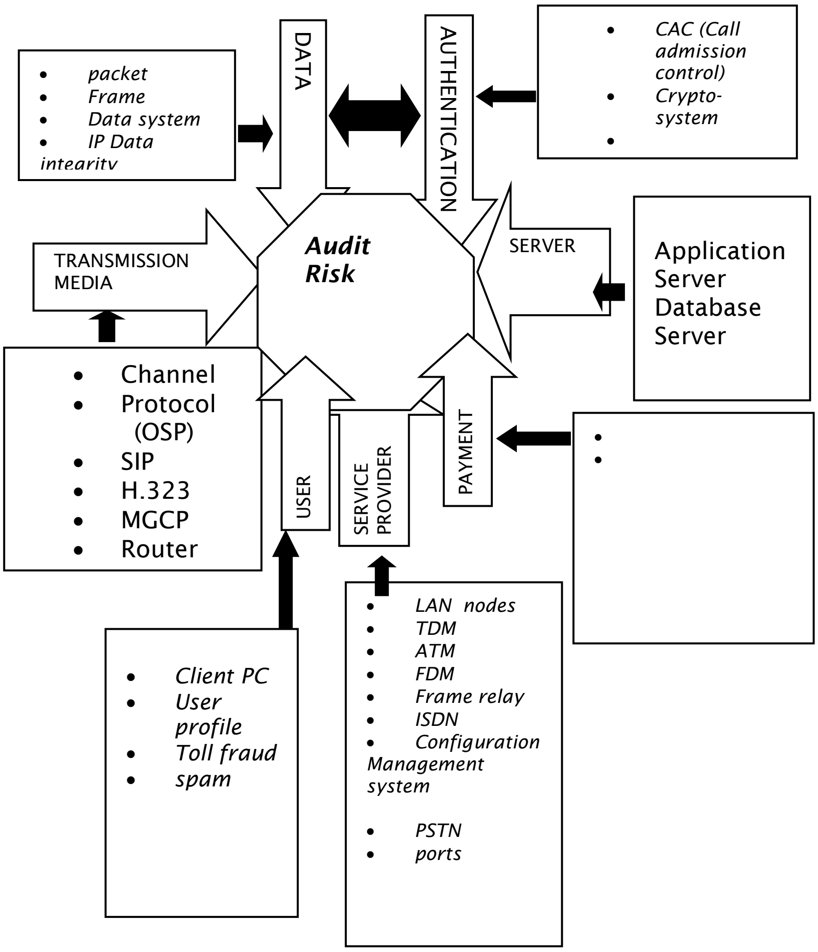
	Z1	Z2	Z3	Z4	Z5	Z6	Z7
Z1	Packet	Channel	Client PC	LAN Modes	Application Server	CAC	
Z2	Frame	Protocol	User Profile	TDM	Database Server	Crypto system	

Z7	Z6	Z5	Z4	Z3
			IP datagram	Data System
	Router	MGCP	H.323	SIP
		Ports	Spam	Toll Fraud
PSTN	Configuration System	ISDN	Frame relay	ATM

LEVEL 4 – Integrate Risk


Integrate Risk
DATA
AUTHENTICATION
TRANSMISSION MEDIA
SERVER
USER
SERVICE PROVIDER
PAYMENT
packet
Frame
Data system
IP Data intearitv
CAC (Call admission control)
Crypto-system
Application Server Database Server
Channel
Protocol (OSP)
SIP
H.323
MGCP
Router
Client PC
User profile
Toll fraud
spam
LAN nodes
TDM
ATM
FDM
Frame relay
ISDN
Configuration Management system
PSTN
ports

Level – 5 Audit Risk



LEVEL 6 - (RISG) Risk Identification Solution Grid

Z6	Z5	Z4	Z3	Z2	Z1	
		IP datagram	Data System	Frame	Packet	Z1
Router	MGCP	H.323	SIP	Protocol	Channel	Z2
	Ports	Spam	Toll Fraud	User Profile	Client PC	Z3
Configuration System	ISDN	Frame relay	ATM	TDM	LAN Modes	Z4
				Database Server	Application Server	Z5
				Crypto system	CAC	Z6
						Z7

Z7

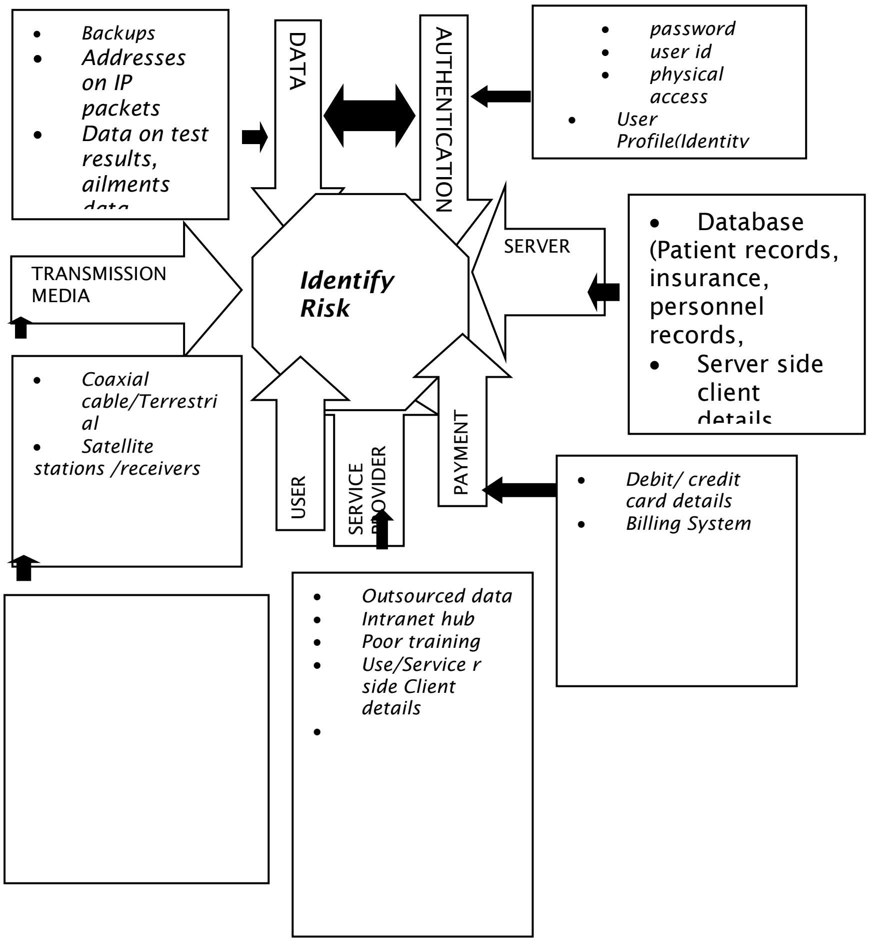
PSTN

SOLUTIONS

(CASE 2) - **James Brown Healthcare (JBH)**

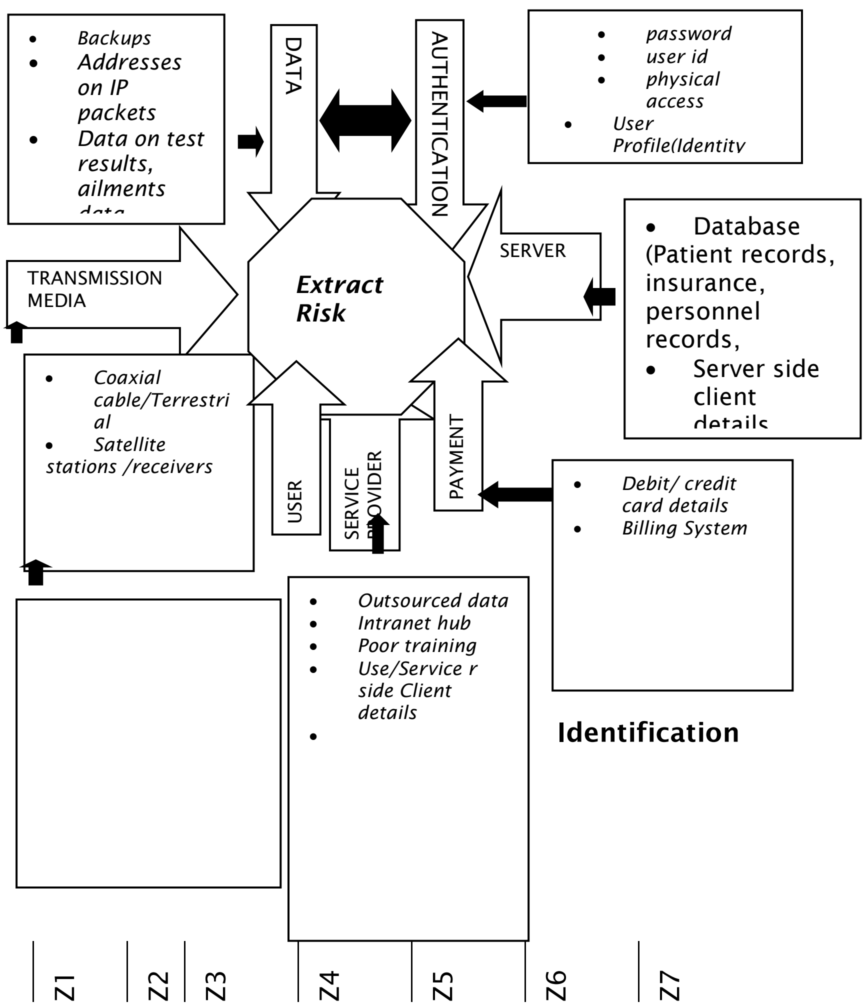
James Brown Healthcare (JBH) Technologies provides clinical and diagnostic workflow software and Internet services for pathology, laboratory and radiology services enabling collaboration among physicians and clinicians and care settings. Recently James Brown Healthcare has decided to move into the Application Service Provider (ASP) market; with the objective that they will have the capability to offer securely delivered clinical data and applications to physicians, hospital workers and clients anywhere in the world via the internet. As both a software vendor and ASP, JBH has taken a proactive approach to contract a security consulting firm to assess the risk that will enable them achieve JBH security goals.

LEVEL 1 – Identify Risk



Backups
Addresses on IP packets
Data on test results, ailments data
DATA
AUTHENTICATION
password
user id
physical access
User Profile(Identity
TRANSMISSION MEDIA
Identify Risk
SERVER
Database (Patient records, insurance, personnel records,
Server side client details
Coaxial cable/Terrestrial
Satellite stations /receivers
USER
SERVICE PROVIDER
PAYMENT
Debit/ credit card details
Billing System
Outsourced data
Intranet hub
Poor training
Use/Service r side Client details

LEVEL 2- Extract Risk


Backups
Addresses on IP packets
Data on test results, ailments data
DATA
AUTHENTICATION
password
user id
physical access
User Profile(Identity
TRANSMISSION MEDIA
Extract Risk
SERVER
Database (Patient records, insurance, personnel records,
Server side client details
Coaxial cable/Terrestrial
Satellite stations /receivers
USER
SERVICE PROVIDER
PAYMENT
Debit/ credit card details
Billing System
Outsourced data
Intranet hub
Poor training
Use/Service r side Client details
Z1
Z2
Z3
Z4
Z5
Z6
Z7

LEVEL 3 - (RIG) Risk Grid

Identification

Z7	Z6	Z5	Z4	Z3	Z2	Z1
			Storage Policy	Medical Data	IP address	Backups
			Transmitte	Receivers	Satellite	Coaxial
						Outsourced data
				Billing System	Credit cards	Debit cards
			User Profile	Physical Access control	User id	passwords

LEVEL 4 – Integrate Risk

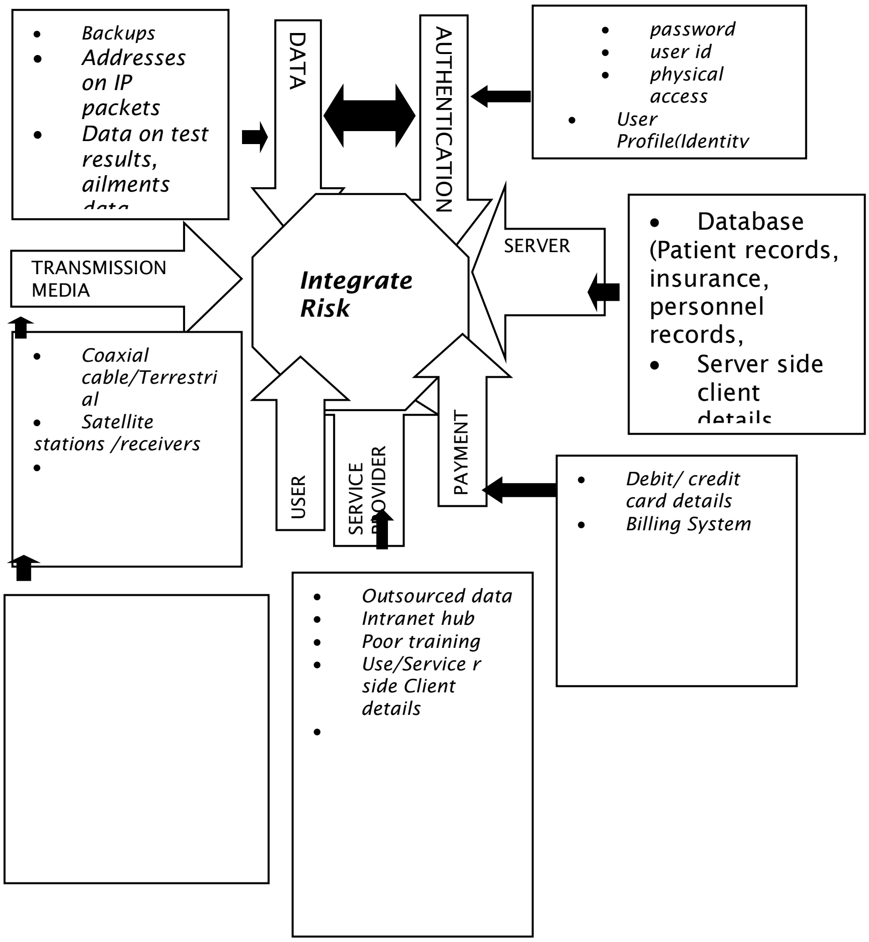
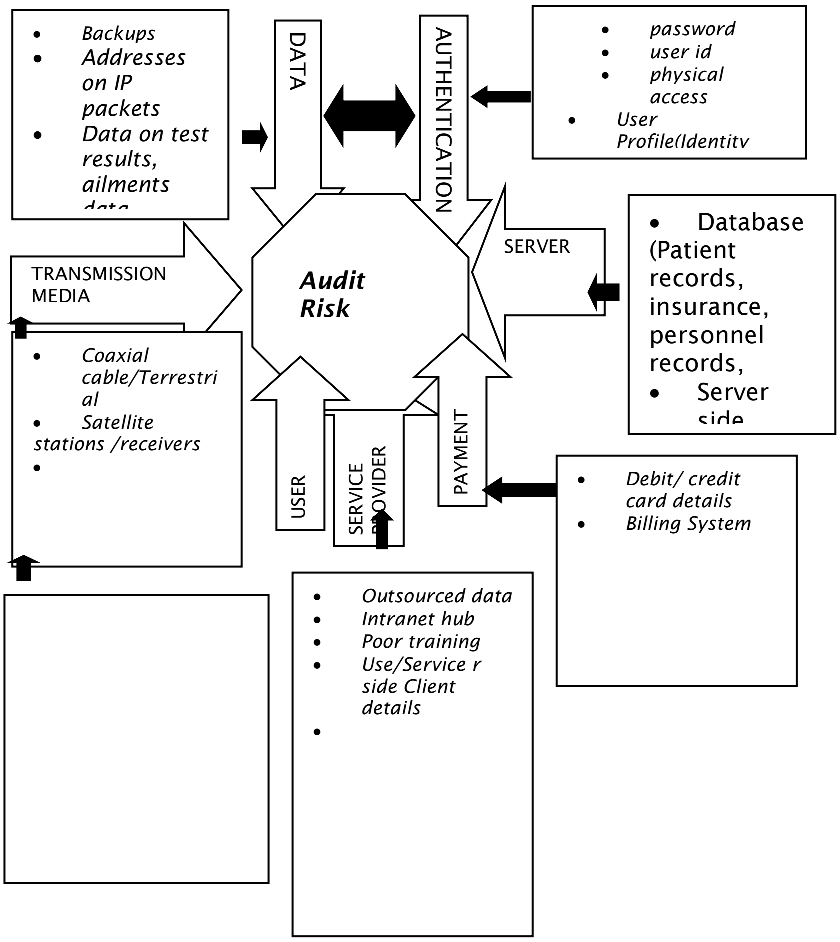


Figure 4

LEVEL 5 – Audit Risk



- *Backups*
- *Addresses on IP packets*
- *Data on test results, ailments data*

DATA

AUTHENTICATION

- *password*
- *user id*
- *physical access*
- *User Profile(Identity*

TRANSMISSION MEDIA

Audit Risk

SERVER

- Database (Patient records, insurance, personnel records,
- Server side

- *Coaxial cable/Terrestrial*
- *Satellite stations /receivers*

USER

SERVICE PROVIDER

PAYMENT

- *Debit/ credit card details*
- *Billing System*

- *Outsourced data*
- *Intranet hub*
- *Poor training*
- *Use/Service r side Client details*

Figure 4

LEVEL 6 - (RISG) Risk Identification Solution Grid

	Z1	Z2	Z3	Z4	Z5	Z6	Z7
Z1	Backups	Coaxial	Outsourced data	Debit cards	passwords		
Z2	IP address	Satellite		Credit cards	User id		
Z3	Medical Data	Receivers		Billing System	Physical Access control		
Z4	Storage Policy	Transmitte			User Profile		
Z5							

Z6							
Z7							

SOLUTIONS

(CASE 3)- **Sahara Ltd Internet Service Provider (ISP)**

"Sahara" is a medium-sized consultancy company with a strong focus on the development of specialist software solutions for their clients. Most clients are companies and institutions with specific structure or non-standard business models that off-the-shelf software (such as a standard ERP system) does not cater for. Typical clients are the governmental tax office, customs offices, police departments, and banks. These clients have strong requirements with respect to the security of their information flow. Clients pay for consultancy and a fee for the software installation at their premises.

Recently, Sahara decided to study a new business model for their company. They have decided to sell services instead of the software. This means that the software is not installed at the client's site, but that it is installed (and maintained) at Sahara’s computer centre. The client uses the Internet to connect to and use these services. This approach has many advantages, most important of which is the long-term business relation between Sahara and it’s clients. Other advantages are: ease of maintenance, sharing of code (e.g. all police departments run the same software with their own data space), guaranteed with respect to performance, availability, security and continuity planning.

Up till now, Sahara had no security model but the management is aware of the potential danger of using the Internet as a go-between. They request a couple of external security experts to study all security risks issues involved in this new business model.

LEVEL 1 – Identify Risk

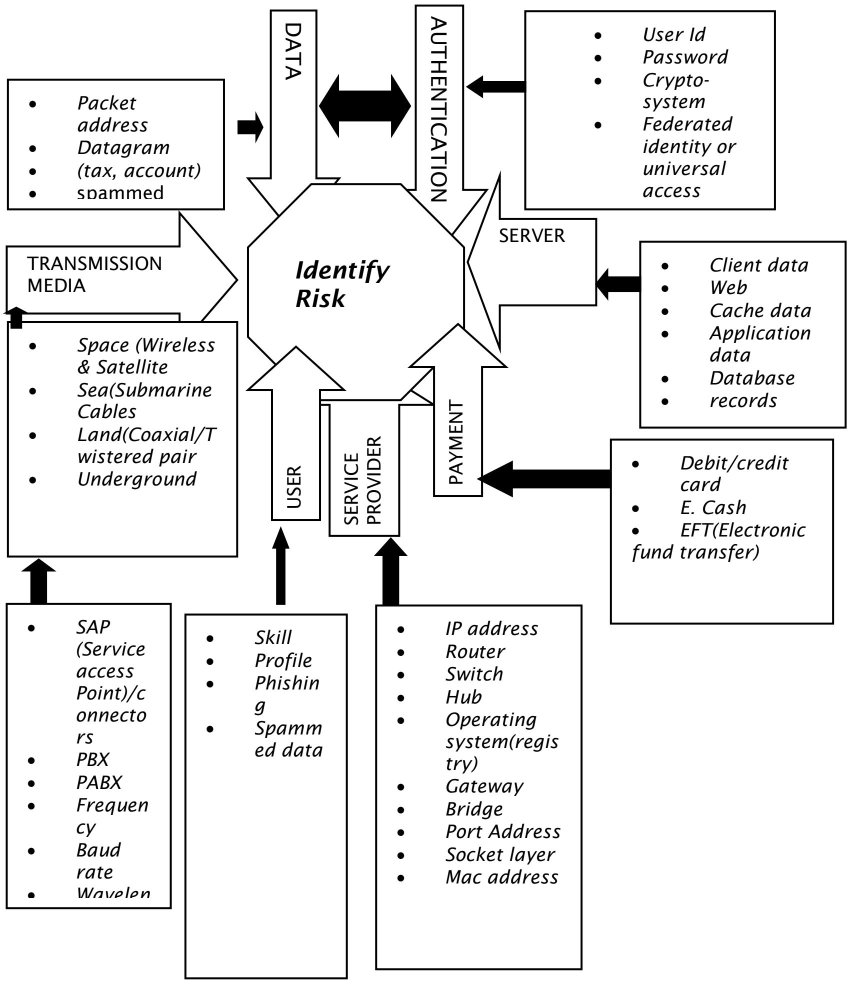

Identify Risk
DATA
AUTHENTICATION
TRANSMISSION MEDIA
SERVER
USER
SERVICE PROVIDER
PAYMENT
Packet address
Datagram
(tax, account)
spammed
User Id
Password
Crypto-system
Federated identity or universal access
Client data
Web
Cache data
Application data
Database
records
Space (Wireless & Satellite
Sea(Submarine Cables
Land(Coaxial/Twistered pair
Underground
Debit/credit card
E. Cash
EFT(Electronic fund transfer)
SAP (Service access Point)/connectors
PBX
PABX
Frequency
Baud rate
Wavelen
Skill
Profile
Phishing
Spammed data
IP address
Router
Switch
Hub
Operating system(registry)
Gateway
Bridge
Port Address
Socket layer
Mac address

Figure 4

LEVEL 2- Extract Risk

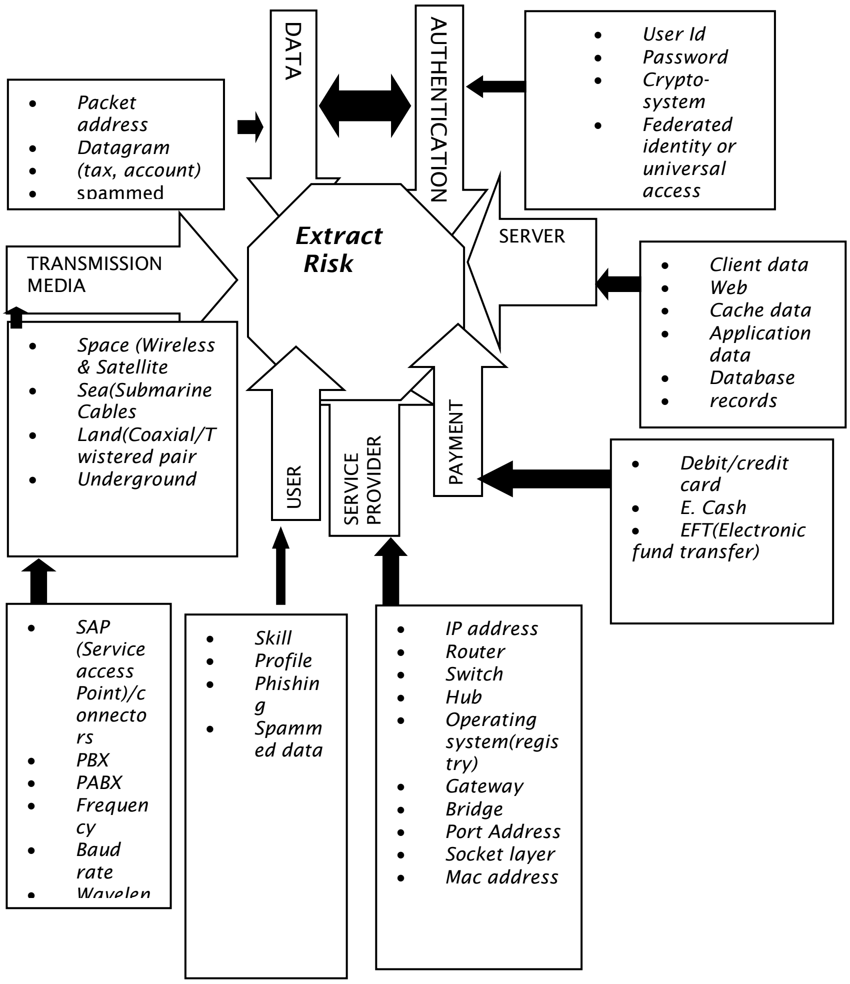


Figure 4

LEVEL 3 - (RIG) Risk Identification Grid

Z7	Z6	Z5	Z4	Z3	Z2	Z1	
IP-Address	Bandwith	Baudrate	Switch	Hub	Location	Skill	Z1
Router	Packet address	ATM	E-cash	EDI	VPN	Satellite	Z2
Wavelength	Earth station	VPN	OSS	E-Chip	Terminator	Gateway	Z3
USER	SAP	PBX	Cyphertext	Password	Socket layer	Repeater	Z4
Sec. Provider	Amplitude	Application	Profile	Cable/ Wire	Connectors	Frame	Z5
Noise	ISP	Web Server	Dbase Server	Cache Server	Frequency	Router	Z6
Circuit	Protocol	Datagram	MAC address	Port address	SAP (Service Access Provider)	Client Server	Z7

LEVEL 4 – Integrate Risk

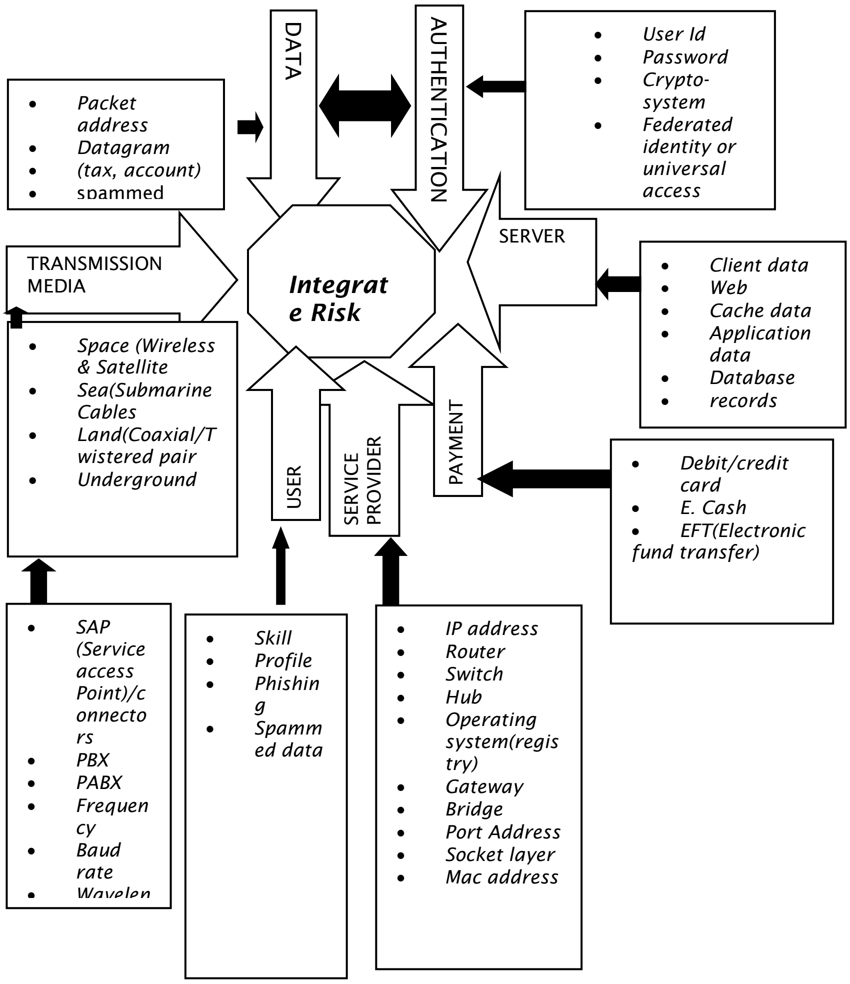


Figure 4

LEVEL 5 – Audit Risk

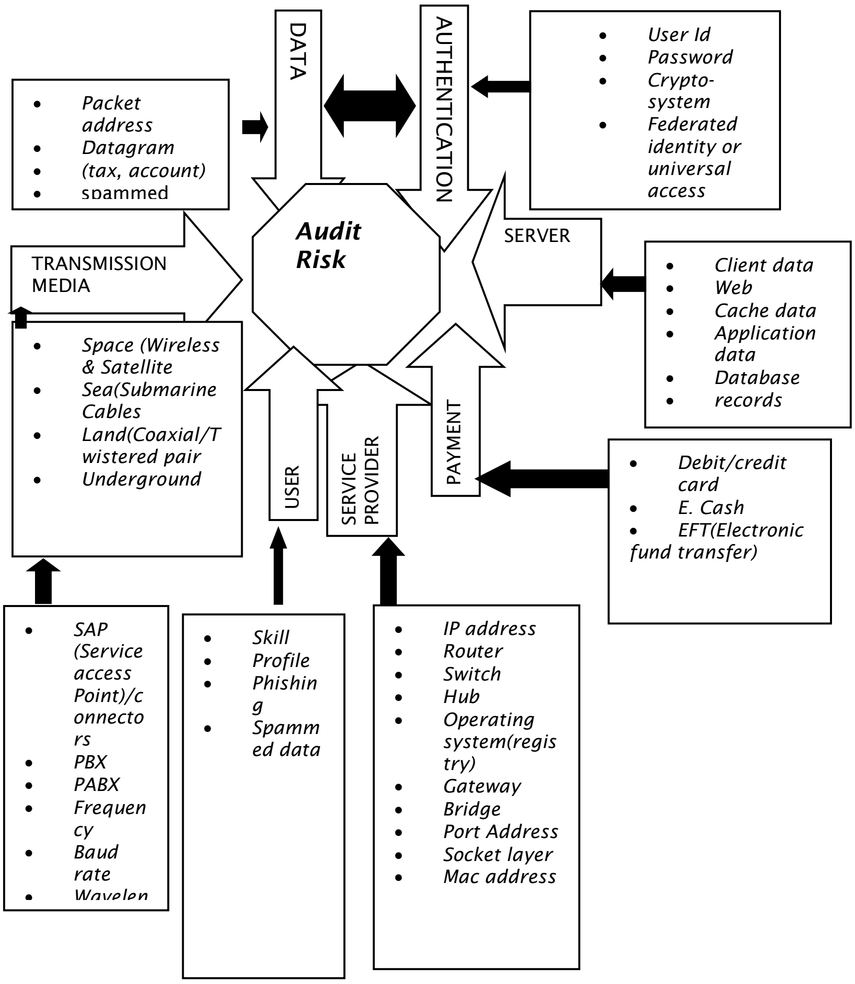

Audit Risk
DATA
AUTHENTICATION
SERVER
TRANSMISSION MEDIA
USER
SERVICE PROVIDER
PAYMENT
• Packet address
• Datagram
• (tax, account)
• spammed
• User Id
• Password
• Crypto-system
• Federated identity or universal access
• Client data
• Web
• Cache data
• Application data
• Database
• records
• Space (Wireless & Satellite
• Sea(Submarine Cables
• Land(Coaxial/Twistered pair
• Underground
• Debit/credit card
• E. Cash
• EFT(Electronic fund transfer)
• SAP (Service access Point)/connectors
• PBX
• PABX
• Frequency
• Baud rate
• Wavelen
• Skill
• Profile
• Phishing
• Spammed data
• IP address
• Router
• Switch
• Hub
• Operating system(registry)
• Gateway
• Bridge
• Port Address
• Socket layer
• Mac address

Figure 4

LEVEL 6 - (RISG) Risk Identification Solution Grid

	Z1	Z2	Z3	Z4	Z5	Z6	Z7
Z1	Skill	Satellite	Gateway	Repeater	Frame	Router	Client Server
Z2	Location	VPN	Terminator	Socket layer	Connectors	Frequency	SAP (Service Access Provider)
Z3	Hub	EDI	E-Chip	Password	Cable/ Wire	Cache Server	Port address
Z4	Switch	E-cash	OSS	Cyphertext	Profile	Dbase Server	MAC address
Z5	Baudrate	ATM	VPN	PBX	Application	Web Server	Datagram
Z6	Bandwith	Packet address	Earth station	SAP	Amplitude	ISP	Protocol
Z7	IP-Address	Router	Wavelength	USER	Sec. Provider	Noise	Circuit

SOLUTIONS

(CASE 4) – **Electronic Payment system in Sudan**

This case assesses the feasibility of the implementation of electronic payment system in Sudan by conducting a risk assessment on existing infrastructure, looking at the human and organisational factors among stakeholders. The field studies were carried jointly with Hesham my postgraduate dissertation student.

CASE STUDY – Electronic payment System in Sudan (Feasibility assessment using SSTM risk assessment and security model)

Introduction

The overall banking policy between 1999 and 2002 of the Central Bank of Sudan considered computerising the banking sector to be the fundamental part of the policy, as a response to the millennium bug in year 2000. The level of computerization prior to this stage was the responsibility of individual banks. As part of this banking sector policy it was compulsory for these standard measures to be implemented. Mr. Sabir Mohamed Al-Hassan (The Governor of the Central Bank) stated that: "The Central Bank compelled the commercial banks to connect their branches through networks. The Central Bank also completed the infrastructure required to connect the commercial banks with the central bank. It is now possible for a customer to check his or her account, or have a transaction processed from any branch.

A report issued by the Central Bank of Sudan in 2006 assessing the performance of the central bank of Sudan indicates that banking technology has been an essential part of the control process. It also reported that the use of the magnetic cheque has improved and simplified financial transactions.

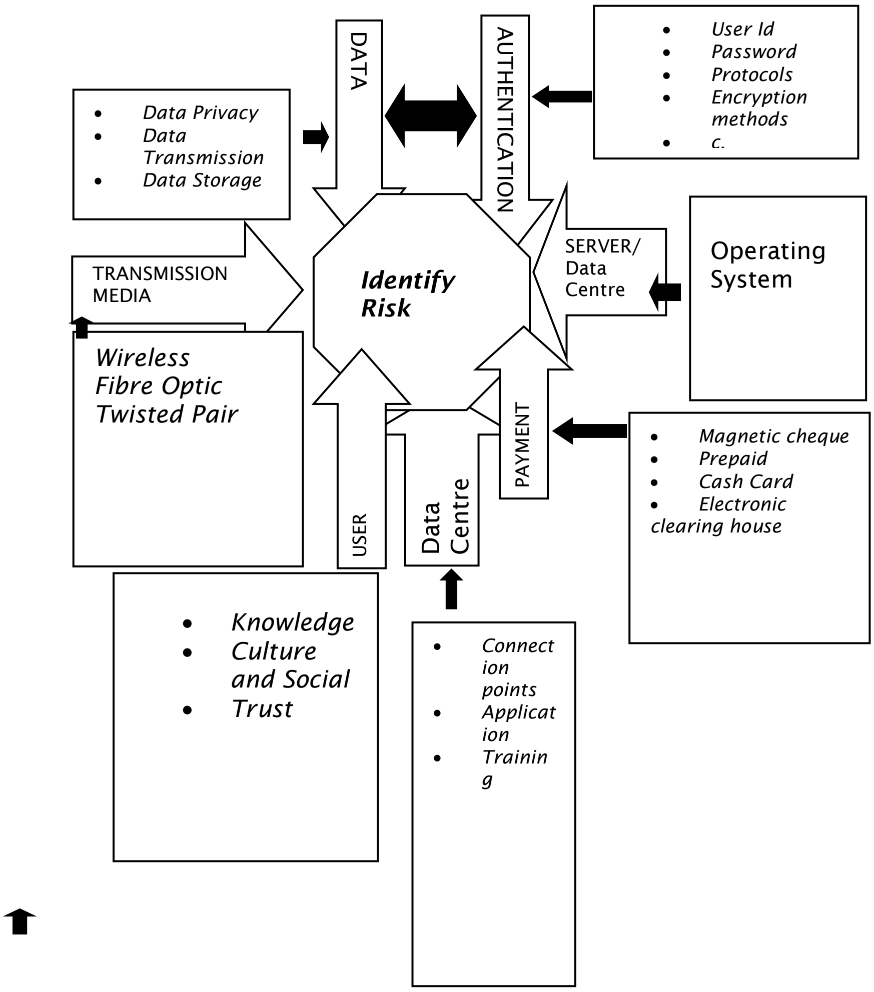
The challenges faced by the Central Bank of Sudan were mainly economical, cultural or technical. As part of the feasibility studies risk assessment was carried out using SSTM.

Results from fact finding

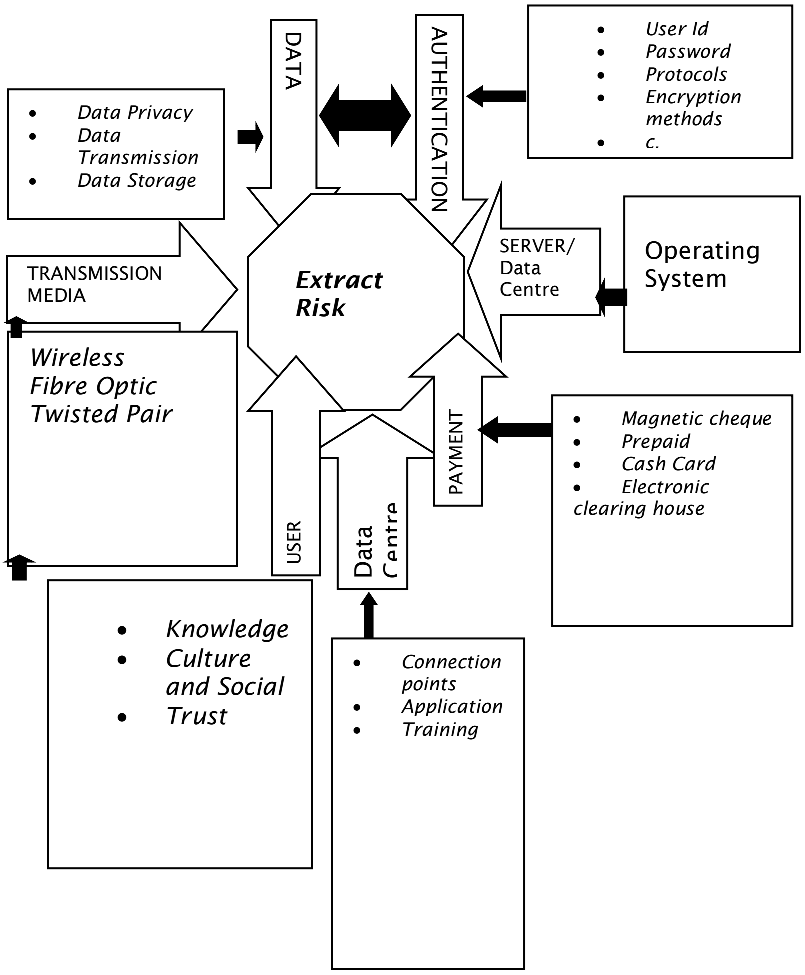
The fact finding served as the basis for collecting data required for the risk assessment process. This questionnaire was designed to measure the readiness of the Sudanese population to welcome the E-Payment system. It is divided into two parts, the first part was distributed inside Sudan, and the second was distributed among Sudanese citizens who lived outside Sudan and already benefiting from E-Payment. The respondents were 61% students, 23% professional, 11% businesses, and 4% others. The youngest respondent was 17 years old, and the oldest was 67. The age groups of the respondents were classified as follows (less than 18) 7%, (18 to 25) 52%, (26 to 34) 21%, (34+) 16%, and 4% unspecified. The analysis of part one is as follows:

The questionnaire was designed in such a way that it assessed the feasibility of E-Payment system implementation in Sudan from the users' point of view. The analysis of the results indicated that 77% of the respondents inside Sudan do not have Bank accounts; most of them gave trust reasons, while 100% of the respondents outside Sudan had Bank accounts, Credit or Debit Cards. The majority of them, both inside and out side Sudan, think it is beneficial, easy to use, or the easiest way to make payment. However, they expressed their concern about privacy, security, and availability. Knowledge is a key factor as it prevented 81% of the respondents inside Sudan from accessing the Internet, whereas it prevented 33% of the respondents outside Sudan from having online banking accounts. It was not the greatest preventative factor, if online risk is taken into account, as it prevents 57% of them from benefiting from online banking. Their response to the role of government question was not impressive as 63% did not give reasons. The questionnaire is meant to investigate the popularity of the banking industry. Amongst the respondents "trust" was a major issue as well as their knowledge about E-Payment systems. The study also examined their ability to adapt to new technology, and the impact of the digital divide.**Using SSTM**Some components of SSTM are modified to match this study. For example it used Data Centre instead of Service Provider, because the data centre of the central bank of Sudan is the focus of this study, this saved the Server's entity as it will be used as a RAS at the Data Centre entity. Instead we added "Service" entity, which included "Connection points", "Infrastructure", "Application", "Training", "Skill", and Customer Service. Also we identified RAS associated with "User" and "Data", as results of the questionnaire showed increasing concern with respect to privacy of personal data, knowledge, and trust.

Level 1: Identifying the risk Below are the risks identified from the fact finding results after applying SSTM at level 1. This is the first step where risks are identified from Risk Access Spots (RAS). The original model does not have RAS at user, or Data levels.


DATA
AUTHENTICATION
User Id
Password
Protocols
Encryption methods
c.
Data Privacy
Data Transmission
Data Storage
TRANSMISSION MEDIA
Identify Risk
SERVER/ Data Centre
Operating System
Wireless
Fibre Optic
Twisted Pair
USER
Data Centre
PAYMENT
Magnetic cheque
Prepaid
Cash Card
Electronic clearing house
Knowledge
Culture and Social
Trust
Connect ion points
Applicat ion
Trainin g

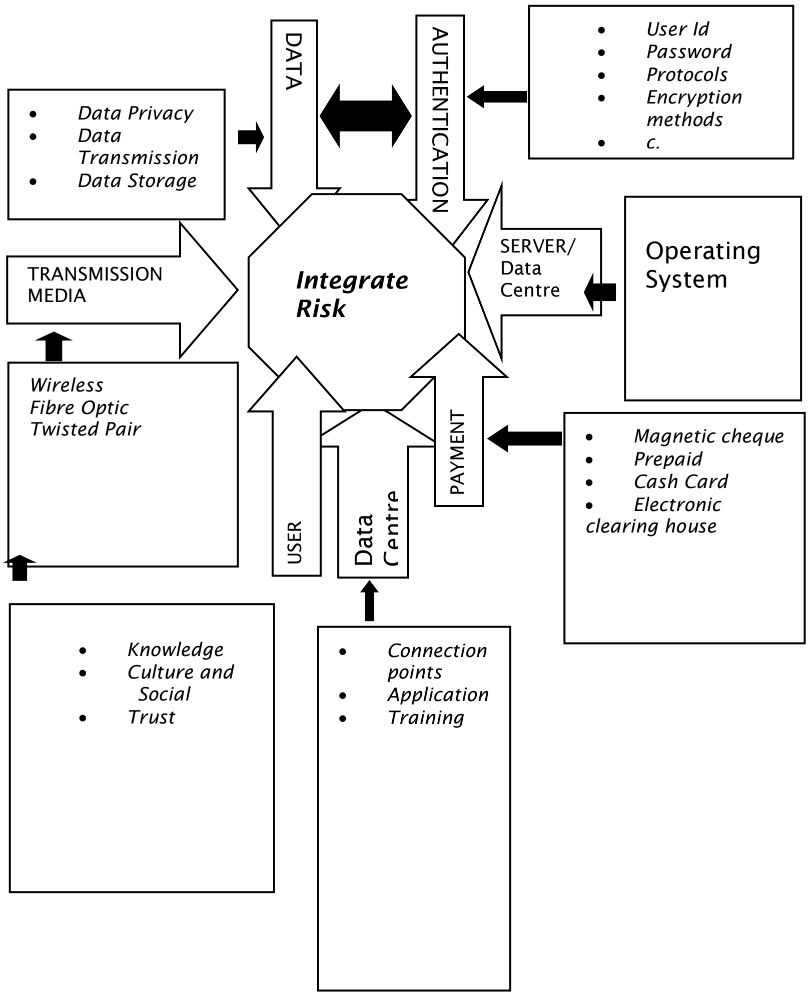
LEVEL 2- Extract Risk



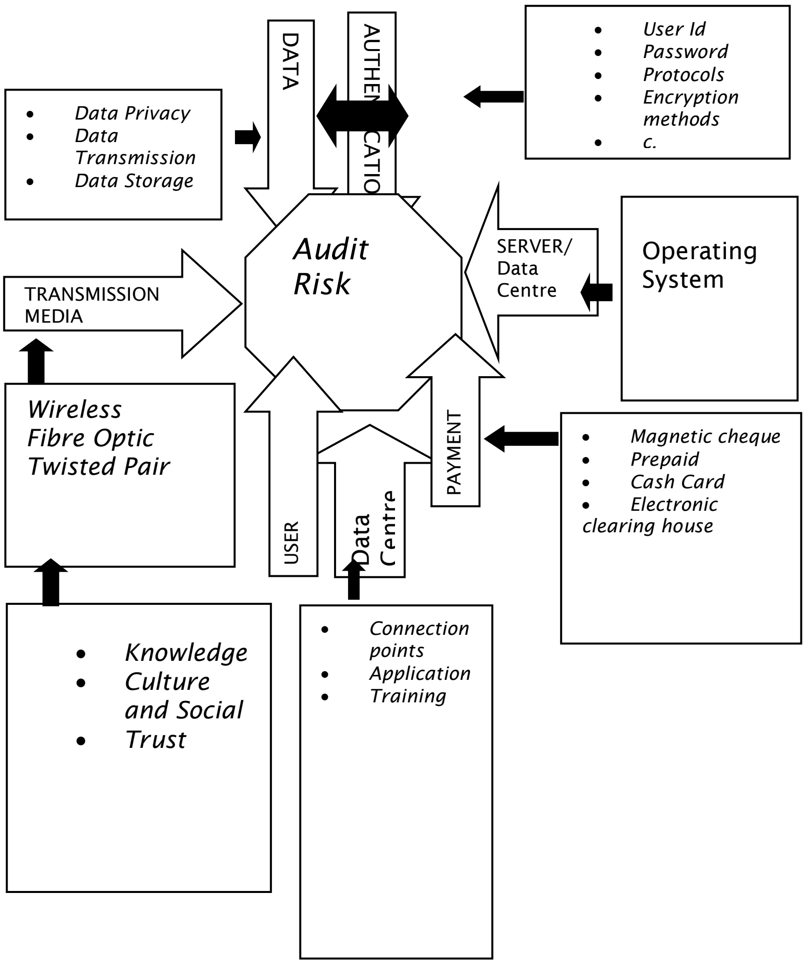
LEVEL 3 - (RIG) Risk Identification Grid

Z7	Z6	Z5	Z4	Z3	Z2	Z1	
		Operating System	Applications	configuration	skill	knowledge	Z1
		Customer Service	Protocols	User ID	Trust	Training	Z2
		Prepaid cash card	Twistted pair	packet	Global IP address	Encryption	Z3
		E-clearing house	Fibre optic	Behaviour	Encryption	Cyphertext	Z4
		Server side	Magnetic cheque	Wireless	Data Storage	Connection points	Z5
							Z6
							Z7

LEVEL 4 – Integrate Risk



LEVEL 5 – Audit Risk


Data Privacy
Data Transmission
Data Storage
DATA
AUTHENTICATIO
User Id
Password
Protocols
Encryption methods
c.
Audit Risk
TRANSMISSION MEDIA
SERVER/ Data Centre
Operating System
Wireless
Fibre Optic
Twisted Pair
USER
Data Centre
PAYMENT
Magnetic cheque
Prepaid
Cash Card
Electronic clearing house
Knowledge
Culture and Social
Trust
Connection points
Application
Training

LEVEL 6 - (RISG) Risk Identification Solution Grid

	Z1	Z2	Z3	Z4	Z5	Z6	Z7
Z1	knowledge	Training	Encryption	Cyphertext	Connection points		
Z2	skill	Trust	Global IP address	Encryption	Data Storage		
Z3	configuration	User ID	packet	Behaviour	Wireless		
Z4	Applications	Protocols	Twisted pair	Fibre optic	Magnetic cheque		
Z5	Operating System	Customer Service	Prepaid cash card	E-clearing house	Server side		
Z6							
Z7							

SOLUTIONS

12.6 SSTM results and analysis

Risk Access Spots (RAS) are mainly gathered from the questionnaire feedback. The number one top priority is *knowledge*. 81% expressed their regret for not having enough knowledge to access the Internet. Also 33% of the respondents outside Sudan do not have online banking accounts for the same reason. The results from SSTM highlight knowledge and computer literacy as hurdles which need to be overcome if an e-payment system is to be successful in Sudan.

Skill and *Training* are connected in many ways. For example, you can not improve skill unless you have good training. Issues such as training and skill are critical to developing economies. For instance skills set in UNIX, Netware, Windows, and CISCO router were low amongst developing economies as compared to advanced economies Williams (2004).

These facts stress the need for training by skilled instructors with the appropriate facilities to improve the skills of employees and therefore make them feel confident when they deal with the new system or solve problems connected to it.

Another important RAS was "trust" as it was the main reason given for not having a bank account. One of the respondents expressed his mistrust by saying:" *I couldn't get cash out of my account because the bank didn't have enough liquidity at that time*". Due to these reasons they prefer to keep their money in an accessible place, such as at home, where they can get it when ever they want it.

12.7 Findings

The findings of this study were extracted from risk assessment using data from interviews, questionnaires distributed to Sudanese citizens both inside and out side Sudan.

At Level 6 of SSTM or RISG, the Risk Access Spots are prioritised. The analysis of the findings of this level demonstrate a high Risk from Users, as all Risk Access Spots highlighted under User are between Z1, and Z3. This indicates the need for investing in training and education. Also the analysis highlighted the following points.

- The Central Bank of Sudan is working hard to improve the banking system and to computerise the banking system, but unfortunately the infrastructure is not yet ready to welcome these changes
- The Central Bank of Sudan is trying to over come some of the infrastructure related obstacles, like using UPS in case of power failure.
- The digital divide between Sudan and other advanced countries is huge as observed in this study.

- There is mistrust among customers with regards to the banking system; due to lack of knowledge of the system.

- The cultural and social beliefs often serve as barriers to change for stakeholders.

12.8 Recommendations made to stakeholders from the study

- More attention needs to be given to basic infrastructural services such as electricity and communications. Although the Sudanese Telecommunication Company (Sudatel) is doing very well, the prices of its services are still high.
- Businesses and profitable organisations should be encouraged to make more use of the banking system, for example they can pay their employees salary, or accept customers bill payments by direct debit.
- Enforce and introduce computer literacy in earlier education stages, and pay more attention to computer literacy in general.
- Make use of scientific studies from advanced economies, and give more support to scientists and scientific researches.
- Use oil revenues to invest in people by encouraging innovation through funding research and supporting distinguished students.
- Promoting knowledge by opening public libraries and providing less expensive public Internet access.
- Promote the banking industry by helping individuals to open bank accounts, for example commercial banks can reduce the minimum deposit required to open an account, or introduce new schemes that suit people with less income.
- Assess the international directives that govern both banking systems and ICT, and produce laws that are suited to the case of Sudan.
- Promoting technology by arranging conferences and setting up societies that encourage experts from advanced economies to get involved in the Sudan ICT and business logic agenda.
- Direct all official and governmental financial transactions to go through the banking sector.
- Provide periodical training sessions to help to Keep the technical employees up to date with technology, also insist on getting them certified.

12.9 Summary

Chapter 12 presented a simulation of SSTM using 4 case scenarios.
The objective of the simulations was to assess the reliability and trustworthiness of the model. It assessed security risk in Online Business Security for heterogeneous and hetero-standard systems with respect to communication networks using Monte Carlo method. The simulations addressed issues with respect to how security was

assessed in organisations which had both local and global network infrastructure, how such risks threatened the confidentiality, integrity and availability of information services. Using SSTM probability of risk was calculated to determine seriousness of risk.

Chapter 13

Emerging Ideas

This chapter examines whether software agents could be trusted for digital evidence on cyber platforms consequently leading to the intelligence required. The analysis covers ad-hoc wireless networks by drawing contrast with regards to the problems associated with each topology type. The main arguments focus on the characteristics of software agents and the nature of ad-hoc wireless networks as the main driving force of cyber platforms. There is also emphasis on agencies that manage the role and functions of the software agents on these networks.

This section presents the arguments against and in favour of software agents with regards to evidence collection in forensic computing on cyber platforms and communication networks. The term communication network is referred to computer and network systems. The main objective of evidence collection in forensic computing is to present electronic evidence that is admissive in court of law. Given this objective, it will be important to evaluate arguments why evidence gathered by a software agent might be or not admissible in a court of law. Sommer (1997) defines evidence collection as "evidence from computers that is sufficiently reliable to stand up in court and be convincing". Trusted related issues associated with software agents and the nature of information that could be acceptable as evidence in post e-crime scenario is exploited to uses essential to homeland security.

Evidence Collection and Homeland Security

According to Rude (2000) Evidence Collection requires some form of methodology in order to establish consistency among different types of investigations. The methodology may or may not be applied in rigid manner. It could serve as a point of reference. The author proposes (5) steps for such a methodology; Preparation, Snapshot, Transport, Preparation and Examination. Based on the review of the methodology it is clear from the paper that, the evidence collected should comprise both external and internal parts of the computer system. This consists of both discovery and recovery. Invariably it is important that both software and Human agents work in a collaborative manner. The recording and documentation aspects of the investigation processes were considered to be paramount in the success of the entire process.

Rodney Mckemmish defines forensic computing as the "process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable". According to the author it comprises four (4) key elements. These are the identification of digital evidence, the preservation of digital evidence, the analysis of digital evidence and the presentation of such evidence in a court of law. The four points raised bear resemblance to key points also discussed by Rude (2000). In the next section we review these steps with regards to Software Agents.

Identifying evidence brings a number of challenges to mind. The troubling key questions are as follows, where will the evidence be? How could it be traced and how will such evidence be collected? The logical answer to such questions will be, human experts in forensic computing will trace and collect such evidence. This is what has been discussed in the literature. Although security defence mechanisms and tools such as firewalls, intrusion detection systems are tools that provide useful information, they are not competent in monitoring dynamic behaviour of Communication Networks on daily basis.

The preservation of evidence could also be tampered and destroyed not only by human error, but also virus and worm attacks. Software agents deployed effectively could contribute to the preservation of evidence in a more productive manner by ensuring that original images of hard disks and file structures are kept till the time an e-crime is committed. The notion here is that, the software agent could serve as a ***black box***, which automatically records the life history of a computer system or any electronic device. The aim of the preservation process is primarily to minimise intrusions, deliberate and accidental changes that may occur to devices central to the investigation process. This might not always be the case. The next paragraph will present both sides of the arguments in relation to the examination of such information.

What are the processes involved in examining the evidence collected? Are there methodologies based on empirical evidence that could be applied at this stage? Or is it solely dependent on the skill set and experience of the forensic examiner and team. According to Rude (2000) there is the need for a methodology in such an investigation. This is to ensure consistency and also serve as a tool in satisfying a court of law. There seem to be no standards governing the application of such methodologies. Tools for analysing such information could encounter a monstrous task if the nature of information depicts a complexity that the tool employed cannot simplify. This could affect the nature and meaning of the preserved information. Supposing we assume that a software agent learns disseminated and shared information on a communication network, it will be better equipped in contributing to the interpretation and examination of preserved information. It should however be noted that this might not always be the case. This is because a software agent could be unreliable and untrustworthy if it encounters other friendly agents on the communication network. It could also be argued that since the software agent originates from a particular agency, it would be loyal to that agency, consequently be reliable and trusted. What about if the agent's behaviour is influenced by other agents? Is that possible? I will assume yes, since characteristics of agents such as cooperation and learning could be compromised. If communication between two agents is fuzzy, there is the tendency that the agent collecting evidence could misinterpret information available to it, and act based on the wrong assumption as a result of information gathered from a malicious agent originating from another agency. The final stage according to (Mckemmish) is to present this information to a court of law. In considering the steps and stages involved, I made certain assumptions, primarily with regards to the existence of rules and methodologies that the examiner must adhere to in order that the entire process succeeds. Rules such as minimal handling of the original, accounting for any change, complying with the rules of evidence associated with the law and legal framework, and not exceeding knowledge or expertise.

Sommer(1997) summarises the processes involved in the investigation based on some general principles. These are as follows: The crime scene has to be "frozen" or seized. There must be continuity of evidence. According to him this means that we have to account for all incidents that have taken place or that took place. All procedures should be auditable. That is, all investigations conducted should be traceable. The stages involved in the process should be clear and void of any ambiguity. According to Hastings (2003), there are five (5) common mistakes that might arise if appropriate rules are not followed in the investigation process. Using the in-house IT staff to conduct a computer forensic investigation could result in catastrophic consequences. This is because in-house personnel usually could be biased to people they are loyal to. Avoid such a mistake by recruiting an independent expect to conduct such an investigation. This suggests that, a software agent employed from an agency and certified by a third party could be highly useful. It could serve as an external independent entity in the investigation process. There are a number of issues that come to mind. I have however focused on trust, which is the central theme of this paper. The next section examines the characteristics and attributes of a software agent with regards to trust in order to understand and appreciate the magnitude of such an issue.

Definition of Agent

An agent is anything that can perceive its environment through sensors and acting upon that environment through effectors. A human agent has eyes, ears and other sensors that allow it to survive and adapt to its environment Russel and Norvick (1995). The term **performance measure** is used to assess the criterion that is used in determining success of an agent. Anything that the agent has perceived so far could be call complete perceptual history, the **percept sequence. A rational agent** is one that does the right thing. The “right” thing might be highly subjective, since what is right in one environment might be wrong in another environment. The approximation of such subjectivity is based on how successful an agent could be in performing a particular task. This could be based on the completeness of the task or other criteria. In summary an agent should be autonomous, adaptive and cooperative in the environment it operates these should be inherent parts of the agent.

Gathering Intelligence with Agents

The rational behaviour of an agent is dependent on four things. These are performance measure, percept sequence, knowledge of environment and actions that the agent could perform. I have highlighted some of these in section 2. The notion of having an agent able to do the right things might contradict with the real world. This is based on some of the reasons mentioned in section 2. The underlining principle here is that doing what is right, might not be necessarily right in another environment. A desirable attribute of an agent is that, it should be autonomous. This means that it should not be under the control of another agent, being it software or human. If the agent solely relies on the build in knowledge part, without being able to learn from its environment then we say that the agent lacks autonomy. Whether an agent lacks autonomy or not we will need to make an assessment of the implications of using an agent for evidence collection. The next section considers the structure of an agent.

Agents and Trust

According to Negroponte (1997) an ideal agent has characteristics similar to an English butler who is well trained and can know your needs, likes, habits and desires. The analogy here means that the most trusted agent is the one that is likely to know your secrets. This assertion could also be verified in the prosecution of Paul Burrell former Butler of Princess Diana for alleged theft. So, ***what is trust***?

This book defines trust as the extent that any functional entity whether human or software relies upon information assimilated from known and unknown sources. The key word here is reliability, a characteristic of quality software. Rotter (1980) also defines trust as a general expectancy that the word, oral or written statement of an individual or group of people could be relied upon. Again the key word here is reliability. Patrick (2002) speculates that when a software agent carries out its instructions then it could be trusted. I think one needs to look beyond that. This is because you could have an agent that could carry out your instructions everyday and time and yet could be untrustworthy. This could be that the agent is a double standard agent. This is also seen in the Babington Plot of **1586**, when Mary Queen of Scotland was imprisoned by Queen

Elizabeth the I. The encrypted messages from Mary sent to her Catholic supporters through a courier was via a double agent working for Francis Walsingham, Elizabeth's spymaster. Her Cyphertext was broken by Thomas Phelipes, master forger and cryptanalyst for Sir Francis Harrison (2004).

Applying trust in software agents suggests that all control functions are made void, by allowing the software agent to determine its own existence. What are the **checks** and **balances** that have to be in place in order to achieve such a level of reliability? The issue of trust is highly dependent on the checks and balances implemented as part of the software agent. Do we need trust because we are vulnerable as stated by Zan (1972).

This book disagrees with this assertion. Although that might be the case in certain circumstances, the view taken here is that trust might be needed in circumstances where relationships amongst people needs to thrive or advance in order to achieve greater goals. Remember the **performance measure,** the criteria use in determining the success in software agents. The next section examines factors that could influence trust.

Factors that affect Trust

Given the definitions and examples of trust situations, it could be argued that trust is relative and subjective as such should be assessed and determined in a given context. The survey of Cranor, Reagle and Akerman(2000) suggest that different people have different baseline for trust. This implies that the criterion or checks and balances put in place for a software agent might not be applicable in every circumstance.

Patrick (2002) highlights six (6) factors discussed in conjunction with Lee, Kim and Moon's model of agent success. These factors are ability to trust, experience, predictable performance, comprehensive information, communication and interface design, presentation and certification and logos of assurance. It should be noted that these views were based on a survey conducted with respect to Internet users. These factors are likely to vary from one circumstance to the other. These factors could also be influenced by the communities and environment they originate. The notion here is that different communities may exhibit different levels of trust because of theirs believes, experiences and risk associated with these environments.

Wong and Sycara in the paper adding security and trust to multi-agent systems propose a framework for addressing security and trust issues. According to the authors adding security and trust improve user's confidence and assurance in successfully carrying out tasks assigned to them. They indicate a number of factors that influence the level of confidence necessary to trust a system. These include corrupted naming and matchmaking services, insecure communication channels, insecure delegation and lack of accountability. The view taken here is that each factor mentioned is important. The author believes that insecure communication channels and insecure delegation are the most sensitive factors that if not managed effectively will degrade the level of trust and confidence that a user is required to exhibit. This is due to the fact that communication networks that support distributed platforms show vulnerabilities which make them susceptible to attacks Williams (2004). These insecure communication channels could comprise but not limited to the following, ports, random access memory (RAM), poor configuration of firewalls, communication media both wired and wireless networks and router tables. Pertaining to insecure delegation, there are issues that may relate to the authenticity of the agent. Are they what they claim to be? How do we verify this level of authenticity? Are there any methods based on empirical evidence? Or do we apply a general security model. These are questions that have not been answered satisfactorily. Given those threats the authors suggest solutions such as using trusted ANSs and matchmakers, making agents uniquely identifiable and give identity of proof that can not be forged when interacting with other agents. Protect communication channel, make agents prove that they are delegates they claim to be (authentication). Make deployers and agencies liable for the actions of their agents. These suggested solutions, threats and trust issues is discussed in the section "agents, trust and evidence collection" by examining arguments in favour and against this research question.

Evidence Collection

The heterogeneous nature of information and distributed systems make it paramount that software agents are able to migrate freely without much hindrance. The importance placed on agent based software engineering also depicts that there is the need for a common agent paradigm and programming language that enable these software agents to communicate in a cooperative manner Papazoglou et al(1992). Retrospectively, this has not been the case Nwana (1996).

Cyber Risks and Vulnerabilities

A wireless communication network is deployed using an unguided media, thus the electromagnetic spectrum. Its boundary extends the limitations of traditional wired networks. In general, a WLAN consists of a central connecting point usually known *as* an Access Point (AP).This could be compared to a hub or switch on a wired network. The access point serves as the point of information interchange or communication between a wireless and wired network *Gust, Mathew (2002). 802.11 Wireless Networks – The Definitive Guide. O'Reilly.*

The RAS of wireless communication networks could range from the electromagnetic spectrum, such as the *frequency and bandwidth which information is transmitted, baud rates, rogue access points, congestions resulting in stealth attacks and IP information on router tables* Williams (2004), Jakobsson, Wetzel and Yener(2003).
In order to determine whether software agents could be trusted for evidence collection, I have reviewed certain attacks that are unlikely to be traced on ad-hoc wireless networks. These attacks have been derived from the paper *"Stealth Attacks on Ad-hoc Wireless Networks*" Jakobsson, Wetzel and Yener (2003). Denial of service (DOS) attack happens by disconnecting networks through degrading of goodput and modification of routing information in order to hijack traffic flow on selected victim nodes. The primary goal of these attacks is to achieve the maximum damage with minimum effort.

Disconnecting networks

An adversary usually creates a large amount of traffic, by dispatching bogus messages to the nodes controlled by the victim. It is not all cases that the victim have to control all nodes Jakobsson, Wetzel and Yener(2003). According to the authors, messages sent from these nodes are disrupted by the attacker. This could be achieved through the modification of router information. This form of attack could result in a disconnection due to unnecessary congestion. This attack was highlighted in a recent documentary of the ITV channel of the BBC (British Broadcasting Corporation) simulating a terrorist attack in may 2004. One of the strategies defence analysts decided to adopt under such a circumstance was to congest communication channels and lines used by the public for mobile communication in order to make channels and lines used by the emergency services more efficient. Given this hypothetical account of this incident, the emergency services might be in difficulty a stealth attack designed to congest the wireless media is launched. Gathering evidence under such a chaotic scenario could be extremely difficult. The second type of attack reviewed is when an adversary modifies routing information in order to hi-jack communication to and fro nodes on the networks.

Modifying routing information

This affects the integrity of the message dispatched. Router information on ad-hoc wireless networks could be available within the electromagnetic spectrum, due to the fluid topology of ad-hoc wireless networks. The difficulty associated with the traceability of this form of attack stems from the fact that, it could be launched from any remote location, provided the attacker has a good guess of the frequency and bandwidth which the communication is taking place. The insertion of bogus messages could be transmitted in a viral or worm-like manner. Cookies could also be employed to camouflage the attacks. Given the two forms of attacks, can a software agent be trusted to trace this type of attack? *If yes, how? And If no, why?* I have summarised both points of view by outlining the underlying reasons. This is based on discussions from previous sections.

A software agent could be deployed on ad-hoc wireless network as an intrusion detection agent that has mobility. This could help in detecting any act of misuse on the network. Due to the learning ability of the agent, it could also be argued that it will adapt to new patterns on the network by responding to the ad-hoc changes that occur on the network. On the contrary the ad-hoc behaviour of network topology could elude the software agent since neural capabilities of these agents could be slow.
Since the role of the agent in this discussion is not to detect and prevent an attack but rather trace the source of the attack for evidence admissive in a court of law, it will be possible for the agent to trace all possible channels of communication on the ad-hoc network and consequently follow up these clues. The challenge here is not traceability but rather whether information collected as evidence could be relied upon in a court of law. Given the discussions in section 3, I have drawn a number of reasons why a software agent could or not be trusted for evidence collection admissive in a court of law.

Benefits for Trusting Agents

- They can adapt to new patterns on both wired and wireless networks

The learning characteristics and capabilities of software agents could enable them to adapt to new communication patterns on the communication networks by learning new activities. Human agents lack the ability to recognise detail and complex trends in a mesh of activities managed by a computer. Most of them are not immediately evident and observable by the naked eye, even if a deliberate effort is invested in tracing such details. For instance software agents could be deployed to move from one network node to another. Such a task could not be assigned to a human agent. This will be considered illogical and inefficient, since the time taken by a human agent will be astronomical and not cost effective as well. This is why most problem solvers will rather rely on techniques such as neural networks in identifying patterns that is not usually traceable by humans.

- Their Independent and Autonomous nature make them neutral. No loyal affiliations

Autonomy help to alleviate bias and loyal affiliations that is likely to influence the performance of the agent with regards to the integrity of the information collected. Undoubtedly autonomy is a coveted quality that any individual, group of persons, example the public seek to be seen in the judiciary. In other words it is expected of any organisational body and its representatives that claim to be independent with respect to the rule of law. The lack of confidence in forensic investigators could sometimes affect the credibility of any information collected, preserved and subsequently presented in a court. The view taken here, suggest that a software agent will be have a higher level of trustworthiness compared to a forensic investigator who is a human agent. This is a point where a defence attorney could challenge a prosecutor in a court of law. It will also be difficult a prosecution team to prove, based on the presumption of innocence.

- They could be used as a black box analogous to the black box installed in airplanes

Continuous activity monitoring on the networks by agents could be useful in a post e-crime scenario. The black box technology installed in aircrafts serves a security purpose which can not be understated. The software agent can play a similar role by continuously collecting information related to activities on the network. Although significant aspects of such activities could be traced from different sources and destinations of the communication network, it takes a lot more time to achieve such objective. This is because the forensic investigate has to rely on the current state of the network or information retrieved from the network log or audit trail.

- In order for the evidence collection process to be successful, expertise of the examiner should be adequate during the evidence collection process.

As part of the ethos of the forensic investigation process, the evidence collector's knowledge should match the expertise required to successfully complete the investigation. Adhering to this process will ensure that satisfactory standards are upheld in the investigation process. This strength could also be a weakness if such requirements are not met.

Demerits of Trusting Agents

- Double agents. An example is the Babington plot of 1586

Software agents are likely to serve as double agents, if the agency which the agent was deployed does not exercise the appropriate level of control. It is also likely that some agents could be exposed to security attacks in the form of virus or worms. These are all problems and issues that have not been discussed in the literature.

- Information (Evidence) collected could be diluted as a result of bogus mess
- ages through vulnerable communication channels and lines.

Bogus messages could be dispatched to intercept, interrupt and distort information being recovered by the agent. This could be detrimental to the integrity of the information gathered. The issue of integrity could affect agents in diverse ways.

- Agents could be made to compromise their stand (integrity).

Some agents could be lured to disbelieve their own believes. This is based on the notion that the characteristics, rules and intelligence that define the existence of believable agents could be reversed, if those characteristics could be traced and deciphered. This undoubtedly can become a major security issue if not properly managed.

- An agent might not be able to preserve information gathered

It is not quite clear in the existing literature whether traditional forensic investigators have the responsibility of preserving evidence gathered or this role is assigned to a forensic technician Alec et al (2003). If this is the case then it suggests that software agents also have similar responsibilities. The author believes this is the case.
If this is the case then software agents have a monstrous task in preserving evidence discovered and recovered. They might face an attack planned and launched by an assassin. In real life an assassin could be employed to eliminate a person who might be in a position to provide evidence that could be admissible in a court of law. It is no wonder why

- Ad-hoc network behaviour could elude the agent

The dynamic and dynamic nature of ad-hoc communication networks could make traceability and monitoring of intrusions almost an invisible task. Although some academics and practitioners might disagree with this view, it is a fact that if an e-crime is committed from a remote location in a developing economy resulting in catastrophic consequences, it will almost impossible to trace the source. The reasons for this are numerous. Although this is not the subject matter for discussion, interested readers could obtain information from the book entitled synchronizing e-security Williams (2004).

- Might not conform to existing legal framework and law

The legal framework and law have still fall short of addressing issues and discrepancies in existing electronic crime, and defining boundaries that do not violate civil liberties. Making a case for evidence gathered by an artificial being or an object that exhibits critical characteristics of a human being is a weak notion, since the law is still struggling to deal with e-fraud and crime. The other disadvantages are;

- Rogue access points could be used in spoofing bogus information

- Insecure delegation and lack of accountability by agents to the law. Agencies might not be accountable to the law

- No established and cooperation amongst existing agencies. Poor collaboration and cooperation amongst heterogeneous platforms.

Summary of Chapter 13

Although there are some advantages for assigning a software agent in collecting evidence on cyber platforms, the disadvantages are enormous. This suggest that in order that a software agent could be trusted in evidence collection on cyber platforms, most of the issues highlighted should be satisfactorily addressed. The conclusion drawn is that they can only be trusted when used in collaboration with a human agent. Some advances had to be made in order for it to be trusted as a sole investigator and evidence collector.

Chapter 14

Discussions

This book brought to light opportunities available to less financially rich countries and how a cross section of them have effectively use cyber technology to create new wealth and assets to booster their economies. There is emphasis on security investment trends, expenditure of countries and organisations in both developing and advanced economies.

The book also explored the safety and security implications for using data mining technologies and strategies. Some of the techniques discussed included profiling, pre screening and detection. Although these technologies have been used widely among intelligence and security agencies, there have been concerns by the wider public of unnecessary snooping of citizens' activities and breach of privacy as well as personal freedoms. The view of the author in this book is that, the hurdle required to be satisfied by security and intelligence agencies may hinder the efficacy to which national and homeland security services are delivered, as a result there is the need for citizens to make compromises.

The role of both private and public sectors is considered unique when public safety and security is at stake. The fundamental difference is that private sectors spearhead the development of these applications with funding support from government. This funding occasionally leads to collaborative research and development initiatives between public and the private sector. The difference is that most technology applications developed by the private sector supports public services.

Training programmes for citizens are important facets that ensure homeland and national security. There are fundamental issues and challenges such as cyber threats and attacks that infringe on our freedoms as well as threaten the stability of the country we live in, organisation we work for or social networks. Our life online whether at home or within a corporate setting is usually affected, especially the processes that support infrastructure at home or organisations we interact with.

Access to training programmes to address issues related to user awareness should be available on a daily basis. Impersonation, masquerading and identity theft are all issues that require solutions that are carefully thought through and implemented to address security shortfalls. Online users provide personal information to social networks in unprecedented fashion and volumes. It is essential that citizens are encouraged to be a part a collective solution that involves local agencies, government and quasi government agencies or solution providers that carryout security functions on a daily basis.

Introduction of a wide range of money transfer and payment systems come with many commercial opportunities. This becomes an enabler for small businesses, startups and entrepreneurs. Technologies such as SET designed by VISA for money transfers and payments provide the new avenues for growth which impacts on businesses and the development of individuals. These new opportunities also require an understanding of the citizen's rights and obligations.

These rights are usually enshrined in the laws of the land and jurisdiction designed to ensure that proper governance is upheld. The application of the citizen's rights also furthers the course good governance, international law and enforcement as well as personal responsibilities.

Notwithstanding the framework of the law and the enforcement of it, its governance to support citizen's rights, there are vulnerabilities that are exploited by hackers to compromise the systems that drive home, corporate and government communication networks. The general notion is that our lives online are exposed to all kinds of attacks. These attacks could be mitigated with the appropriate risk security models put in place. These system models provide an understanding of the risk spots and security vulnerabilities of the systems we use on a regular basis.

The emergence of terrorism and associated cyber tools commonly exploited to complement attacking methods used by terrorists has not been addressed effectively. Emerging systems such software agents, profiling tools and a suite of software, policy and strategies may be employed to provide a more cohesive and holistic counterterrorism response to threats and attacks.

This book proposed a number of innovative strategies and tools for mitigating threats from Terrorists. These tools and strategies comprise the fight against Ideology, ability to enable ordinary citizens train and educate fellow citizens, avoid unnecessary legal jargons where possible when communicating to citizens, use ordinary citizens as driving force and engine and establish a close strategic alignment with goals of emerging economies applying the principle of synchronizing security processes, investments and goals has been discussed as central to deploying an effective holistic response capable of providing the security and defence deserved by the ordinary citizen.

References and Bibliography

"IFLA", IFLA Medium-term Program, 1986-1991, IFLA, The Hague, 1988. Quoted in Aguolu, I. E. (1997)"Accessibility of information: a myth for developing countries?" *Journal of New Library World*, Vol. 98 No. 1 pp. 25-29.

"UNESCO", UNESCO Statistical Yearbook, (1991) UNESCO, Paris. Quoted in Aguolu, I. E. (1997) "Accessibility of information: a myth for developing countries?" *Journal of New Library World*, Vol. 98 No. 1 pp. 25-29.

Adam, L, (1996) "Electronic communications technology and development of Internet in Africa", *Information Technology for Development*, Vol. 7, No. pp. 133-44.

Aguolu, I. E. (1997) "Accessibility of information: a myth for developing countries?" *Journal of New Library World*, Vol. 98 No. 1 1997 pp. 25-29.

Alterman, J. B.(2000) "The Middle East's Information Revolution," *Current History*, January, pp. 21–26.

Annis, S, (1991) "Giving voice to the poor", *Foreign Policy*. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Arreymbi and Williams (2005). Economics of Electronic Security, Economics of Electronic Business Processes. Ed. Paulus S, N. Pohlman, Reimer H Vieweg.

Arunachalam, S. (1998) "Information age haves and have-nots", *Educom Review*, Vol. 33, No. 6, pp. 40-4. Quoted in Okunoye, A and Karsten, H (2003) "Global access to knowledge", *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Avgerou, C. (1998) "How can IT enable economic growth in developing countries?" *Information Technology for Development*, Vol. 8, No. 1, pp.15-29. Quoted in Okunoye, A and Karsten, H (2003) "Global access to knowledge", *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Berners-Lee, T., Cailliau, R., Luotonen, A., Nielsen, H., Secret, A., (1993) "The World Wide Web", *Communications of the ACM*, Vol. 37, No. 8, pp. 76-82. Quoted in Cheun, W (1998) *Journal of Industrial Management & Data Systems*, Vol. 98 No. 4 pp. 172-177.

Alethia, C. (2009). Towards an Emergency Response Report Card:
Evaluating the Response to the I-35W Bridge Collapse.
Journal of Homeland security and emergency Management .

Allison, Graham (2006). "Cardinal Challenge: The world must take seriously North

Korea's nuclear provocation." *Richmond Times-Dispatch*, October 26, 2006.

Allison, Graham (2007). "Fast action needed to avert nuclear terror strike on U.S.."
Baltimore Sun, July 2, 2007.

Bahutule A(2010). Lawmakers accuse BP chief executive for oil spill. Retrieved June 21, 2010, from findtut Web Site:http://findtut.com/lawmakers-accuse-bp-chief-executive-for-oil-spill-286051

Bullock, J., Haddow, G., Coppola, D., & Yeletaysi, S. (2009). *Introduction to homeland security.* Oxford: Elsevier.

Bhatnagar, S. (2000) "Social implications of information and communication technology in developing countries: lessons from Asian success stories", *The Electronic Journal of Information Systems in Developing Countries*, Vol. 1, No. 4, pp. 1-10. Quoted in Okunoye, A and Karsten, H (2003) “Global access to knowledge”, *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Banks, W. C., Nevers, R. D., & Wallerstein, M. B. (2008).
Combating terrorism, strategies and approaches. Washington DC: CQ Press.

Barron, J., & Schmidt, M. (2010). *From surburban father to a terrorism Suspect.*
New York: New York Times.

Bean, H.(2007). The role of homeland Security Information Bulletins within Emergency
Management Organisations: A case study of enactment.
Journal of homeland security and emergency response .

Berry, C.(1998). *The library of congress,*
bibliography on future Trends in terrorism. Federal Research Division.

Brian J Gerber, D. B. (2007). *US Cities and Homeland Security:*
Examining the role of financial conditions and administrative capacity in municipal preparedness efforts. Pubic Finance and Management.

Bullock, J., Haddow, G., Coppola, D., & Yeletaysi, S. (2009).
Introduction to homeland security. Oxford: Butterworth-Heinemann.

Bean. (2007). The role of homeland security information bulletins within emergency management organisations: A case study of enactment.
Journal of Homeland Security and Emergency Response .

Berry. (1998). *The library of congress, bibliography on future trends in terrorism.*
Washinghton: Federal Research Division.

Carlson. (2003, June 2). Federals look at data mining.
The E-week Enterprise News & Reviews , pp. 5-9.

Cockburn, C., Wilson, T.D. (1996) "Business use of the World-Wide Web", *International Journal of Information Management*, Vol. 16, No. 2, pp. 83-102. Quoted in Cheun, W (1998) *Journal of Industrial Management & Data Systems*, Vol. 98 No. 4 pp. 172-177.

CBO. (2005). *Federal funding for homeland security:*
An update. Economic and Budget Issue Brief . CBO.

CGCC. (2008). *Institutional challenges in implementing the UN global*
counter-terrorism strategy. Center on Global Counterterrorism Strategy.

CRS. (2006). *Homeland Security: Roles and Missions for United States*
Northen Command. CRS.

Caron Carlson, (May, 12, 2003) Federals look at data mining, The E-week Enterprise News & Reviews.

Clyde Wayne Crews Jr., (January 9, 2000) 'Partial' Information Awareness, Cato Institute

Curriero, F. C., Heiner, K. S., Samet, J. M., Zeger, S. L., Strug, L., & Patz, J. A. (2002).
Temperature and mortality in 11 cities of eastern United States.
American Journal of Epidemiology , 80-87.

DeRosa. (2004). *Data mining analysis for counterterrorism.* CSIS.

Delong and Froomkin (2000). Speculative Microeconomics for Tomorrow's Economy. Internet publishing and beyond. Kahin B and Varian R. Hal

Doob, L.W., (1961) "*Communication in Africa: A Search for Boundaries*", Yale University Press, New Haven, CT. Sourced from Aguolu, I. E. (1997) "Accessibility of information: a myth for developing countries?" *Journal of New Library World*, Vol. 98 No. 1 pp. 25-29.

Fletcher. (2006). The indefinable concept of Terrorism.
Journal of International Criminal Justice , 894-911.

Garfield, E. (1979) "2001: an information society?", *Journal of Information Sciences*, Vol. 1, No. 4, pp. 209-15.

Graham, A. (2006, October). Cardinal Challenge:
The World Must Take Seriously North Korea's Nuclear Provocation.

Richmond Times Dispatch .

Gasser, H.P. (2002). Acts of terror "terrorism" and international humanitarian Law. *IRRC* , 547-570.

GAO. (2004). *Combating Terrorism: Evaluation of selected characteristics in national strategies related to terrorism: GAO-04-408T*. GAO.

GAO. (2008). *First Responders' Ability to Detect and Model Hazardous Releases in Urban Areas is significantly limited: GAO-08*. GAO.

Gyves, Clifford M. (2006). *Policing Toward a Decawed Jihad: Anti-terrorism intelligence techniques for law enforcement.* NAVAL POSTGRADUATE SCHOOL.

Harris, R, (1998) *Internet Hosts per Head of Population, by Region*, Faculty of IT, UNIMAS Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Hashim, A. (2006). In Kamien, *The McGraw-Hill homeland Security Handbook.* New York: McGraw-Hill.

Heyman, & Ethan. (2008). Homeland Security in an Obama Administration. *CSIS Homeland Security Smart Brief* , 27-35. Volume 1 No 1.

HM Government. (2009). *Expectations and Indicators of Good Practice set for category 1 and 2 Responders, The Civi Contingencies Act 2004.* London: Cabinet Office.

HM Government. (2006). *Government Response to the Intelligence and Security Committee's Report into the London Terrorist Attacks on 7th July 2005.* London: Paliarment.

Heritage Foundation (2009), *Iran's nuclear threat the day after*, Iran working group
SR-53, Heritage Foundation

International Telecommunication Union (ITU) (2004), African Telecommunication Indicators 2004. http://www.itu.int/ITU-D/ict/publications/africa/2004. [Accessed 10 March 2006]

ITU, (1999) *Challenges to the Network: Internet for Development*, International Telecommunication Union, Geneva. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Jimba, S., Atinmo, M., (2000) "The influence of information technology access on agricultural research in Cameroon", *Internet Research: Electronic Networking Applications and Policy*, Vol. 10, No. 1, pp. 63-71. Quoted in Okunoye, A and Karsten, H (2003) “Global access to knowledge”, *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

John, M. (1995), "Third world faces `information poverty'", CD News Bank Comprehensive, Reuters America. In Srikantaiah, T. K. and Xiaoying, D. (1998) “The Internet and its Impact on Developing Countries: Examples from China and India” *Journal of Asian Libraries*, Vol. 7 No. 9, pp. 199-209.

Jack L. Jones. (2004). *Confronting an Old enemy: Terrorism and the changing face of Military Intelligence.* CRS.

J.Turley, R.Ron, K.Corrigan, (2002) Panel 1,Subcommittee on Aviation Hearing on Aviation security with a focus on passenger profiling.

J.Turley, R.Ron, K.Corrigan, (2002) Panel 1, Subcommittee on Aviation Hearing on Aviation security and the future of the airline industry

Jones, M and Marsden, G. (2004) “Please turn ON your mobile phone” – first impression of text-messaging in lectures. Proceedings of the 6th International Symposium on Mobile Human-Computer Interaction (Mobile HCI ’04) LCNS 3160: 436-440. Glasgow, UK. Springer.

Jones, M and Marsden, G. (2006), Mobile Interaction Design, Wiley, & Sons Ltd. England.

Kaplan. (2007). *Homeland security technologies.* Council of Foreign Relations:Washinghton.

Karsten, H (2003) “Global access to knowledge”, *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Kauppi, M. (2006). Counterterrorism Analysis and Homeland Security. In D. Kamien, *McGrawHill Handbook of Homeland Security* (p. 413). McGrawHill.

Kenney, G, (1995) "The missing link information”, *Information technology for development*, Vol. 6, pp. 33-8.

Kim S Nash, Computer world. Framingham: http://proquest.umi.com/pqdweb?RQT=572&VType=PQD&VName=PQD&VInst=PROD&pmid=23762&pcid=775437&SrchMode=3Feb.9 1998, Vol. 32, Iss. 6; pg. 1, Electronic profiling

Khan, M.H., 2001, "Rural poverty in developing countries: implications for public policy", *International Monetary Fund Economic Issues Series 21*, 1-13. Quoted in Dao M. Q (2004) “Rural poverty in developing countries: an empirical analysis”, *Journal of Economic Studies* Vol. 31 No. 6, pp. 500-508.

James R Askers, Aviation week & space Technology, New York:http://proquest.umi.com/pqdweb?RQT=572&VType=PQD&VName=PQD&VInst=PROD&pmid=28974&pcid=4426671&SrchMode=3 2003, Vol. 158, Iss. 13; pg. 21, White House Budget Office Questions Effectiveness of Passenger Profiling

Knezo, G. J. (2006). *CRS Report for Congress, Homeland Security Research and Development Funding, Organisations and Oversight.* CRS.

Koh, H. S. (2002). Future Trends and Prospects for Terrorism after 11 September 2001. *Journal of Singapore Armed Forces* .

Kraft, M. (2006). Counterterrorism legislation and the Use of Rule of Law. In D. Kamien, *Handbook of Homeland Security* (p. 325). McGrawHill.

Laqueur, W. (2001). *History of Terrorism.* New Jersey: New Brunswick.

Lewitt, M., & Jacobson, M. (2008). *Terrorist Threat and US Response, A changing landscape.* Washington: The Washington Institute for near east policy .

Lucey, & Rosen. (2001). *Emerging Technologies: Recommendations for Counterterrorism.* New Hampshire: Dathmouth College Hanover.

Masters. (1999). *Practical neural networks recipes in C++*. London: Academic Press.

Madon, S (2000) “The Internet and Socio-Economic Development: Exploring the Interaction”, *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Mansell, R, Wehn, U, (1998), “*Knowledge Societies: Information Technology for Sustainable Development*”, Oxford University Press. Quoted in Madon, S (2000) “The Internet and Socio-Economic Development: Exploring the Interaction”, *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Metz. (2005). IT architecture for homeland security. In Kamien, *McGraw-Hill Homeland Security Handbook* (pp. 71-79). New York: McGrawHill.

MIDS Press Release: "New data on the size of the Internet and the matrix", http://www.mids.org/mids/pressbig.tml>. Sourced from Srikantaiah, T. K. and Xiaoying, D. (1998) “The Internet and its Impact on Developing Countries: Examples from China and India” *Journal of Asian Libraries*, Vol. 7 No. 9 pp. 199-209.

Morales-Gomez, D., Melesse, M., (1998) "Utilising information and communication technologies for development: the social dimensions", *Information Technology for Development*, Vol. 8, No. 1, pp. 3-14. Quoted in Okunoye, A and Karsten, H (2003) "Global access to knowledge", *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Mueller R S (2007) Retrieved on 14th June 2010 from FBI Web.
Site:
http://www.fbi.gov/congress/congress07/mueller011107.htm.

Nordas, R., & Gleditsch, P. N. (2007). Climate chamge and conflict. *Political Geography* , 2-14.

Nagy, H. (1991) "Information Technology in World Bank Lending: Increasing the Development and Development Impact", *World Bank Discussion Papers*, 120, World Bank, Washington, DC. In

(National Terror Alert, 2009). Retrieved May 11, 2010,
from National Terror Alert Web site:
http://www.nationalterroralert.com/updates/2009/10/20/terror-related-arrest-began-in-las-vegas/:

Nikki Swartz Information Management
Journal. Lemexa: Vol. 38, Iss. 2; pg. 18, 1 pgs, U.S. to Start Airline Background Checks

(Night Club bombing, n.d). Retrieved May 14, 2010, from the BBC website:

http://news.bbc.co.uk/1/hi/uk/6255960.stm:

NRC (1996) "*Bridge Builders: African Experience with Information and Communication Technology*", National Academy Press. Quoted in Madon, S. (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Pluchinsky, D. (2006). A Typology and Anatomy of Terrorist Operations. In D. Kamien, *McGrawHill Handbook of Homeland Security* (p. 365). McGrawHill.

O'Malley, M. (2006). Preparing a City for Terrorism. In D. Kamien, *McGrawHill Handbook of Homeland Security* (p. 311). MacGrawHill.

Odedra, M., Lawrie, M., Bennett, M., Goodman, S., (1993) "International perspectives: sub-Saharan Africa: a technological desert", *Communications of the ACM*, Vol. 36, No. 2, pp. 25-9. Quoted in

Okunoye, A and Karsten, H (2003) "Global access to knowledge", *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Panos (1998) "*The Internet and poverty*", Panos Media Briefing, 28, The Panos Institute, London. Quoted in Madon, S (2000) "The Internet and Socio-Economic

Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Press, L (1996) "The role of computer networks in development", *Communications of the ACM*, 39, 2. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Qureshi, S, Cornford, T, (1994) "*Networking and development: the Comnet-It project*", Baskerville, R,

Rosen J and Lucey C (2001), *Emerging technologies:* recommendations for
counter – terrorism. edited volume Institute for Security Technology Studies, Dartmouth College Hanover, New Hampshire

Roy Mark (March 19, 2003) Digital Rights Group Takes Swipe at CAPPS II, Business News.

Roy Mark, (September 29, 2003), TSA May Order Airlines to Share Data, The leading event for the wired and wireless ISPs

Smithson, S, Ngwenyama, O, DeGross, J.I., Transforming Organisations with Information Technology, Elsevier Science B.V. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Sadowsky, G (1996) "The Internet Society and Developing Countries", Article Sourced From http://www.isoc.org/

Schramm, W., (1964) "*Mass Media and National Development: The Role of Information in the Developing Countries*", Stanford University Press, Stanford, CT. Sourced from Aguolu, I. E. (1997) "Accessibility of information: a myth for developing countries?" *Journal of New Library World*, Vol. 98 No. 1 pp. 25-29.

Semich, J.W., (1995) "The World Wide Web: Internet boomtown", *Datamation*, Vol. 40, No. 1, pp. 37-41. Quoted in Cheun, W (1998) *Journal of Industrial Management & Data Systems*, Vol. 98 No. 4 pp. 172-177.

Srikantaiah, T. K. and Xiaoying, D. (1998) "The Internet and its Impact on Developing Countries: Examples from China and India" *Journal of Asian Libraries*, Vol. 7 No. 9, pp. 199-209.

Srikantaiah, T. K. and Xiaoying, D. (1998) "The Internet and its Impact on Developing Countries: Examples from China and India" *Journal of Asian Libraries*, Vol. 7 No. 9, pp. 199-209.

Shays. (2006). Congressional Oversight over Homeland Security and the Dynamic Appropriation. In D. Kamien, *McGrawHill Handbook of Homeland Security.* McGrawHill

Swartz. (2004). US to start airline background checks.

Information Management Journal , 18,1.

Talero, E., Gaudette. P., (2000) "Harnessing information for development: a proposal for a World Bank group strategy", Finance and Private Sector Development, 13 April, Quoted in Okunoye, A and

The White House. (2004). *Homeland Security Presidential Directive 10(HSPD-10):*
Biodefense for the 21st Century. The White House.

The White House. (2007). *Homeland Security Presidential Directive 18 (HSPD-18): Medical*
Countermeasures Against Weapons of Mass Destruction. The White House.

Tomisek. (2002). *Homeland Security: The new Role of Defense.* Strategic Forum 189.

Turner, C. (1988) "*Organizing Information: Principles and Practice*", Clive Bingley, London. Sourced from Aguolu, I. E. (1997) "Accessibility of information: a myth for developing countries?" *Journal of New Library World*, Vol. 98 No. 1 pp. 25-29.

Thuraisingham. (2003). *Web data mining technologies and their applications in*
Business Intelligence and Counter-terrorism. New York: CRC Press.

Turley. R. C. (2002). *Subcommittee on aviation hearing and the future of airline security.*
Panel 1 subcommittee.

UN. (2007). *Security council holds first-ever debate on impact of climate change, 5663rd meeting.* New York: United Nations Department of Public Information.

UNESCO (2002). Institute for statistics, Sub-Saharan Africa Regional Report. UNESCO, 19 April 2002.

Wehn, U. (1998) "*Internet access for all: the obstacles and the signposts*", Development Research Insights, 25, Institute of Development Studies, University of Sussex. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Williams G B (2003), Synchronizing E-Security. Kluwer

Williams. G.B. (2007). Online business security systems.
(Boston), MA: *Springer Verlag.*

Wolfbeis Otto S. "Fiber-optic chemical sensors and biosensors" Analytical Chemistry, vol. 76 No.12, June 15, 2004

Woodrow, W. (1916). *The State, The functions of Government.*

World Bank, (1995) "Harnessing Information for Development", World Bank Group Vision and Strategy, World Bank International Bank for Reconstruction and Development.

World Bank, (1999) "*Knowledge for development*", The World Bank Development Report 1998/1999, Oxford University Press. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Wright. (2008). Technology and terrorism: How the internet facilitates radicalism.
Forensic Examiner , 14-20.

Yim, S. C. (2006). Homeland Security's National Strategy Position: Goals, Objectives,
Measures Assessment. In D. Kamien, *McGrawHill Hnadbook of Homeland Security.*
McGrawHill.
http://news.bbc.co.uk/1/hi/uk/6255960.stm:

Zachaman R. (2004), ICTs and the World of Work weaving a Bright New Fabric or a Tangled Web? Information Technologies and International Development MIT Press.

6. References

Cranor et al (2000), Beyond concern: Understanding Net Users. Attitudes about on-line privacy, The internet upheaval: Raising Questions, seeking answers in communication policy, MIT Press, Cambridge

Foner L.(1996), A security architecture for multi-agent matching. In Proceedings of the International conference on Multi-agent systems, pages 80-86.

Gust and Mathews(2002). 802.11. Wireless Networks- The definitive Guide. O' Reilly

Harrison K(2004). Lessons learned from Cryptography. 2nd International Workshop on wireless security in collaboration with BCS. ISBN: 1-85924-216-2

Hastings G.(2003). 5 common mistakes in Computer forensics

Jakobsson, Wetzel and Yener (2003). Stealth Attacks on Ad-Hoc Wireless Networks IEEE VTC Fall. Reprinted with permission in the 2nd international workshop on wireless security in conjunction with BCS. ISBN: 1-85924-216-2

Mckemmish R.(1999) What is forensic computing? Australian Institute of Criminology (Trends & Issues) in crime and criminal justice. ISSN – 0817-8542, ISBN 0—642-241023. No 118

Negnoponte(1997),. "Agents: From direct manipulation to delegation" Software Agents, J.M Bradshaw, ed. AAAI Press/MIT Press

Patrick A.S (2002). Building Trustworthy Software Agents. IEEE Internet Computing. Nov/Dec

Noblett, Pollit and Presley(2000). Recovering and examining computer forensic evidence

Nwana(1996). Knowledge Engineering Review, Vol. 11, No 3 pp. 205-244

Rotter (1980). " Interpersonal Trust, Trustworthiness, and Gullibility, "Am. Psychologist, vol. 35 no. 1

Rude T (2000). Evidence Seizure Methodology for Computer Forensics, CISSP.

Russell and Norvig (1995). Artificial intelligence. A modern approach. Prentice Hll Series in Artificial Intelligence.

Sommer P(1997). Computer forensics, an introduction. Virtual City Associates

Willaims G.(2004), "Simulating intrusions via synchronizing e-security methodology on global wired-wireless networks" 2nd International Workshop on wireless security in collaboration with BCS. ISBN: 1-85924-216-2
Williams G (2004) Synchronizing E-Security, Kluwer

Wong and Sycara (Adding Security and Trust to Multi-Agent Systems) DARPA contract F30602-98-2-0138 and by ONR Grant N00014-96-1222

Yasinsac et al (2003) Computer Forensics Education. IEEE Security & Privacy

Zand (1972). "Trust and Managerial Problem Solving, "Administrative Science Q. Vol. 17, pp. 229-239

On-line References

www.catsa-acsta.gc.ca (22/02/04)

http://www.house.gov/transporation/aviation/09-21-01/09-21-01memo.html(25/02/04)

http://investor.ncr.com/news/20040114-126604.cfm (28/03/04)

http://www.fairisaac.com/Fairisaac/Solutions/innovations_neural_networks4.htm (27/04/04

http://www.statsoftinc.com/datamine.html#mining (01/04/04)

http://www.dbmsmag.com.9807m01.html (13/02/04)
SearchDatabase.com News Writer.

Appendix 1

This section presents a compilation from Phillips Nizer LLP (2007) on Electronic Communication Privacy Act 47 U.S.C Section 230, Electronic Communications XE "Communications" Privacy Act, Stored Wire and Electronic Communications and Transactional Records Access.

18 U.S.C. §§ 2701-2711§ 2701. Unlawful Access to Stored Communications XE "Communications" (a) Offence - Except as provided in subsection (c) of this section whoever -(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section. (b) Punishment - The punishment for an offence under subsection (a) of this subsection is - (1) if the offence is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain -(A) a fine under this title or imprisonment for not more than one year, or both, in the case of a first offence under this subparagraph; and(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offence under this subparagraph; and(2) a fine under this title or imprisonment for not more than six months, or both, in any other case.(c) Exceptions - Subsection (a) of this section does not apply with respect to conduct authorized(1) by the person or entity providing a wire or electronic communications service;(2) by a user of that service with respect to a communication of or intended for that user; or(3) in section 2703, 2704 or 2518 of this title. § 2702. Disclosure of Contents (a) Prohibitions - Except as provided in subsection (b) - (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service -(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.(b) Exceptions - A person or entity may divulge the contents of a communication (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service; (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or (6) to a law enforcement agency – (A) if such contents -

(i) were inadvertently obtained by the service provider; and(ii) appear to pertain to the commission of a crime.(B) if required by section 227 of the Crime Control Act of 1990. § 2703. Requirements for Governmental Access(a) Contents of Electronic Communications XE "Communications" in Electronic Storage - A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section. (b) Contents of Electronic Communications XE "Communications" in a Remote Computing Service – (1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity -

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purpose of providing any services other than storage or computer processing.(c) Records Concerning Electronic Communication Service or Remote Computing Service – (1)(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to any person other than a governmental entity.(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity - (i) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant;(ii) obtains a court order for such disclosure under subsection (d) of this section;(iii) has the consent of the subscriber or customer to such disclosure; or(iv) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title).(C) A provider of electronic communication service or remote computing service shall disclose to a governmental

entity the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under subparagraph (B).(2) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer. (d) Requirements for Court Order - A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction described in section 3127(2)(A) and shall issue only if the governmental entity offers specific facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.   (e) No Cause of Action Against a Provider Disclosing Information Under This Chapter - No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under this chapter.

(f) Requirement To Preserve Evidence –(1) In general. - A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention - Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewed request by the governmental entity. §2704. Backup Preservation(a) Backup Preservation –1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a). (3) The service provider shall not destroy such backup copy until the later of (A) the delivery of the information; or(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider –(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and(B) Has not initiated proceedings to challenge the request of the governmental entity. (5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its

sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.(b) Customer Challenges – (1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement –(A) stating that the application is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and(B) Stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken there from by the customer. §2705. Delayed Notice(a) Delay of Notification –(1) A governmental entity acting under section 2703(b) of this title may –(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.(2) An adverse result for the purposes of paragraph (1) of this subsection is –(A) endangering the life or physical safety of an individual;(B) flight from prosecution;(C) destruction of or tampering with evidence;(D) intimidation of potential witnesses; or(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application or by certification by a governmental entity, but only in accordance with subsection (b) of this section.(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that –(A) states with reasonable specificity the nature of the law enforcement inquiry; and(B) informs such customer or subscriber – (I) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place; (ii) that notification of such customer or subscriber was delayed; (iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and (iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.(b) Preclusion of Notice to Subject of Governmental Access - A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in –(1) endangering the life or physical safety of an individual;(2) flight from prosecution;(3) destruction of or tampering with evidence;(4) intimidation of potential witnesses; or(5) Otherwise seriously jeopardizing an investigation or unduly delaying a trial.§2706. Cost ReimbursementPayment XE "Payment" - Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored. (b) Amount - The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order

was issued for production of the information).

(c) Exception - The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.§ 2707. Civil ActionCause of Action - Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) Relief - In a civil action under this section, appropriate relief includes –(1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection (c); and (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

Damages - The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court. (d) Disciplinary Actions for Violations - If a court determines that any agency or department of the United States has violated this chapter and the court finds that the circumstances surrounding the violation raise the question whether or not an officer or employee of the agency or department acted wilfully or intentionally with respect to the violation, the agency or department concerned shall promptly initiate a proceeding to determine whether or not disciplinary action is warranted against the employee.

(e) Defence - A good faith reliance on –a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;a request of an investigative or law enforcement officer under section 2518(7) of this title; or (3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defence to any civil or criminal action brought under this chapter or any other law.

(f) Limitation - A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.§ 2708. Exclusivity of RemediesThe remedies and sanctions described in this chapter are the only judicial remedies and sanctions for no constitutional violations of this chapter.§2709. Counterintelligence Access to Telephone XE "Telephone" Toll and Transactional Records

(a) Duty to Provide - A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required Certification - The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director, may -

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that –(A) the name address, length of service, and toll billing records sought are relevant to an authorized foreign counterintelligence investigation; and (B) there are specific facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that -

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with -

(i) an individual who is engaging or has engaged international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or (ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States.

(c) Prohibition of Certain Disclosure - No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

Dissemination by Bureau - The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement That Certain Congressional Bodies Be Informed - On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.§ 2710. <u>Wrongful Disclosure of Video Tape Rental or Sale Records</u>

(a) Definitions - For purposes of this section -

(1) the term "consumer" means any renter, purchaser, or subscriber of goods or services

from a video tape service provider;
(2) the term "ordinary course of business" means only debt collection activities, order fulfilment, request processing, and the transfer of ownership;(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and (4) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) Video Tape Rental and Sale Records(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d);
(2) A video tape service provided may disclose personally identifiable information concerning any consumer – (A) to the consumer; (B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought; (C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;(D) to any person if the disclosure is solely of the names and addresses of consumers and if -

(i) the video tape service provider had provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and
(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;(E) to any person if the disclosure is incident to the ordinary course of business of the video taper service provider; or(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if - (i) the consumer is given reasonable notice, by the person seeking the disclosure of the court proceeding relevant to the issuance of the court order; and
(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure. If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.Civil Action –(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court(2) The court may award - actual damage but not less than liquidated damages in an amount of $2,500; (B) punitive damages;

(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(D) such other preliminary and equitable relief as the court determines to be appropriate.
3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.
4) No liability shall result from lawful disclosure permitted by this section.
(d) Personally Identifiable Information - Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State or a political subdivision of a State.

(e) Destruction of Old Records - A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

(f) Preemption - The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

¶ 2711. Definition for chapter As used in this chapter-1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and (2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communication system.

Source: HYPERLINK "http://www.phillipsnizer.com/library/topics/computer_fraud.cfm" http://www.phillipsnizer.com/library/topics/computer_fraud.cfm: accessed: 25/01/2007. A compilation by Martin Samson