Int. J. Adv. Res. Sci. Technol. Volume 4, Issue 7, 2015, pp.474-480.

IJARST

International Journal of Advanced Research in Science and Technology

journal homepage: www.ijarst.com

ISSN 2319 – 1783 (Print)

ISSN 2320 – 1126 (Online)

Security Challenges in Telecommunication Networks and Mechanisms Used by The Companies in Tanzania

Adum Joseph* and Enock Ernest Chenya

Faculty of Applied Science and Technology, Kampala International University, Dar es Salaam constituent College, Tanzania.

****Corresponding Author's E-mail: josephadum@yahoo.com***

ARTICLEINFO

Article history:

Received 11 Nov. 2015

Accepted 27 Nov. 2015

Available online 06 Dec. 2015

Keywords:

Security challenges,
Information Systems,
Security Mechanisms,
Telecommunication companies,
Airtel Tanzania

ABSTRACT

The major purpose of this research was to assess the security challenges in telecommunication networks, and the mechanism used by Airtel Telecommunication Company in Tanzania to protect its information. The case study research design was used because a case study is a comprehensive description and analysis of a single situation or a number of specific situations. A self-designed structured questionnaire was used to collect data from 150 respondents selected randomly from Information Technology (IT) experts, end users of the system and customers of Airtel Tanzania. The researcher collected 150 completed questionnaires. Data were analyzed using percentage, frequency and statistics. The findings showed that cultural and legal practice when dealing with security across international borders is a complex challenge in security of information system in Airtel Tanzania, and standard mechanisms used to control and protect information system of the telecommunication were Password policy system and user Authentication. It is therefore recommended by the researcher that the standard security measures such as Intrusion Detection systems (IDSs) and Biometrics should be used to deter threats to the system. The researcher also recommend that the company should extensively conduct staff training on how to use the mechanism to protect the information system of Airtel company Tanzania. The use of secure supported applications should be implemented as a mechanism to prevent accidental and intended data loss.

PAPER-QR CODE

IJARST Volume-4, Issue-7

Citation: *Adum Joseph. et.al. Security Challenges in Telecommunication Networks and Mechanisms Used by The Companies in Tanzania, Int. J. Adv. Res. Sci. Technol. Volume 4, Issue 7, 2015, pp.474-480.*

Introduction:

The permanent nature of security threats and the increasing complexity of Information technology (IT) infrastructures are currently leading organizations throughout the world to revise their approaches towards information security. Hiring the Information and Communication Technologies (ICT's) equivalent of military men, i.e. security technologists and white-hat hackers, and entrusting security to them is no longer sufficient.

All over the world, there is the realization that managing secure information is one of the most difficult tasks and challenges to implement and maintain effectively in telecommunication companies. Experience has shown that the more sophisticated hackers can attack routers and firewalls and change the security controls that an organization has established to keep intruders out. Many astute organizations have risen to this challenge by fighting fire with fire that is, they have established a team of technical specialists that attempt to hack their own systems to discover security holes and to ensure that established controls remain as they were intended (Herold F Tipton, 2005).

In developed countries such as United States of America (U.S.A), modern cryptography provides fundamental techniques with which to secure communication and information (Kawachi and

Koshiba, 2006). Cryptographic protocols such as digital signatures, commitment schemes, oblivious transfer schemes and zero-knowledge proof systems have contributed towards the construction of various security systems. There are many works (Goldreich, 2004; Ferguson et al., 2010) that cover such topics as block ciphers, block modes, harsh functions, encryption modes, signatures, message authentication codes, implementation issues and negotiation protocols, among others.

Many computer security standards in China are not compulsory and some regulations applied only to government organizations. To illustrate, Wu stated that at present even the widely available Pretty Good Privacy (PGP) 128-byte encryption program could be downloaded from the Internet in China and private users here could use it legally. Wu said the State Council would likely promulgate compulsory certification laws for encryption products by Fall 1999. When Econoff mentioned Public Security regulations that advise against the use of foreign-origin security software and browsers for "sensitive" uses, Wu dismissed this as a serious restraint on sales, and implied that as long as the foreign software was properly certified it could be used (Wu, 1999).

China's push for the development of indigenous innovation and standards is an important context for evaluating that country's current measures to protect information security.8While China's ex-traordinary economic success has been evident for the past three decades, Chinese industry faces increasing pressure to move from labor-intensive, low-value-added activity into more productive, higher-value-added areas. In fact, China's ability to move up the industrial value chain is an important precondition for the country's continuing rapid economic and social development (Scott Kennedy, 2006).

The Chinese government has strongly encouraged indigenous innovation and has explored various policies to support these goals. The "blueprint" for this is China's "Outline for Medium- and Long-Term Plans for Science and Technology development (2006–2020)." A number of other plans and programs from the Ministry of Science and Technology, like China's 863 Program, also support the development of indigenous innovation (Guojia, 2006).

Users are typically delegated a certain amount of trust. They are expected not to violate the provided trust. In organizations with sensitive information, security policies are used to specify what user actions regarding the system are acceptable. Unfortunately, some users ignore policy and make decisions that affect the confidentiality, integrity, and availability of systems and information. Users that violate their trust can do so through the interfaces provided to access the system as opposed to only through the introduction of malicious software. User interfaces of commercial off-the-shelf (COTS) products may not have built-in policy enforcement mechanisms that are robust enough to support an organizational security policy and prevent these kinds of abuses.

Some operating systems and applications provide mechanisms to enforce policy through configurations. Two mechanisms used to provide policy enforcement include ACLs and policy configurations. Proper configuration of ACLs can support the concept of least privilege and prevent users from directly accessing information for which they are not authorized. However, this is not always completely enforceable on systems that only provide discretionary access control (DAC). For instance, suppose that user A is authorized read access to file S and user N is prohibited by policy from reading S. If A creates a new file C, which is a copy of S, and gives N read access to C, then a policy violation occurs because N has access to the contents of S. In this regard, DAC is unable to support the desired security policy fully.

In Nigeria, the major challenge of information security in telecommunication companies is finding qualified information security staff, which will likely continue to be the case in the near future in majority of African countries. Driving the hiring challenge is the immaturity of the solutions from information security vendors, the limited number of qualified staff available, and the unique blend of information security skills required. Business executives will need to invest more in this area to overcome these challenges. Due to the immature market, lack of standards, and numerous point solutions, training is a problem for security staff. The industry has not had the time to grow the staff necessary for these roles. In addition, the information security challenges keep growing at a rapid pace, constantly expanding the list of technology to be deployed, and the information security staff just can't keep up. This translates into more time and money to get your staff trained on commercially available products (Dr. Alabi, G.A, 1996)

Purpose of the study

The study was conducted to assess the security challenges in telecommunication networks, and the security mechanism used by Telecommunication companies in Tanzania to protect its systems. The following research questions guided the research.

i) What are the security challenges in telecommunication networks faced by Airtel Tanzania
ii) What are the security mechanisms used by Airtel company to protect the information and other systems used by the company

Literature review:

Security challenges in telecommunication networks faced by Airtel Telecom Company Tanzania

Edelson (2010) suggest that security challenges could be categorized based on their effects on the three

fundamental security requirements such as confidentiality, integrity and availability of VoIP networks where threats against confidentiality endanger the overall content of the interaction between two endpoints which can as well expose the call data such as telephone numbers dialed and call durations. Security threats against integrity tend to strongly affect the trust issues on the caller's identity, the recipient's identity, the messages transferred, or the call record logs; while those against the availability of the network resources tend to deny legitimate users access to system resources thereby making it extremely difficult to make or receive a call.

Doherty, N.F, and Fulford H (2006) argue that theft of proprietary information is also a major risk to information security. When intellectual property (IP) is in an electronic form, it is much easier to steal. If this information is stored on computers connected to the Internet, thieves can potentially steal it from anywhere in the world. According to the 2003 CSI/FBI computer crime and security survey in the USA, theft of IP remains the highest reported loss. These types of security weakness will only get worse as the Internet continues to grow in usage and complexity.

According to Clinton K et all (2005), mobile workforce and wireless computing also have emerged as a serious challenge to the telecommunication companies. The arrival of mobile computing devices has had a significant impact on everyday life. Wireless communications liberate employees and consumers from relying on phone lines to communicate. Information availability and communications have greatly increased due to mobile computing devices. With the convenience of these devices, information security concerns increase because the confidential information stored on them needs to be protected.

According to Sanchez et all (2009), the fastest spreading mass mailing worm to date was My Doom in January 2004. At the height of the outbreak, more than 100,000 instances of the worm were intercepted per hour. My Doom relied on people to activate it and enable it to spread. Cleverly disguised as an innocuous text file attachment, unsuspecting users opened the attachment and launched the worm. The rapid spread of these threats makes it increasingly difficult to respond quickly enough to prevent damage. This poses a big challenge to the security of the information systems.

In the current information age, there is clearly a challenge in managing security using the conventional approaches (G. Dhillon and J. Backhouse, 2001). The evolution of business model from being hierarchical-oriented to an emergent organization, form one of the crucial challenges requires serious attention concerning to the Information System Security of the company (A. Kankanhalli, et al, 2003). Current policies and procedure are not ready to support the emergent organization (A. Zuccato, 2007). Emergent company like airtel Tanzania is very dynamic and appears to have higher volatility feature. Interfaces of such systems are primarily designed to support and manage the end user. Designers of the systems may not always consider the implications of the product in an environment where access to sensitive information should be controlled. Likewise, non-security-focused system may not be designed to support an organization's security policy.

According to Goldreich O ED (2004), Brute force attacks involve manual or automated attempt to guess valid passwords. A simple password guessing program can be written in approximately 60 lines of C code or 40 lines of PERL. Many password guessing programs are available on Internet which is a very big challenge in airtel company information system. Most hackers have a "password hit list", which is a collection of default passwords automatically assigned to various system accounts whenever they are installed. Insiders abusing their access are provided the tools to do so from the system designers that do not provide organizations with the flexibility to support a security policy. This represents a security design problem in user interfaces. A number of common elements within application and system interfaces provide avenues for users to circumvent policy. These common features include menu items; standard operating system interfaces; selective policy settings; and application extensibility through mobile code, scripting, and add-ins.

Some applications have the ability to automate internal tasks through scripts. Some script technology, such as JavaScript, enhances the user experience by animating tasks, performing calculations, or automating application operations. In the case of browsers and other applications like Microsoft Office products, local users frequently have access to a script's source code. A malicious user may alter the code to cause the application to perform other functions not originally intended by the script. Likewise, nefarious users may develop their own scripts to subvert the interface or, in the case of a database application, the current transaction.

Security mechanisms used by Airtel Tanzania to protect its systems

Markus and Isomäki (1999) argue that Global System of Mobile network (GSM), which is a widely used mobile phone system, implements several security mechanisms designed to protect confidentiality over radio interfaces, subscriber authentication, subscriber anonymity to external parties, and prevent the use of stolen terminals . However, a speech call made between two GSM operator networks or between a GSM phone and a fixed phone traverses the fixed network, and is subject to the same security considerations in speech and signaling as for a fixed network. CDMA mobile networks are also exposed to the same threats and attack vectors as a GSM network.

According to EU regulations (2002), the data protection standards that apply in the case of public telecommunications networks – including issues of security, privacy and direct marketing are all set up. In applying this rule in practice, telecommunications companies should be mindful of the strong privacy impact of logging the details of particular calls made by individual subscribers. The Data Protection Commissioner's advice is that telecommunications companies should only store such privacy-sensitive data for a limited period of time – say three to six months – to enable routine billing queries to be addressed. The Regulations also introduce rules for the publication of telephone directories, to ensure that the privacy of individual subscribers is safeguarded. Such security mechanism and regulations if adopted by airtel Telecom Company will the regional and international subscribers to be harmonized and regulated appropriately.

Richard.C. et al (2011), argue that airtel Telecommunication Company can use some access control mechanism as one of the best security mechanisms. But they suggest one problem is that Telecommunication Companies and other wireless networks is a multi-hop network which makes it difficult to applied secure access control over different transmission media. But some security mechanism such as AAA (Authentication, Authorization, and Accounting) can be implemented at Airtel Telecom Company. In AAA mechanism, there is central server which provides a secure mechanism for communicating customers. It saves from unauthorized terminal to access data of another trusted terminal. AAA server manages the secure mean of communication between trusted terminals.

Francis .G. et al (2005) argues that obtaining the necessary credentials for information security requires considerable training and experience. The Certified Information Systems Security Professionals (CISSP) credential is an internationally accredited certification and requires passing a test on a broad range of information security topics with a minimum of four years of work experience. Executive will need to consider longer term strategies to address these needs because finding trained staff is not just a question of money but also of the time necessary to build the team around a limited number of qualified staff.

John Kimmins et al (1995) suggest that Biometric access controls is a more sophisticated method of controlling access to computing facilities than badge readers, but the two methods operate in much the same way. Biometric used for identification include fingerprints, handprints, voice patterns, signature samples, and retinal scans. Because biometrics cannot be lost, stolen, or shared, they provide a higher level of security than badges.

Access control is a security mechanism which is the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. Access Control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. The Access Control Framework describes a model that includes all aspects of access control in Open Systems, the relationship to other security functions (such as Authentication and Audit), and the management requirements for Access Control (http://www.itu.int/ITU-T/ studygroups/com17/telsecurity html).

Methodology:

The researcher used case study research design because a case study is a comprehensive description and analysis of a single situation or a number of specific situations. A self-designed structured questionnaire was used to collect data from the 100 respondents selected randomly from Information Technology (IT) experts, end users of the system and customers of Airtel Tanzania.

Table 1: Distribution of the sample population of the study

Respondents	Number	Percentages (%)
Information Technology (IT) expert	10	06.7
End users of the system	40	26.7
Airtel customers	100	66.6
Total	150	100%

Closed questionnaire was designed to collect data from Airtel headquarter staff to customers in the city, it was used to collect data from a wide range of individuals as it provided a direct answers since it comprised of written questions that were filled by the respondents.

The face validity of questionnaire was established by giving the questionnaire to research experts for scrutiny on its validity. The questionnaire was administered to 150 respondents as indicated in table 1 above.

Analysis of the findings

Table 2: Management of regional and global network regulations is a complex

Category	Frequency	Percent (%)
Strongly disagree	1	0.6
Disagree	10	6.6
Undecided	18	12
Agree	32	21.3
Strongly agree	89	59.3
Total	150	100%

Source: Primary field data (2015)

The table 2 above shows that the management of regional data security of the telecommunication is very

challenging as it is indicated by majority of respondents where 59.3% of the respondents strongly believe that regional security management due to other countries' culture and regulations regarding data security and privacy is very difficult in such protected sectors. When looking at legal and regulatory requirements, they have common thread to address issues stemming from fraud, theft, and malfeasance, from both internal and external threat actors, of a particular data set of information. These threat actors could be located anywhere in the world. Increasing data-breach reports have shown the gaps and holes in the security posture of the company. Criminal organizations are using these security shortfalls to gain sensitive information for profit. Senior management is being held responsible for the security of the data that is within the company. However, 12% of the respondents neither agree nor disagree with this case.

This finding seems to be the contentious with Michael Nelson (2011) who argues that in some cases, governments themselves may present a threat to data security in some countries, the instances in which government bodies, such as police or intelligence agencies may access personal data are not clear to service providers (Airtel telecommunication company) or their customers.

Table 3: Information System Security policies are defined but not enforced and implemented

Category	Frequency	Percentage (%)
Strongly disagree	1	0.6
Disagree	16	10.6
Undecided	12	08
Agree	42	28
Strongly agree	79	52.6
Total	150	100

Source: Primary field data (2015)

The table 3 above showed that 52.6% of the respondents strongly agreed that information systems security policies are well defined and stipulated but are not practiced, enforced and implemented, this is a big challenge and pose a security risks, threats and vulnerability to the information, network and the entire systems of the company. This justifies why most of the telecommunication companies loose many sensitive information and data despite they have a well documented and regulated policies on information system security policy within the company. Other respondents (08%) however are not aware and not sure if such case exists in a Telecommunication Company like airtel Tanzania. They could not verify the fact or false about that practice exist or doesn't in the company. Some respondents were not in agreement with such issues to exist in the company as 10.6% of the respondents did not agree. They are hopeful that every policies regarding network security and any other systems in the company are well defined, regulated and enforced which are in operation.

This finding is in contentious to current literature which seemed to be consistent on security policy definition, enforcement and implementation. Schneier & Bruce (2000), state that Policies, standards, guidelines, and training materials that are obsolete and not enforced are particularly dangerous to Telecom company like airtel because management is often deceived into believing that security policies do not exist and that the Company is operating more effectively than it actually is. All Telecom Companies need to periodically review, test, and discard un-enforced and otherwise obsolete rules, controls, and procedures to avoid this false sense of security. An alternative to periodic reviews is to specify a time limit for applying policies and standards and assign limited life span to mandatory controls, specifying when they should become effective and when they should be nullified or replaced, a technique generally referred to as sunsetting.

Table 4: Hackers manipulate the network systems and alter it to make free calls

Category	Frequency	Percent (%)
Strongly disagree	2	1.3
Disagree	08	5.3
Undecided	22	14
Agree	28	18.6
Strongly agree	90	60
Total	150	100

Source: Primary field data (2015)

From the table 4 above, majority of the respondents believe with the information that hackers manipulate and invade the systems as it is indicated by 60% of the respondents who strongly agree with that. They believe that it is because of this that most telecom companies in Tanzania loose many data about the customers. Some respondents were not sure whether hackers can invade and access the telecommunication data and information as it was indicated by 14% of the respondents.

Table 5: Security mechanisms used by Airtel Tanzania

	Mostly used		Used sometime		Least use		Not Use	
	Freq	Per (%)	Freq	Per (%)	Freq	Per (%)	Freq	Per (%)
IDS	15	03.3	10	06.6	69	46	76	50.6
Bio	15	10	57	38	57	38	64	42.6
PP	75	50	60	40	10	06.6	02	01.3
PS	55	36.6	23	15.3	14	09.3	08	05.3
TT	150	100	150	100	150	100	150	100

Source: Primary field data (2015)

In support to this finding, Boman K et al. (2002) agree and argue that, with the integration of the core 3G networks, the PSTN and the Internet, the networks have opened up additional vulnerabilities and provided malicious attackers easy access through the Cross Network Servers. The Internet is open and accessible to

one and all with simple equipment. It is also very easy for malicious attackers to break into Internet servers due to much vulnerability.

Table 5 above shows the response from the selected respondents on security mechanisms used by Airtel Tanzania to protect its network and other systems in the Company. The result showed that more than half of the respondents (50%) agree that airtel Company Tanzania mostly use password police (PP) as a method of authentication to protect its system. This implies that it is the easiest mechanism to understand and simple for users to apply in order to access the system at their convenience, while 36.6% of the respondents indicated and believe that physical security (PS) is the most appropriate mechanism which the company always uses to protect and guards its information, networks and other systems of the company. Physical security mechanisms involve deployment of man force and other physical equipments to protect the information and other systems of the company. The result also showed that 10% of the respondents believe that airtel Tanzania mostly uses Biometric (Bio) as its security mechanisms to protect its information and other systems of the company, because of its nature of security protection. *Biometric* security mechanism is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Intrusion Detection System (IDS) is the mechanism that must have been believed by the respondents not being practiced by the company as it was shown by the least number of respondents; only 3.3% of the respondents believe that it is the mechanism mostly being applied as its security mechanism for information and other systems protection in the company.

Conclusion:

The study was conducted purposely to determine challenges to telecommunication networks and the security mechanisms used by Airtel Company as a method of data protection. The findings of this research seem to indicate that the management of data security and privacy is a critical challenge especially regionally. When looking at legal and regulatory requirements, they have common thread to address issues stemming from fraud, theft, and malfeasance, from both internal and external threat actors, of a particular data set of information. These threat actors could be located anywhere in the world. Increasing data-breach reports have shown the gaps and holes in the security posture of the company. Criminal organizations are using these security shortfalls to gain sensitive information for profit. Senior management is being held responsible for the security of the data that is within the company.

Based on the results of the study, telecommunication companies are faced with security challenges which it is essential that telecom company operators need to put their best foot forward to secure their networks and services. It is also critical that they conduct periodic risk assessments of their networks and twist their security programs to adapt to the ever-changing security environment. As new vulnerabilities are discovered, new threats emerge, and security products evolve, the company need to take judicious decisions to choose the right security solutions and methodologies, in line with their risk appetite.

The findings also point out security mechanisms use for data protection and privacy of the company. Security mechanism for data and information needs to be applied in all areas of data, information and privacy about customers as security threats are not just focused on telecom companies, but any type of company. For telecommunication companies, more vigilance is required at the global level, which is fed by local levels of oversight, can keep the company management abreast of the regulatory climate the company faces, and while reducing fraud, theft and malfeasance.

Recommendations and further studies:

Recommendations:

The researcher recommend that practicing strong governance and security practices will create fewer chances of security incidents from occurring while taking a proactive stance when a true security incident occurs. Appropriate communications at the local level will create a partnership with law enforcement that is invaluable during international issues.

The telecommunication companies need to design, develop and practice security framework to respond with the dynamic emergence of security issues in networks and information systems around the globe. This will avoid the vulnerable threats to the networks and telecommunication industries.

Further study:

Basing on the findings of the research, the researcher identified the areas that still needed to be studied and provided some recommendations which will be of great help for future research.

During the research as well as the analysis process several other ideas turned up that could be of interest and worthwhile to be investigated more thoroughly. It would be interesting to study more closely the relationship between the network management and users access control in telecommunication systems in Tanzania. The study would clearly demonstrate mechanisms to control and prevent both passive and active attacks to the systems.

The researcher also recommends that research need to be conducted to implement and establish Directive on attacks against information systems which aim to strengthen the fight against cyber-crime

Reference:

1. A Zuccato, “Holistic security management framework applied in electronic commerce,” *Computers & Security*, vol. 26, no. 3, 2007, pp. 256-265.

2. A Kankanhalli, et al., "An integrative study of information systems security effectiveness," *International Journal of Information Management*, vol. 23, no. 2, 2003, pp. 139-154.
3. Boman K, Horn G, Howard P,Niemi V, "UMTS security", Electronics & Communication Engineering Journal, Volume: 14 , Issue: 5 , Oct. 2002, Pages:191 - 204
4. Doherty.N.F, and Fulford.H. (2006). ""Aligning the Information Security Policy with the strategic information systems plan". *Computers & Security* 25(2): 55-63.
5. Edelson, ―Voice over IP: Security pitfalls, *Network. Security*, no. 2, pp. 4–7, Feb. 2010.
6. EU (2002), *European Communities (Data Protection and Privacy in Telecommunications) Regulations, 2002* (Statutory Instrument 192 of 2002) – came into effect on 8th May 2002.
7. Ferguson, N., B. Schineier, Eds. (2010), *Cyptography Engineering: Design principles and practical applications*, Wiley publishing
8. Francis G, Clinton K (2005). "Computer forensics laboratory and tools" *Journal of Computer Science in Colleges* 20(6): 143-150
9. G Dhillon and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal* vol. 11, no. 2, 2001, pp. 127-153.
10. Goldreich.O., ED. (2004). "*Foundations of Cryptography: Basic Applications*, Cambridge University Press.
11. Harold F.Tipton (2005). Handbook of Information Security management: https://www.cccure.org/Documents/HISM/ewtoc.html.
12. http://www.itu.int/ITU-T/studygroups/com17/telsecurity.html)
13. Kawachi, A. and T. Koshiba (2006). Progress in Quantum Computational Cryptography. *Journal of Universial Computer Science* 12 (6): 691-709.
14. Markus and Isomäki (1999), Security in the Traditional Telecommunications Networks and in the Internet", November 1999.
15. Michael Nelson (2011), telephone interview by USITC staff, August 11, 2011.
16. Okechukwu E.muogilim, kok-keong loo , Richard comely "Wireless Mesh Network security: a traffic engineering management approach " Journal of Network and Computer Applications 34 (2011) 478–491.
17. Rocke (2001), Is the Good News about Compliance Good News about Cooperation?" Downs, Rocke, Barsoom, International Organization, Vol. 50, No. 3, pp. 379-406
18. Sanchez L. E., A. S.O. Parra, et al. (2009). "Managing Security and its maturity in small and medium sized Enterprises" *Journal of University Computer Science* 15(15): 3038-3058
19. Schneier, Bruce. Secret and Lies: Digital Security in a Networked World. Wiley Computer Publishing, 2000.
20. Sean M. Price (2009), *Information Security Management Handbook*, 2009 CD-ROM Edition
21. State Council of the People's Republic of China, "Guojia zhongchangji kexue he jishu fazhan guihua gangyao [Outline for medium-and long-term plans for science and technology development],2006–2020,"February 9, 2006, http://www.gov.cn/jrzg/2006-02/09/content_183787.htm.
22. Wu (1999), *Information Security* a June report from U.S. Embassy Beijing Scott Kennedy, "The Political Economy of Standards Coalitions: Explaining China's Involvement in High-Tech Standards Wars," Asia Policy 2 (July 2006): 41–62;