

Is Cybercrime one of the weakest links in Electronic Government?

Shalini Kesar, Ph.D.

Assistant Professor of Information Systems,
Department of Computer Science & Information Systems,
College of CIET, Southern Utah University,
Utah, USA.

Email: Skesar2@gmail.com

Abstract: This paper provides an insight to the increasing problem of cybercrime in the context of electronic government. It takes examples from the UK government to argue that it is no longer possible to just rely on technical controls while securing electronic government transactions. Reports and studies reflect that illicit acts such as cybercrime are predominantly the result of not only disregard for basic information security and but also lack of awareness about the importance of social issues associated with information technology. Consequently, focusing on the technical controls provides only a *partial* solution while managing cybercrime particularly in electronic government context.

1. Introduction

Information Technology (IT) has impacted how Government now provides services to the citizens and business. In the UK, for example, effort to offer electronic services to its citizens has indeed intensified over the years. In 2000, “electronic government agenda” was launched to extend the use of Information and Communication Technologies (ICTs) within the local government. Overall the objective of Electronic Government (eGov) in the UK was to offer services electronically and also to expand to e-governance and e-democracy. Electronic services refer to service delivery through Internet or other ICT methods. It also includes delivery by telephone if the staff receiving the call can access electronic information and/or update records online. In order to achieve multiple objectives such as delivery of efficient customer services, the UK government has set up an e-Government Unit (eGU) to formulate IT strategy and policy, promote best practices across departments and delivered citizen-centered online services. The UK Government also outlined a set of ten guidelines as a framework for the development and management of local government websites¹. These guidelines provide assistance to senior managers and web management teams at a local level. Given that the public sector is the biggest user of IT, it is not surprising that in 2006-2007, people’s concerns about the environment have extended to the sustainability of IT and risks associated with it. Recognizing the need to share data securely within eGov and to tackle mitigating risks associated with cybercrime, data security and integrity is underpinned by key factors that drive the publication of the Information Assurance Strategy. It provides guidelines for local authorities to secure their information systems. With this, it is hoped that UK government’s aim to deliver better, more efficient services for everyone by providing a safe way for citizens and business to use government services online is met.

¹Source: <http://www.egov.vic.gov.au/index.php?env=-categories:m1784-1-1-8-s>

2. Tackling Cybercrime

Given the earlier well established documents and reports about information security breaches, the word “safe” is indeed an ambiguous word. This is because evidence from various sources (for example, Audit Commission Report 2005) suggests that incidents of cybercrime² are increasing in number causing significant concern among organizations across the globe. In the UK, 2006 report highlighted an increase of 18% of households with internet access said their home computers had been affected by a virus. This had increased to 27% in 2003/04³. One-third said the virus had damaged their computers. Furthermore, biennial Department of Trade and Industry (DTI) Security Breaches survey reports that 62% of UK businesses had an information security breach in the 2006 alone⁴. Further, it was indicated that in mid 2008 alone, around 16.5 million (65%) of UK households had access to the Internet (an increase of 8 per cent since 2007). More recently, the [Norton Cybercrime Report: The Human Impact](#), defines cyber crime as including viruses, [identity theft](#), online hacking, online harassment, online scams, phishing and sexual predation, and questioned 7,000 adults in 14 countries, including the UK. In 2010, the Information Commissioner's Office (ICO) report⁵ warned organizations that they need to minimize the risk of mistakes, as the amount of losses reported tops 1,000. It also report revealed that 254 breaches were as a result of information being disclosed in error, 307 were as a result of stolen data or hardware and 233 due to lost data or hardware⁶. These statistics may underestimate the real situation as many organizations including government may be unaware that the information security of their information systems has been actually compromised.

It is clear that the growing problem of cybercrime is further compounded by the fact that such cases are not restricted to one particular country and are rarely reported. Hence, cybercrime could have a greater impact than the conventional crime. Of the intrusion attempts that appeared to have come from outside the organizations, the most common countries of origin appeared to be United States, United Kingdom, China, Nigeria, Korea, Germany, Russia, and Romania. What is even more alarming is that it is the employees who pose one of the greatest threats to organizations today. Keeping in mind the ‘push’ on the emergence of eGov in the UK and increasing problems of cybercrime, it is prudent that the UK government is vigilant about issues associated with minimizing such crimes.

In response to the growing problem of cybercrime, the UK has established an Office of Cyber Security (OCS) that is initially set up in the Cabinet Office⁷. The OCS will have overall ownership of this Cyber Security Strategy will provide strategic leadership across government for cyber security issues. It emphasizes that the “UK needs a coherent approach to cyber security, and one in which the Government, organizations across all sectors, the public, and international partners all have a part to play. The Strategy outlines the Government’s approach and puts in place the structures that the UK needs in order to weave together new and existing work to move towards our vision”⁸.

² The Audit Commission Report (2001), defines computer fraud as an unauthorized input, or alteration of input; suppressing/misappropriation of output from a computer process; alteration of computerized data; alteration or misuse of programs, but excluding virus infection. In other words, computer fraud is a deliberate misappropriation by which an offender tries to gain unauthorized access to the organization’s Information Systems (IS).

³ Source: The Home Office, Fraud and Technology Crimes: Findings from the British Crime Survey 2003/4, the 2004 Offending Crime and Justice Survey and administrative sources, September 2006

⁴ Source: Department of Trade & Industry, Information Security Breaches Survey: Technical Report, April 2006 06/803

⁵ See <http://www.scmagazineuk.com/ico-reports-that-the-nhs-has-disclosed-305-security-losses-as-the-amount-of-breaches-tops-1000/article/171205/>

⁶ see http://www.theregister.co.uk/2009/07/10/nhs_malware/

⁷ See <http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf>

⁸ <http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf>

Cyber Security Operations based at GCHQ⁹ was launched to tackle the growing problem of cybercrime. GCHQ is one of the three UK Intelligence Agencies and a part of the UK's National Intelligence Machinery. GCHQ works in partnership with the Security Service (also known as MI5) and the Secret Intelligence Service (also known as MI6) to protect the UK's national security interests. Whilst the UK cybersecurity centre has approximately 20 members of staff under control of the Cabinet Office, it appears to still be in the process of being formed, the plan is for the unit to monitor the internet for threats to UK infrastructure and counter-attack when necessary.

Against this backdrop, this paper argues in trying to minimizing cybercrime within eGov, equally focus needs to be given to technical, formal and informal (social) issues associated with IT. This is because focusing on the technical issues only provides a *partial* solution while managing cybercrime. Furthermore, increasing sophistication of employees and the kind of information required for 'success' of eGov implies that it is no longer possible to maintain effective security by technical controls (see Audit Commission 2005). Furthermore, information security researchers and practitioners comment that opportunities for cybercrime may well be spread within an organization where different responses arise from work pressures and working conditions conducive to cybercrime (Croall 2001; Kesar and Rogerson 1998; Kesar 2005). Studies on cybercrime are eager to propagate the idea that such illicit acts are predominantly the result of disregard for basic information security strengthens the argument in presented in this paper.

3. Relevant Literature: Information Security and eGov

Within eGov context, studies are broadly categorized into areas that examine: 1) evolution and development (Wimmer, 2002; Layne & Lee, 2001; Srivastava & Teo, 2005; Heeks and Bailur, 2006; Metaxiotis and Psarras, 2004); 2) adoption and implementation (Moynihan, 2004; Heeks, 2002; Poon & Huang, 2002; Al-Sebi and Irani, 2005), and 3) impact on citizens and businesses (Moynihan, 2004; Banerjee & Chau, 2004). Researchers such as Heeks and Bailur (2006) and Im and Seo (2005) specially focused on across implementations. In addition, implementation of eGov has also been studied at the local level in the UK by Weerakkody and Choudrie (2005) who suggest that many authorities are lagging behind the national expectations for eGov (also see studies by Choudrie et al., 2005). Interestingly among the inhibiting factors reported in earlier studies include lack of understanding of issues linked with management of cybercrime (Ebrahim and Irani, 2005; Choudrie et al, 2005).

Within information security area, researchers argue that cybercrime is dependent on organizations creating a climate that perhaps provides potential offenders with 'suitable opportunities' to readily misappropriate information systems (for example, see Forester and Morrison 1994; Kesar and Rogerson 1998; Dhillon 2000; Audit Commission 2001 and 2005; Kesar 2005). Such 'suitable opportunities' are mainly created through inadequate and/or lack of understanding of basic security policies and procedures (Audit Commission, 2005). No doubt, different jobs provide a different "illegitimate opportunity structure" within organizations for employees to exploit. Within information systems studies in particular, these types of control to combat cybercrime, can be seen where researchers have used the general deterrence theory from criminology to predict the use of deterrent security countermeasures (for security polices and guidelines, security awareness programs and preventative security software). Information systems researchers have relied on deterrence theory, which although useful, has been recently criticized for its limitations (see D'Arcy and Hovav 2004).

From the above discussion, it becomes clear that cybercrime is complex in nature and encompasses different types of acts. The complexity associated with such crimes within organizations can be *fully* understood when the context of the work place is also taken into account (see Dhillon 2000; Audit Commission 2005).

⁹ See http://www.gchq.gov.uk/about_us/index.html

4. The Weakest Link: Cybercrime

This section discusses the importance of technical, formal and informal controls while managing cybercrime in the context of eGov. Some recent case studies conducted at the UK local authorities are also highlighted to substantiate the argument presented in this paper (for example, Kesar and Jain, 2007). Although, cybercrime did not occur within these local authorities, findings labelled some of them as a 'high' risk in the context of creating 'suitable opportunities' conducive to cybercrime.

4.1 Technical Controls:

Earlier work in information security was dealt with under a broader term of 'Computer Security', which was primarily developed for the US military. Such measures catered more for structures that were hierarchical where they had centralized information processing. The structures and how information is processed within organizations today is different. Much flatter structures of government and more autonomy and delegated financial powers to employees exist today. This may be commercially efficient but increased flexibility improves the chances of 'suitable opportunities' to commit cybercrime within the government. Furthermore, dramatic increase in the number and technical sophistication of information systems users at local authorities in the UK government also increases the potential of occurrence of cybercrime. According to the Annual Report of 2007, over 29,000 information systems have been delivered, including the following examples, which illustrate the extent of individual systems that have gone from 'work in progress' to 100% completion (for details, see Annual Report, 2007). It also points out that "A more vigilant, secure and safer United Kingdom is critically dependent upon a modern, joined-up approach to information across the whole system". More recently, the government has announced [funding for a police unit dedicated to tackling cybercrime](#) and clamping down on internet fraud in general. No doubt such measures will improve the prevention and detection of cybercrime while implementing eGov. However, effective measures while addressing the problem of cybercrime in eGov context tends to be more inclined towards technical solution.

Studies highlight a gap between the use of IT and the understanding of security implications inherent in its use by the employees in general (Dhillon, 2000). This also perhaps explains why figures representing the number of information systems within organizations that have been successfully penetrated without detection are startling (Audit Commission Report, 2005). Further Internet and other networks, as stated above expose government to an increased risk that information systems will be accessed improperly by employees to commit cybercrime (Kesar, 2005). Tools, techniques, and various handbooks have been developed in order to detect and prevent intentional illicit activities within the UK government. However, this is not enough as it is difficult to secure systems in a heterogeneous, networked computer environment. Many websites report cases of cybercrime within National Health Services (NHS). Nine NHS trusts in the UK have admitted losing patient records in a fresh case of wholesale data loss by government services, it has emerged. Further, at least 168,000 patients have been affected by security breaches, which came to light during a data security review by the Government¹⁰. Another similar report recorded £140 million in fraud and overpayment has been detected by the Audit Commission's National Fraud Initiative (NFI) report 2006/07. Although the report did not indicate the nature of the cybercrime, it pointed out that this was a 26 per cent increase from £111 million in 2004/05¹¹.

Although, it is hard to achieve a 'completely' safe working environment since IT is constantly changing, it is clear that technical controls alone will not be enough to combat cybercrime in a *transforming* eGov environment. With this in mind, formal, technical and informal controls in the context of eGov are discussed below.

¹⁰http://www.timesonline.co.uk/tol/life_and_style/health/article3090664.ece

¹¹<http://www.audit-commission.gov.uk/reports/PRESS-RELEASE.asp?CategoryID=PRESS-CENTRE&ProdID=FE2760D1-6074-435F-8056-DAAF333CCCB0>

2.2 Formal Controls:

Formal controls within organizations relate to physical access controls, systems development, maintenance controls, changing of passwords, library controls, and system performance measurement aids. These controls play a prominent role in the management of cybercrime. This is because such controls are not mandated by law or by any external commission or government bodies but it is the responsibility of the management to define, administer, monitor and enforce controls on employees. Moreover, reviewing and updating process of corporate policy should be governed by the organization's objectives and the level of vulnerabilities. Part of eGov implementation, key parts of a £12.7 billion programme is to upgrade the [NHS's](#) information technology. A report also mentioned that: "Ultimately data security and confidentiality rely on the actions of individual members of NHS staff in handling care records and other patient data. To help provide assurance, the department and the NHS should set out clearly the disciplinary sanctions that will apply in the event that staff breaches security procedures¹²." Such statements clearly echo the importance of policies and formal controls. As Conger et al (1995) point out, lack of policies and formal rules within organizations are interpreted by employees as a license to do what they wish. Within NHS Trust, one of the major hospitals showed the incompatibility between the way doctors work in practice and the high security needed to protect large databases of confidential patient information under the £12.7bn. This was mainly due to password sharing policy being violated among employees¹³.

The Office of the e-Envoy¹⁴ is part of the Prime Minister's Delivery and Reform team based in the Cabinet Office. The Office of the e-Envoy has completed the revision of the security frameworks that are aimed at those establishing, procuring and providing e-Gov services including certain mandatory guidelines and process such as Best Value Performance Indicator (BVPI). As a sign of the growing recognition to deal with increasing problem of cybercrime, the UK government cabinet launched the Cyber Security Strategy as a first step¹⁵.

Cases studies conducted within the local authorities in the UK reflect many incidences where many policies set out by the government were not completely followed by employees (Kesar and Jain, 2007). Among various reasons, one included lack of understanding of the legalization and regulations.

In the context of eGov, it can be argued that formalized rules and regulations will help in facilitating bureaucratic functions in order to resolve any ambiguities and misunderstanding within different government agencies. This is because the higher the level of dependency on IT, the greater the likelihood of local authorities within the government to become vulnerable to cybercrime. It is therefore important that the government need to implement effective and systematic policies with tougher sanctions and penalties.

2.3 Informal Controls:

According to Liebenau and Backhouse (1990), an informal system is dynamic in nature where people have capacity to meet changing circumstances. Indeed, by sustaining informal systems, organizations can respond to the new threats and opportunities that they may face. Thus, people working in an informal system within organizations have the adaptability and flexibility to recognize new conditions. Both formal and informal controls are important systems because the characteristics of a government cannot simply be represented by formalized rules. Training programs that include staff awareness and professional development programs could be conducted considered as both formal and informal controls. Such measures will not necessarily reach a definitive conclusion but will alert employees to the risks of cybercrime. In general, training at different levels within government will help in increasing general awareness and understanding of the potential damage that can be caused by cybercrime. Awareness results in alertness in areas where dishonesty, conflict of interest, and exploitation may occur and ensures employees apply current standards (Liebenau and Backhouse, 1990). It may

¹²<http://www.guardian.co.uk/society/2009/jan/27/nhs-it-computer-programme-health-public-accounts-committee>.

¹³<http://www.computerweekly.com/Articles/2008/05/30/230883/password-sharing-leaves-nhs-audit-trail-in-tatters.htm>

¹⁴ See <http://archive.cabinetoffice.gov.uk/e-envoy/index-content.htm>

¹⁵ http://news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm
interactive.cabinetoffice.gov.uk/.../national_security_strategy.pdf

be appropriate to leave such issues as part of informal controls where bureaucratic procedures can be avoided and management can be relied upon to continue to be sensitive to behavioural changes among staff such as personal or group conflicts. Controls and policies are of no value unless there is awareness and appreciation among employees. Several studies and reports prove that management lack requisite awareness and understanding of information security issues (Audit Commission 2005). Such lack of awareness is one of the most important reasons for security breaches constantly arising from within the government. This was clear in the findings of the case study conducted in one particular local authority (See Kesar and Jain, 2007). More recently annual report for 2008-2009 of NHS revealed that the information, including the names, addresses, NHS numbers, dates of birth and clinical data of about 100 patients, was disclosed without authorization¹⁶.

In light of this, it is important that training and development programs cater for the employees at all levels of local authorities within the government. Consequently, controls and policies require full support of the staff within the government and checks and controls can only be successfully implemented when the staffs supports the concept of those checks.

5. Concluding Remarks

It is clear the UK government's vision is about "making government *transformational* through the use of technology—creating and retaining the capacity and capability to innovate and use technology effectively as technology itself develops" (EGovernment Unit). The UK Government although is making substantial investment to support improvements to infrastructures as well as services to the citizen, it is evident they will continue to face many challenges while minimizing cybercrime. Hence, an equal consideration of technical, formal and informal controls need to be taken into account while managing cybercrime. In other words, mere implementation of state-of-art technical mechanisms as part of managing cybercrime will not alone be adequate in minimizing 'suitable opportunities' for employees to commit such acts. To conclude, it is hoped this paper's argument provides some insight into significant issues linked with minimizing cybercrime within the context of eGov. In doing so, it adds significant contribution to the "few and isolated" studies in this area.

References

1. Audit Commission: Your business@ risk: an update of IT abuse. London, Audit Commission Publications, HMSO (2001).
2. Audit Commission: IT and Abuse Survey. Audit Commission Publications, HMSO (2005)
3. Banerjee, P., and Chau, P. Y. K. "An Evaluative Framework for Analyzing e-Government Convergence Capability in Developing Countries," *Electronic Government* (1:1), 2004, pp. 29-49.
4. Clarke, R., Ed. (1997). *Situational crime prevention: successful case studies*. Albany, NY, Harrow and Heston.
5. Conger, S., Loch, K.D., and Helft, B.L. (1995). "Ethics and information technology use: a factor analysis of attitudes to computer use." *Information Systems Journal* 6 (4): 161-184.
6. CSI/FBI: *Computer Security Issues and Trends*. San Francisco, CSI (2005)
7. D'Arcy and Hovav (2004). The role of individual characteristics on the effectiveness of IS security countermeasures. Tenth Americas Conference on Information Systems (AMCIS) 2004, New York: 1-8.
8. Forester, T. and P. Morrison (1994). *Computer ethics: cautionary tales and ethical dilemmas in computing*. Cambridge, The MIT Press.
9. Heeks., R. and Bailur., S. "Analyzing e-Government Research Perspective, Philosophies, Theories, Methods and Practice", *Government Information Quarterly*, 2006.

¹⁶ http://www.theregister.co.uk/2009/07/28/nhs_direct_email_data/

10. Irani., Z, Lover, P., E., Elliman, T., Jones, S., and Themistocleous, M., "Evaluating E-Government: Learning from Experiences of Two UK Local Authorities", *Information Systems Journal*, (Vol 15), pp. 61, 2005.
11. Kesar, S. (2005). *Interpreting computer fraud committed by employees within organizations*. PhD Thesis (Information Systems). Salford, University of Salford, UK.
12. Kesar S. and Jain, V. "[E-government implementation challenges in the UK: a case study at the Trading Standards Department](#)" *Electronic Government- an International Journal* (Special Issue: From Implementation to Adoption: Challenges to Successful E-Government Diffusion), Vol. 4, Issue 4, pg 395-411.
13. Layne, K., and Lee, J. "Developing Fully Functional E-Government: A Four Stage Model," *Government Information Quarterly* (18), 2001, pp.122-136.
14. Liam, W. "Barriers to e-Government Integration". *The Journal of Enterprise Information Management*, (18), 5, 2001, pp.511-531.
15. Liebenau, J., and Backhouse, J. (1990). *Understanding information: an introduction*. London, Macmillan.
16. Mimicopoulos, M., G., "e-Government Funding Activities & Strategies", Department of Economics and Social Affairs, 2004.
17. Moynihan, D. P. "Building Secure Elections: E-Voting, Security, and Systems Theory. *Public Administration Review* (64:5), 2004, pp. 515-528.
18. Poon, S., and Huang, X. "Success at E-Governing: A Case Study of ESDLife in Hong Kong," *Electronic Markets* (12:4), 2002, pp. 270-280.
19. Streib, G., and Navarro, I. "Citizen Demand for Interactive e-Government: The Case of Georgia Consumer Services in Hong Kong," *The Americans Review of Public Administration*, (36: 3), 2002, pp. 288-300.
20. Srivastava, S. C. and Teo, T. S. H. "Electronic Government as a Guided Evolution in Singapore: Vision for the World in the 21st Century", in *Academy of Management Best Paper Proceedings (AOM 2005)*, Honolulu,Hawaii, 2005, pp. E1-E6.
21. Wimmer, M. A. "Integrated Service Modelling for Online One-stop Government," *Electronic Markets*, (12:3), 2002, pp. 149-156.