Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.7, No.3, 2017

Cyber Security: Basics in Fighting Computer Attacks and Crimes

Ewurah S.K Mahama Prof Xu Xiaolin
Huazhong University of Science and Technology
College of Public Administration, 1037 Luoyu Road, Wuhan 430074, PR China

Abstract
It is clear that computers and information systems are central in daily business operations in both public and private sectors. E-commerce and eGovernance have gained international attention as substitutes for the human riddled snail pace management systems. However, computers and ICTs do not only replace the human inefficiencies but also assume human attacks and sicknesses known as cyber attacks and computer crimes. They range from hacker's activities to malwares. This paper explored the occurrences and efforts in mitigating them through thorough literature review and desk research.
Keywords: Cyber Security, Computer Crimes, Data Breaches

1 Introduction

Computers and Systems are not only replacing humans at work but also inheriting human disorders. They are made of hard and soft components and malfunction if hardware breaks down. However, businesses, governments, and private associations, such as NGOs depend on these information systems and ICTs for their survival. This makes critical infrastructure highly vulnerable if computers fail. In eGovernment installations, information is the lifeblood of government business and ICTs therefore play a pivotal role in many national and local administrations. Government exchanges information and knowledge with citizens, between citizens with other governments, and among government entities in eGovernment systems. We derive a variety of different ends from these systems (World Bank, 2009). However, these systems have become vulnerable and insecure due to cyber attacks. These vulnerabilities occur due to outdated software and policies (Miller, 2007). The Internet is global in nature and that makes it possible for hackers to attack and do harm anywhere with any device in the world. We must not ignore that in this complex networked world, there are bad guys out there seeking to take advantage of users to create havoc and /or cause harm for their own commercial, political and social gain. Some of the technologies that are targeted cyber criminals include email, instant messaging, cell phones the World Wide Web, social networking and global positioning systems. Cyber warfare is also on the move and poses as a threat to critical infrastructure of modern societies. The targets are major health, financial, government, and industrial institutions to destroy or phish their information systems. For instance, it has been observed that 90 per cent of them worldwide agree that they have not prepared enough to protect themselves against cyber crime or computer attacks. Taiwan, US, China, Russia and South Korea are targets of attacks. Information systems now are ubiquitous like the telephone system. Thus, computers are connected to another in an to exchange data through communication lines such as digital subscriber line (DSL) lines or cable modems and become vulnerable to penetration by outsiders. The fixed Internet addresses become fixed target for hackers. The threat of cyber-criminal activity is worrisome and requires multi-stakeholder approach to fight it. Despite the above narrative, there is little research on cyber security/computer attacks and awareness creation in Ghana (Boateng et al., 2010)

1.1 Research Methods

The paper was purely exploratory in design. The approach was therefore mostly ingrained in qualitative research (Yin, 2003). In order to establish the methodological approaches that have been used in the literature, we have classified them into non-empirical and empirical with reference to Alavi and Carlson (1992). The non-empirical articles include conceptual orientation and illustrative articles. These articles primarily focus on ideas, frameworks, models and speculation about the policies of cyber security and computer crimes. Based on the insights derived from the theories, conceptual orientation articles, and documents we documented and established conceptual frameworks, ICT applications, and policies of data breaches (e.g., Laudon and Laudon, 2014, Eversheds, 2000). They also sought suggestions from practitioners. The illustrative articles described authors' opinions about ICT applications and security policies and gave practical advice and guidance for improving them (e.g., FireEye, 2013; US Homeland Security Cyber Security R&D Center, 2009; Farwell and Rohozinski, 2011; Tankard, 2011). The common approach for collecting data in the select empirical literature is through surveys. Most of these articles are cross sectional(e.g., NIST (2014), ITU-T (2012), ISO (2012)), while some studies used a longitudinal survey (Helmbrecht et al., 2013). Finally, case study (Laudon and Laudon, 2014) and field study (Baoteng *etal*, 2010) are also used to collect data. The paper is generally a desk and literature reviews and findings therefore informed. Section two highlights some of the incidences of computer attacks and the processes involved. Section three and four provide for some proposed solutions and conclusion respectively.

2 Computer/Cyber Attacks Trends

Systems Security and user Privacy have been described as some of the areas where eGovernment faces obstacles (Jaeger, 2003). Computers are in committing crimes or targets of hackers as shown in table 8 in the world of cyber security and computer attacks. Information systems hold data on citizens' legal matters and health issues that are sensitive to be protected. Systems and data protection is therefore key for the success of any eGovernment systems and ICTs in general. For instance, the same technology that links you to people internationally can also be used for monitoring your personal conversation (Strickland, Baldwin, & Justen, 2005). Also, the technology you use in to voting securely and with no errors, it can be used to rig election through malicious software (e.g., 2016 US-Russia rigging allegation). The control of the systems is variously been called Googlearchy/Googleocracy issues (Hindman, 2009) or infocracy (Snellen, 2002; Zuurmond, 1998). In brief, computer crime is a challenge for both public and private sectors and employees are prime suspects of such crimes. They use their computers in committing these crimes internally. Hence, these computers can be classified as both instruments and targets in cyber crime as shown in table 1.

Tabe 1: Table computers as instruments and targets

COMPUTERS AS TARGETS OF CRIME	**COMPUTERS AS INSTRUMENTS OF CRIME**
Breaching the confidentiality of protected computerized data	Theft of trade secrets
Accessing a computer system without authority	Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and video
Knowingly accessing a protected computer to commit fraud	Schemes to defraud
Intentionally accessing a protected computer and causing damage, negligently or deliberately	Using e-mail for threats or harassment
Knowingly transmitting a program, program code, or command that intentionally causes damage to a protected computer	Intentionally attempting to intercept electronic communication
Threatening to cause damage to a protected computer	Illegally accessing stored electronic communications, including e-mail and voice mail
	Transmitting or possessing child pornography using a computer

Information systems at different offices are networked and an attack at any access point has great domino effect on the whole Internet if there are no security measures. The potential for abuse or fraud has a universal consequence in the network. According to a survey, malware infection (67%) is the most common type of attack experienced, The rest are phishing fraud (39%), insider abuse (25%), attacks by botnets (29%), and laptop and mobile hardware theft (34%) and the cost of this is significant (Laudon and Laudon, 2014). The table 2 below shows some of these crimes or attacks.

Table 2: Cyber/Computer Crimes

CYBER/COMPUTER CRIMES	DESCRIPTION
Social engineering	Tricking employees into revealing their passwords by pretending to be legitimate members of the company in need of information
Click fraud	Fraudulently clicking on an online ad without any intention of learning more about the advertiser or making a purchase
Pharming	Redirects users to a bogus Web page, even when the individual types the correct Web page address into his or her browser
Evil twins	Wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet, such as those in airport lounges, hotels, or coffee shops.
Phishing	Setting up fake Web sites or sending e-mail messages that look like those of legitimate businesses to ask users for confidential personal data
Identity theft	A crime in which an imposter obtains key pieces of personal information, such as social security identification numbers, driver's license numbers, or credit card numbers, to impersonate someone else.
Cyber warfare	A state-sponsored activity designed to cripple and defeat another state or nation by penetrating its computers or networks for the purposes of causing damage and disruption.
Hacking	To gain unauthorized access to a computer system
Spoofing	Involve redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination
Denial-of-service (DoS)	Hackers flood a network server or Web server with many thousands of false communications or requests for services to crash the network.
Sniffing	Illegal eavesdropping program that monitors information traveling over a network
SQL injection attacks	SQL injection attacks take advantage of vulnerabilities in poorly coded Web application software to introduce malicious program code into a company's systems and networks.
Viruses	Spread from computer to computer when humans take an action, such as sending an e-mail attachment or copying an infected file
Worms	Independent computer programs that copy themselves from one computer to other computers over a network
Trojan horse	A software program that appears to be benign but then does something other than expected

Source: (Laudon and Laudon, 2014)

2.1 Data breaches and Cyber challenges

Trust in information systems raise people acceptability for ICT systems implementation. (Marsh & Dibben, 2003). If citizens have trust in government, they will be willing to use eGovernment services (Tolbert & Mossberger, 2006). The rustworthiness therefore is key to convince people to use eGovernment services (Carter & Belanger, 2006). In the context of eGovernment, the trust issue arises from concerns about sharing security issues. In 2011, 351 responses made of experts from U.S. universities and banks reported that 46 percent experienced a computer insecurity and data breach within that year. These attacks target sensitive information and authentication credentials (Fire Eye, 2013). It is difficult to fight most of the attacks because they are well coordinated, targeted and increasingly sophisticated, resulting in persistent attacks (Farwell and Rohozinski, 2011; Tankard, 2011). The main problem is how to identify the trends at the early stages (cf. ENISA report, Helmbrecht et al., 2013). However, we can't afford to watch on as they happen due to the huge liabilities involved such as defamation of officials through email harassment and criminal issues (such as breach of copyright, obscenity, other relevant legislation or data protection) (Eversheds, 2000). It has been observed network security breaches are caused due to user lack of knowledge. Both systems specialists and end users commit such errors. End users especially enter faulty data thereby introducing errors during data processing because they don't follow the proper instructions or using proper computer equipment. ICT specialists too may introduce serrors as they develop and design software. Table3 shows some of these high cases of data breaches and computer infections worldwide reported by Laudon and Laudon (2014)

Table 3: Data Breaches and Computer Infections

DATA BREACH	DESCRIPTION
U.S. Veterans Affairs Department	In 2006, the names, birth dates, and social security numbers of 17.5 million military veterans and personnel were stolen from a laptop that a Department of Veterans Affairs employee had taken home. The VA spent at least $25 million to run call centers, send out mailings, and pay for a year of a credit monitoring service for victims.
Heartland Payment Systems	In 2008, criminals led by Miami hacker Albert Gonzales installed spying software on the computer network of Heartland Payment Systems, a payment processor based in Princeton, NJ, and stole the numbers of as many as 100 million credit and debit cards. Gonzales was sentenced in 2010 to 20 years in federal prison, and Heartland paid about $140 million in fines and settlements.
TJX	A 2007 data breach at TJX, the retailer that owns national chains including TJ Maxx and Marshalls, cost at least $250 million. Cyber criminals took more than 45 million credit and debit card numbers, some of which were used later to buy millions of dollars in electronics from Walmart and elsewhere. Albert Gonzales, who played a major role in the Heartland hack, was linked to this cyber attack as well.
Epsilon	In March 2011, hackers stole millions of names and e-mail addresses from the Epsilon e-mail marketing firm, which handles e-mail lists for major retailers and banks like Best Buy, JPMorgan, TiVo, and Walgreens. Costs could range from $100 million to $4 billion, depending on what happens to the stolen data, with most of the costs from losing customers due to a damaged reputation.
Sony	In April 2011, hackers obtained personal information, including credit, debit, and bank account numbers, from over 100 million PlayStation Network users and Sony Online Entertainment users. The breach could cost Sony and credit card issuers up to a total of $2 billion.

For computer viruses, Symantec said the number of bad software in the world is more than good software in 2007, and every 10 downloads contain one bad from the Web (Drew and Kopytoff, 2011). According to them, small businesses suffer 36 percent of computer attacks today than big companies due to the small companies incapacity to shield against different types of threats (Symantec, 2012). The following examples in table 4 are some of these viruses and infections.

Table4: Computer viruses/infections

NAME	TYPE	DESCRIPTION
Conficker (aka Downadup, Downup)	Worm	First detected in November 2008 and still prevalent. Uses flaws in Windows software to takeover machines and link them into a virtual computer that can be commanded remotely. Hadmore than 5 million computers worldwide under its control. Difficult to eradicate.
Storm	Worm/ Trojan horse	First identified in January 2007. Spreads via e-mail spam with a fake attachment. Infected up to10 million computers, causing them to join its zombie network of computers engaged incriminal activity.
Sasser.ftp	Worm	First appeared in May 2004. Spread over the Internet by attacking random IP addresses. Causes computers to continually crash and reboot, and infected computers to search for more victims. Affected millions of computers worldwide, disrupting British Airways flight check-ins, operations of British coast guard stations, Hong Kong hospitals, Taiwan post office branches, and Australia's Westpac Bank. Sasser and its variants caused an estimated $14.8 billion to $18.6 billion in damages worldwide.
MyDoom.A	Worm	First appeared on January 26, 2004. Spreads as an e-mail attachment. Sends e-mail to addresses harvested from infected machines, forging the sender's address. At its peak, this worm lowered global Internet performance by 10 percent and Web page loading times by as much as 50percent. Was programmed to stop spreading after February 12, 2004.
Sobig.F	Worm	First detected on August 19, 2003. Spreads via e-mail attachments and sends massive amounts of mail with forged sender information. Deactivated itself on September 10, 2003, after infecting more than 1 million PCs and doing $5 to $10 billion in damage.
ILOVEYOU	Virus	First detected on May 3, 2000. Script virus written in Visual Basic script and transmitted as an attachment to e-mail with the subject line ILOVEYOU. Overwrites music, image, and other files with a copy of itself and did an estimated $10 billion to $15 billion in damage.
Melissa	Macro virus/ worm	First appeared in March 1999. Word macro script mailing infected Word file to first 50 entries in user's Microsoft Outlook address book. Infected 15 to 29 percent of all business PCs, causing $300 million to $600 million in damage.

3. Efforts In Fighting Cyber Menace

3.1 Internet Monitoring

ICTs are at the heart of running an effective business. They are distributed both within and through out the organisation agencies within their business environment. Most companies or organisations would like to exercise control over the use of these computers by introducing software that can enable extensive monitoring of personnel PC and Internet use (Laudon and Laudon, 2014). Some employees have full access to organisation ICTs and information systems and some abuse the easygoing nature of the workplace internet where strict AUP is lacking in browsing the Web, surfing social media sites, and consuming a huge volume of bandwidth for downloading stuff. According to research, 46 percent of surveyed agencies experienced an attack the previous past year and 25% is caused by insider abuse (Laudon and Laudon, 2014). As a matter of policy principle, employee internet and ICTs activity should be guided against frequent use of social media (e.g., Twitter and Facebook) and other networking sites; personnel login; visit to adult sites; logout times; and the copying or downloading of confidential information. There are many ways to institute such monitoring mechanism. The common ones include sending the software as an e-mail attachment to staff as well as adding it to the handbook of them. The policy can also be made part of the employee working conditions in the organisation. Monitors can use the software to trace marks of usage and log keystrokes. In additions, there are some traditional ways that employers can use to control their employees in the offices. These are opening checking telephone logs, collecting information from point-of-sale terminals; recording telephone calls and getting information from credit reference agencies. The domino effect is that some employees will get angered at the concept of being monitored but at the end, it will definitely restore order, increase productivity and reduce activity on nonbusiness apps. The monitoring system has a lot of benefits for employees as it does for the employers. As we can see in the foregoing, it can monitor exactly what an individual is doing, so the software can facilitate in troubleshooting and staff training. It follows the exact problem that happens at any given time. Also, it helps organisations to reports easily to CERTs. The monitoring software records and tracks all data for credit card transactions. There is no argument that the employers have the right to make sure staff online activity is not harmful or illegal to the organisation. Nonetheless, under many data protection laws it is clear that employers must make sure the law is followed laws.

3.2 Information sharing

The best way is sharing of Internet challenges and current status for all organizations including national authorities (Hernandez-Ardieta et al., 2013. There are three ways to do: listing of security steps information sharing; reporting security loopholes, and reporting data breaches (Gordon et al., 2006). Currently, the most effective security information sharing is normally achieved via informal relationships and ad-hoc (US Homeland Security Cyber Security R&D Center, 2009). Information is power and sharing it seems hawking your power, which have serious implications or challenges. These challenges are rooted deeply because cyber issues sharing needs effort of multi-stage cooperation. The interdependence between information systems and the power , the attacking agent using to cause attacks showed its capability and it is crucial. For example, questions about the legal dependencies and regulatory compliance, which allowed to share when and what in the organisation including what can we learn from current implementations of Security and control policies are dear to the sharing process design. Many control bodies have emerged, including NIST (2014), ITU-T (2012), ENISA, ETSI and ISO (2012) recommended for the creation of national cyber security centers, (Computer Emergency Response Team (CERT)) which are currently surfacing all over the world. These control teams play aggregating role and coordinating security occurrence using electronic means such as file exchange/storage, email, VoIP, IRC and the Web (ENISA, 2011). NIST, ENISA, ETSI and ISO already created standards for this effect, and will also upgrade old regulations for the future. Accordingly, Ghana had also established a Computer Emergency Response Team (CERT) that stands ready to respond to cyber-attacks, albeit to match Ghana's own realities and aspirations in fighting cyber crimes and computer attacks. The focus is on raising awareness of cyber-related risks by building resilience against attacks, intrusions, and malware and security failures. In 2015, Cabinet had approved Ghana's accession to the Budapest Convention on cyber-crime. This Convention pursues criminal policy to protect countries against cyber crime. In addition, the following elements can also help in information sharing effort to fight these attacks (DHS, 2003; OMB, 2005):

- Review: Of data security policies to ensure they are working as intended; that review being itself reported on to some central body, including the reporting of any data deficiencies (agencies clearly having to balance here the embarrassment of reporting deficiencies versus the risk of some deliberately unreported deficiency later coming to public attention);
- Incident reporting: Reporting of data security incidents both within and outside the agency;
- Collaboration: Working with the private sector on areas of critical data infrastructure, and sharing of knowledge and warnings;
- Intelligence: Greater efforts to identify sources of data attacks and

- Continuity: Emphasis on robust contingency planning to ensure feedbacks in case key eGovernment systems are attacked.

3.4 Data and systems protection mechanism

Data and Security issues are being partly studied (Cavusoglu et al., 2004; Campbell et al., 2003; Gordon and Loeb, 2001, 2002, 2003; Hausken, 2006; Schenk and Schenk, 2002; Gordon et al., 2006 and Tanaka et al., 2005). To prevent the kind of problem in the foregoing, many public agencies use both general and application controls to safeguard and restore client's confidence in eGovernment systems. The input controls are most important; they can be built into the process of data entry in the system. Normally, if the security is compromised, a programmed message pops up indicating direction on the challenge, and no entry can be allowed until the problem is no more in the system. General controls can also be followed to secure computer systems (Heeks, 2004.). These controls are grouped into three main controls: Malware to address virus, fire or power issues (e.g. encryption and firewalls); Communications to monitor user access over computer systems and Access controls for checking user access to digital and physical components of an eGovernment system (e.g. passwords and security guards). Such controls represent one way in which agencies can make sure network based systems are formal, secure, consistent and organizationally protected. The worry is that, many companies do not regulate their systems. Many experts in the security sector blame lack of liability for damages on customers by organisations account for their loose security and control policies (Laudon and Laudon, 2014). Box 2&3 contain some of the guiding policy principles for Internet acceptable use policies (AUP) and methods for reviewing, protecting and processing data in organisations recommended by Pell, 1999.

Box 2 Internet Acceptable Use Policy (Pell, 1999):

- Acceptable Use: Internet use is intended to support organizational goals, within organizational guidelines.
- Privileges: Internet use is a privilege, not a right, which can be withdrawn.
- Privacy: Internet use can be monitored and employees can have no expectation of privacy.
- Email Guidelines: On good practice in email use over the Internet.[8]
- Unacceptable Use: The Internet is not to be used for purposes conflicting with departmental goals or for illegal or unethical purposes. This includes personal usage (though, see discussion in main text) and transmission of material that is likely to be pornographic, racist or sexist; that contains language inappropriate for an office environment; or that contains a virus. It also includes sharing accounts or sending messages in someone else's name.
- Penalties: Inappropriate use will result in account cancellation. Misuse can result in disciplinary action, potentially leading to job termination, or prosecution for illegal actions.
- Services: No warranties are provided, nor is there any responsibility for the accuracy of information obtained; there is no responsibility for damages suffered while using the Internet.
- Security: Security guidelines must be followed

Box 3 Reviewing Sensitive Public Information

The following questions will assist security professionals in reviewing sensitive information that has been, or could be, made publicly accessible.

- Has the information been cleared and authorized for public release?
- What impact could the information have if it was inadvertently transferred to an unintended audience?
- Does the information provide details concerning enterprise security?
- Does the information contain personnel information such as biographical data, addresses, etc.?
- How could someone intent on causing harm misuse the information?
- What instructions should be given to legitimate custodians of sensitive information with regard to disseminating the information to other parties such as contractors?
- Could this information be dangerous if it were used in conjunction with other publicly available information?
- Could someone use the information to target personnel, facilities or operations?
- Could the same or similar information be found elsewhere?
- Does the information increase the attractiveness of a target? (OCIPEP, 2002)

4. Conclusion

The management of any information system (s) and ICT infrastructure involves activities aim at ensuring the availability, efficacy and efficiency of a given physical and human system and its related information technology facilities, networks and assets. CERTs can take advantage of the discovering covert cyber attacks and new malwares by issuing early warnings and advice about how to secure networks, and selectively distribute threat intelligence data to protect computers and information systems. This paper provided some insights to motivate the need in detail and worked out the requirements for an information sharing system and security policy guidelines. We highlight many efforts in creating awareness about legal aspects, system vulnerability ,and security policieswith respect to standardization bodies such as ISO and the National Institute of Standards and Technology (NIST). Thus, the role(s) of certain establishments and structures such as Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), are considered and

evaluated in terms of what we could learn from them in terms of applied processes, available protocols and implemented policies. We conclude with a critical review of the state of the art literature on cyber issues and highlight important considerations when building effective security information sharing platforms for the future. We recommend and conclude that it is of the utmost importance to develop appropriate tools and methods to assist in designing and implementing secure systems in a way that guarantee reliable information systems.

Reference:

Alavi, M., & Carlson, P. (1992) A review of MIS research and disciplinary development. Journal of Management Information Systems, 8(4), 45–62

Boateng, R., Avevor,I., Longe, O., Mbarika, V., Isabalija, Stephen R. (2010) Cyber Crime and Criminality in Ghana: Its Forms and Implications. Americas Conference on Information Systems (AMCIS)

Campbell, K., Gordon, L., Loeb, M., Zhou, L. (200) The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. J. Comput. Security 11 (3), 431–448.

Carter, L., & Belanger, F. (2006) The utilization of e-government services: Citizen trust, innovation, and acceptance factors. Information Systems Journal, 15(1), 5–25.

Cavusoglu, H., Mishra, B., Raghunathan, S. (2004) The effect of internet security breach announcements on shareholder wealth. Int. J. Electron. Commerce 9 (1), 69–104.

DHS (2003) The National Strategy to Secure Cyberspace. Washington, DC: Department of Homeland Security.

Drew, Christopher and Verne G. Kopytoff. (2011) "Deploying New Tools to Stop the Hackers." The New York Times

Eversheds (2000) E-Government, Best Value and the Law. Northampton: Society of Information Technology Management.

Gordon, L.A., Loeb, M., Lucyshyn, W., Richardson, R. (2006) CSI/FBI computer crime and security survey, http://www.gocsi.com/.

Gordon, L.A., Loeb, M.(2001) Using information security as a response to competitor analysis systems. Commun. ACM 44 (9), 70–75.

Hausken, K. (2006) Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. Informat. Syst. Frontiers 8 (5), 338–349.

Hindman, M. (2009) The myth of digital democracy. Princeton, NJ: Princeton University Press.

Laudon, Kenneth C. and Laudon, Jane P . (2014) " Management Information Systems: Managing the Digital Firm" NY: Pearson Education

McCue, A. (2002) 'Hackers target vital organisations', Computing, 29 March: 8.

Marsh, S., & Dibben, M. (2003) The uses of trust in information science and technology. Annual Review of Information Science and Technology, 37, 465–498.

Miller, B. (2007) European cities link to improve quality of life. Government Technology.Retrieved January 3, 2009, from www.govtech.com/gt/95828

OCIPEP (2002) 'Securing Publicly Available Information', Information Note No. IN02-005, Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, ON. http://www.ocipep-bpiepc.gc.ca/.

OMB (2003) E-Government Strategy. Washington, DC: Office of Management and Budget. http://www.whitehouse.gov/omb/egov/2003 egov_strat.pdf.

Pell, J.D. (1999) Internet Acceptable Use Policy. Kern County, CA: Kern County. http://www. lgov.org/document/doclist.asp.

Schenk, M., Schenk, M. (2002) Defining the value of strategic security. Secure Business Quart. 1 (1), 1–6.

Smith, P. (1999) 'Work and training', Government Computing, September: 30–31

Snellen, I. (2002) Electronic governance: Implications for citizens, politicians, and public servants. International Review of Administrative Sciences, 68, 183–198

Symantec. (2012) "Symantec Internet Security Threat Report."

Tanaka, H., Matsuura, K., Sudoh, O. (2005) Vulnerability and information security investment: An empirical analysis of E-local government in Japan. J. Account. Public Policy 24, 37–59.

Tolbert, C., & Mossberger, K. (2006) The effects of e-government on trust and confidence in government. Public Administration Review, 66(3), 354–369.

World Bank. (2009) Definition of e-government. Washington, DC: World Bank Group. Retrieved January3, 2009, from go.worldbank.org/M1JHE0Z280

Yin, R. K. (2003) Case study research: Design and methods (3rd ed.). Thousand Oaks, CA: Sage.

Zuurmond, A. (1998) From bureaucracy to infocracy: Are democratic institutions lagging behind? In I. Snellen & W. B. H. J. van de Donk, (Eds.), Public administration in an information age: A handbook
(pp. 259–272). Amsterdam: IOS Press