Concerning the Implementation of Cyber-Security in the ICT Strategy

Scott Hofman, s0943941

December 1, 2011

The fluidity within IT – a sector defined by its continuous resource and information renewal - requires systems to undergo an overhaul every few years. In keeping with this, the Efficiency and Reform Group (ERG), a branch of the Home Office of the United Kingdom Government, released a proposal in March of 2011 entitled the 'Government ICT Strategy' (Information and Communications Technology). In it, the Government promises to standardize and simplify the existing technologies within their systems (ERG, 03/2011). But with technological change comes concerns about security – how will this Strategy address the growing threat of unauthorized individuals stealing data and how will future attacks be dealt with? In a response issued by the Committee of Public Accounts of the House of Commons, they identify one of the weaknesses of the ICT Strategy as "only mak[ing] one reference to cyber-security."(Commitee of Public Accounts, 2011) To keep current with the march of technology, and to safeguard the private data housed within the Government's databases, the ICT must address these issues of cyber-security before its implementation.

We define cyber-security as the protection of sensitive data - i.e. records of the general populace or international discussions that should remain private. Hackers utilize multiple techniques to extract this information, from technological (software that gains privileged access to computer systems (Parliamentary Office of Science and Technology, 2011)) to 'social engineering' (exploiting people into providing data through social means). Cyber-security is the process of averting these attacks by both software means, such as detecting intrusions or firewalls, and alerting employees to the potential dangers in cyberspace.

Thus, a lack of cyber-security in a government-proposed implementation should be cause for concern. Cyber-security as an issue warrants multiple mentions because of its reactive nature. The threats and attackers change constantly – individuals outside the UK's jurisdiction continue to write new viruses and new software will have exploitable flaws. The problem with cyber-security lies in its nature of not knowing what the issue of the future will be, or, put another way, "only people who understand how attacks are carried out can be expected to be effective defenders." (SANS, 2009) If you are not actively trying to infiltrate a system, you will not understand what flaws your system has, and thus will be unprepared to deal with an attack. This lack of knowledge makes it difficult to prepare for such attacks.

However, the UK Government has long realized the threat of cyber-security breaches. Multiple measures have been proposed to alleviate the threat of hackers; the first of these was in the 1990s with the BS 7799. More recently, the Standard of Good Practice released an updated information guide to security and risk management in 2011. The British Computer Society has a code of conduct for the development of software, and the UK government itself has a document entitled 'Cyber Security Strategy of the United Kingdom,' published at the end of November 2011.

The common theme with these documents is an all-purpose recommendation system – tactics that can be applied to any software, regardless of capability or purpose. This is the standard approach of cyber-security, a technique known as risk management, used globally by both governments and businesses. Risk management tools are necessary every time software is considered. The ability to implement standardized protocols exists; the question becomes if this can be practically implemented on a scale as large as the UK Government.

The decisive factor for successful cyber-security lies with its users. "Effective security depends not only on technology but also on the employees…using information systems and networks." (Cyber Security Research and Development, 2009) With multiple employees

accessing data every day, the fact that "…people are often the weakest link in the security chain" (Cyber Security Research and Development, 2009) remains the pressing issue.

To amend this, training is needed. It is of the utmost importance that individuals dealing with secure data take the necessary precautions to safeguard their usage. Informing employees of the standard protocols, and strictly enforcing them, is the strongest cyber-security known to date. The UK government recognizes this – in the 'Cyber Security Strategy,' they decree they will "...educate and empower people and firms to protect themselves online." (Cabinet Office, 2011) The same paper indicates that "80% or more of currently successful attacks exploit weakness that can be avoided by following simple best practice..." (Cabinet Office, 2011) SANS, a company that provides computer security training for over 165,000 security professionals, mandates that there should also be "[cyber-security] policies [that] explain what is expected from managers, employees, and the Cyber Security organization." (SANS, 2009)

However, a fiscal problem arises from this methodology. There needs to be funding and manpower for such an endeavour. While it is true that governments are aware of the growing cyber-security issue, it is unclear whether there is an adequate amount of funding for the solution. House of Commons, Committee of Public Accounts member Stella Creasy, in an interview session conducted to review the ICT Strategy, was quoted as saying, "America has already identified that it needs double the number of people with these [cyber-security] skills working within Government." (Committee of Public Accounts, 2011) This demand, coupled with "a worldwide shortage of people with these [cyber-security] skills" (Committee of Public Accounts, 2011) reveals a potentially problematic future for cyber-defence.

A £650 million budget was quoted by Ian Watmore to implement cyber-security (Committee of Public Accounts, 2011). There is no way of knowing whether this amount is large enough. The recent rise of the cyber domain hinders financial estimates on the matter – since no one has had to worry about effective cyber-security in the past, no one knows how much money will be enough. The United States Department of Defense is requesting $2.3 billion dollars to spend on cyber defence (Department of Defense, 2011) – the UK should weight its budget to proportionally reflect that spent by the US. Another potential countermeasure would require an adapting budget to meet the current needs, based on the recommendation of a security expert.

This is a role that needs to be created before the Strategy continues. However, the ICT Strategy refers to a 'lack of accountability' amongst security professionals, in regards to information risk. To proceed with this strategy, there needs to be a defined role whose job responsibilities include mitigating the risk of cyber-attacks, training employees in cyber-security, and taking full responsibility for failures that result from his negligence. SANS suggests that successful plans can be implemented when this manager

> "learn[s] the basics, implement[s] policies and plans through effective management, and work[s] diligently to publicize required security practices throughout the organization...." (SANS, 2001)

Only once this role is filled can the plan begin. Yet one should question whether the plan should progress at all. The implementation is possible, and the resources are available, but ethically should they proceed? An analysis of the BCS Code of Good Practice, the British Computer Science document detailing the proper methods for the creation of software, reveals multiple breaches of conduct. Even with the ICT in planning, it should constantly use the Code of Good Practice as a guideline for a proper industry standard.

Firstly, in the attempt to address the issues of implementation, the ICT Strategy refers to a number of steps. These include "the requirements of cyber-security and information

assurance will be embedded in the common ICT infrastructure." (ERG, 03/2011) and "These solutions must balance the need to be open, accessible and usable with the growing cyber-security threat..." (ERG, 03/2011)

While these examples help to explain the eventual goal, they fail to provide objective measures, a violation of 'Code of Good Practice 3.1 - When Managing a Programme of Work' (BCS, 2004). Without these measures, there is no standard to compare the project's progression with, or to determine how close the finishing goal is.

Another failed adherence to the Code of Good Practice is the Strategy's application of risk management. The ICT Strategy does not mention potential risks for the delivery of a secure system, nor does it have a method of alerting the customer of failure (affecting both the central Government and the general populace). These are breaches of Code of Good Practice 3.1 - When Managing Project Risk (BCS, 2004):

- Seek out the real risks to the customer, the organisation and any suppliers.
- Resist the temptation to identify only the manageable risks.
- Openly and frankly discuss with your customer the options for allocating, managing, mitigating and insuring against the risks
- Devise mitigation actions that will reduce the chances of the most serious risks happening

These issues need addressing before the Strategy can proceed. If the individuals in charge of implementing the Strategy move ahead without fixing the above issues, they are not fit for that role. But such decisions can be made at the time of implementation, when all the facts are evident. The House of Commons has made their hesitations clear, and those in charge will no doubt carefully analyse any potential risks in respect to these hesitations.

And indeed, the Strategy is moving ahead. The Government released a document entitled 'Government ICT Strategy - Strategic Implementation Plan' in October of this year. Designed to augment the March 2011 report, the Strategic Implementation Plan provides an overview while attempting to quell any doubts held by the House of Commons.

Concerning cyber-security, most issues have been lessened. The Plan will "…balance the need to be open, accessible and usable with the growing cyber-security threat and the need to handle sensitive information with due care" (ERG, 10/2011) and have "[t]he requirements of cyber-security and information assurance…embedded in the common ICT infrastructure." (ERG, 10/2011)

To address the lack of accountability within cyber-security, the Plan ends each section proposing an action with the name of the individual who can be held liable. In the section entitled 'Risk Management Regime', John Taylor, CIO for the Ministry of Defence, will be its accountable Senior Responsible Owner (ERG, 10/2011).

Also within the Risk Management section are quantifiable standards. Base measures include percentage of software without security support and percentage of software with regular patches. These percentages can be indicative of the project status, and allow for a quantitative goal. In addition, deadlines are included in the Strategy Action for an overall completion date. "Government will develop an appropriate and effective risk management regime for information and cyber-security risks for all major ICT projects and common infrastructure components and services." (ERG, 10/2011) This bullet point is given with an estimated completion time of April 2012.

With this information comes a caveat – the current progress is given as "estimating the scope." (ERG, 10/2011) To give a completion date without scope will create problems, especially given the Government's propensity to delays (this Plan, for instance, should have been released in August rather than October). Combine this with the fluid nature of

technology and the high risk of cyber-attacks, and the project seems likely terminate before it begins. There still is no plan to alert the public of a failure within the system, nor can we be sure that these quantifiers provide an accurate representation of the system.

That the ICT Strategy's implementation of cyber-security, an enterprise in risk management, itself lacks risk management, should be cause for concern. Despite warnings from the House of Commons that cyber-security was absent in the report, and that there are still BCS Code of Good Practice violations, the ICT strategy will proceed. Its implementation will occur sometime within the next year, if everything goes according to plan. While updating and improving Government controlled technology is crucial, the ICT must go about this the correct way. Without addressing these risks, the chance of project failure has risen dramatically.

Word Count: 1969

Bibliography

Bott, Frank. "Chapter 11 - Computer Misuse and the Criminal Law." *Professional Issues in Software Engineering*. London: Taylor & Francis, 2001. Print.

Bott, Frank. "Chapter 14 - Data Protection, Privacy and Freedom of Information, Chapter 15 - Internet Issues." *Professional Issues in Information Technology*. Swindon: British Computer Society, 2005. Print.

"Bruce McConnell Discusses Government's Role in Cybersecurity." *The Wall Street Journal*. 27 June 2011. Web. 30 Nov. 2011. <http://online.wsj.com/article/SB10001424052702304791204576401462981059024.html>.

"Code of Conduct." *BCS - The Chartered Institute for IT*. British Computer Society, 8 June 2011. Web. 30 Nov. 2011. <http://www.bcs.org/category/6030>.

“Code of Good Practice.” *BCS – The Chartered Institute for IT.* British Computer Society, 1 Sept. 2004. Web. 30 Nov. 2011. <www.bcs.org/upload/pdf/cop.pdf>.

"The Comprehensive National Cybersecurity Initiative." *The White House*. National Security Council, 2010. Web. 30 Nov. 2011. <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.

Hoover, J. Nicholas. "DARPA Boosts Cybersecurity Research Spending 50% - Government - Security - Informationweek." *InformationWeek*. 07 Nov. 2011. Web. 30 Nov. 2011. <http://www.informationweek.com/news/government/security/231902495>.

Johnson, James B. "Successfully Managing Cyber Security." *SANS Institute Reading Room* (2001): 1-8. *SANS Institute*. Web. 30 Nov. 2011. <http://www.sans.org/reading_room/whitepapers/services/successfully-managing-cyber-security_224>.

"SANS: Top Cyber Security Risks - Executive Summary." *Computer Security Training, Network Security Research, InfoSec Resources*. SANS, Sept. 2009. Web. 30 Nov. 2011. <http://www.sans.org/top-cyber-security-risks/summary.php>.

Savvas, Antony. "Government Office of Cyber Security Mired in Confusion Warn MPs." *Computerworld UK*. 03 Mar. 2011. Web. 30 Nov. 2011. <http://www.computerworlduk.com/news/security/3263407/government-office-of-cyber-security-mired-in-confusion-warn-mps/>.

"The Standard of Good Practice for Information Security." Information Security Forum, 2007. Web. 30 Nov. 2011. <https://www.securityforum.org/userfiles/public/2007_sogp_pub.pdf>.

United Kingdom. Cabinet Office. *The UK Cyber Security Strategy*. By Francis Maude. 25 Nov. 2011. Web. 30 Nov. 2011. <http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy>.

United Kingdom. Committee of Public Accounts. House of Commons. *Information and Communications Technology in Government*. HC 1050 ed. Session 2010–12. 22 June 2011. Web. 30 Nov. 2011. <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/1050/1050.pdf>.

United Kingdom. Efficiency and Reform Group. Cabinet Office. *Efficiency and Reform Group Homepage*. Web. 30 Nov. 2011. <http://www.cabinetoffice.gov.uk/unit/efficiency-and-reform-group>.

United Kingdom. Efficiency and Reform Group. Cabinet Office. *Government ICT Strategy - Strategic Implementation Plan*. Oct. 2011. Web. 30 Nov. 2011. <http://www.cabinetoffice.gov.uk/content/government-ict-strategy-strategic-implementation-plan>.

United Kingdom. Efficiency and Reform Group. Cabinet Office. *Government ICT Strategy*. Mar. 2011. Web. 30 Nov. 2011. <http://www.cabinetoffice.gov.uk/content/government-ict-strategy>.

United Kingdom. Parliamentary Office of Science and Technology. Houses of Parliament. *Cyber Security in the UK*. Sept. 2011. Web. 30 Nov. 2011. <http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf>.

United States. Cyber Security Research and Development. Department of Homeland Security. *National Cyber Security*. By Martin N. Wybourne, Martha F. Austin, and Charles C. Palmer. 2009. Web. 30 Nov. 2011. <http://www.cyber.st.dhs.gov/docs/i3pnationalcybersecurity.pdf>.

United States. Department of Defense. *SUMMARY OF THE DOD FISCAL 2012 BUDGET PROPOSAL*. 14 Feb. 2011. Web. 30 Nov. 2011. <http://www.defense.gov/home/features/2011/0211_fiscalbudget/SUMMARY_OF_THE_DOD_FISCAL_2012_BUDGET_PROPOSAL_with_Charts_Updated_1710_02.14.2011.pdf>.

United States. Government Accountability Office. *Emerging Cybersecurity Issues Threaten Federal Information Systems*. May 2005. Web. 30 Nov. 2011. <http://www.gao.gov/new.items/d05231.pdf>.

United States of America. National Cyber Security Division. Department of Homeland Security. *US-CERT: United States Computer Emergency Readiness Team*. Web. 30 Nov. 2011. <http://www.us-cert.gov/cas/tips/>.