Cyber security culture and ways to improve security management

Trim, P.R.J., Lee, Yang-im, Ko, E. and Kim, K.H.

This is a copy of a chapter published in: Trim, P.R.J. and H.Y. Youm (ed.) Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership Republic of Korea British Embassy Seoul, pp. 21-26.

SECTION 2: Cyber Security Perspectives

Paper 4: Cyber security culture and ways to improve security management

Peter R.J. Trim, Yang-Im Lee, Eunjo Ko and Kyung Hoon Kim

Introduction

There is no doubt that the cyber security issues and challenges facing managers in both private sector and public sector organizations is consuming greater attention and will continue to do so in the years ahead. However, although it is relevant to suggest that those dealing with organizational security issues do need additional resources in terms of investment in people, processes and technology, it has to be said that a more holistic view has to be taken regarding the skill base of society and how managers in organizations can recruit appropriately skilled cyber security individuals, who are better able to defend the organization against cyber attacks than is the case at present. It can also be argued that academics and university researchers need to broaden their appreciation of what cyber security involves, and think in terms of engaging in interdisciplinary or multidisciplinary research projects.

This paper starts with a section entitled cyber security issues and challenges, and continues with addressing the knowledge and skill gap. Next, attention is given to information sharing and organizational learning, and this is followed by identifying the central issue. The paper ends with a list of recommendations.

Cyber security issues and challenges

It was reported in the Department for Business, Innovation and Skills 2013 *Information Security Breaches Survey*, that (BIS, 2013a, p.3):

"… companies are struggling to keep up with security threats, and so find it hard to take the right actions. The right tone from the top is vital – where senior management are briefed frequently on the potential security risks, security defences tend to be stronger".

The report makes clear that small businesses are experiencing increased levels of denial-of-service attack. In addition, networks are being penetrated by outsiders and outsiders are stealing intellectual property. According to Iain Lobban, the Director of GCHQ (CESG, 2012), areas at risk include: intellectual property; commercially sensitive data relating to negotiating positions; government and industry services, which are subject to disruption; and organizational partners, subsidiaries, supply chains vis-à-vis information security weaknesses. Broadly speaking, management need to focus on: people, processes and technology (CESG, 2012). Bearing in mind managers need to understand what is at risk; need to know where the threat is likely to come from; have an idea about the form the threat will take and the resulting impact and/or consequences for the organization if the risk manifests into an attack; it is clear that management need to manage the risks by: planning, implementing and reviewing (BIS, 2013b). The WARP (warning, advice, and reporting points) programme comes within the Information Sharing Strategy of the Centre for the Protection of National Infrastructure (CPNI) and has a number of advantages for organizations: it is cost effective owing to the fact that it is based on sharing information about incidents/cyber attacks; and it promotes a community approach to identifying and solving problems (http://www.warp.gov.uk/background.html).

CPNI have done much to improve governance, for example, the HoMER (Holistic Management of Employee Risk) approach offers guidance and advice to senior management regarding how the risk associated with employees can be reduced. For example (CPNI, 2012):"HoMER is an interactive guidance document designed to help organisations manage these risks. The guidance provides examples of good practice principles, policies and procedures, backed up by case studies. The guidance will help organisations build effective countermeasures, and respond to and recover from incidents when they occur.

HoMER is aimed at board members and other owners of people risk and shows users the steps that can be taken to change their organisation's approach to personnel security. Through creating a positive culture supported by strong corporate governance and a fair, compliant and transparent legal framework, an organisation can successfully prevent, protect and manage employee risk.

Risk of damage from the actions of employees or contractors working on your behalf. Most incidents stem from errors or omissions but there is also a threat of malicious activity including, in extreme cases, actions by criminals, terrorists or foreign powers………HoMER provides guidance or organizational governance, security culture, and controls to help you mitigate people risk. The key elements of HoMER are:
Take a risk-based approach
Manage people risk holistically
Develop the security culture needed by the business
Appoint a senior single owner of people risk
Act in an ethical, legal and transparent manner".

The GISES (Global Intelligence and Security Environmental Sustainability) model (Trim, 2005) can help managers to develop a security-intelligence interface. More specifically, it focuses attention on: how managers can produce a security culture; how managers can develop trust based relationships; and how information sharing can be facilitated. In addition, the SATELLITE (Strategic Corporate Intelligence and Transformational Marketing) model (Trim, 2004) can be used to link more firmly environmental issues with business intelligence planning. The objectives are to produce a hybrid security culture; and to encourage managers to think of security as a core activity.

Addressing the knowledge and skill gap

Policy makers and their advisors are addressing the knowledge and skill gap that exists and they are to be applauded for doing so. Notwithstanding, more needs to be done and it needs to be done urgently, if that is, the more sophisticated forms of cyber attack are to be dealt with. For example, researchers based at various organizations including universities and government research centres and institutions, as well as those in the corporate and not-for-profit sectors, need to share knowledge and experience. By joining forces in order to pool specialist knowledge and expertise they will be able to produce additional cyber security knowledge that provides a more integrated and joined up approach to counteracting cyber attacks. The advantage of sharing information and/or case examples with staff in partner organizations and indeed government agencies, is that trends relating to cyber attacks can be identified and organizational vulnerability reduced. The reason why this is important is because as the UK and Korea engage more fully in trade related activities, it is crucial to secure the business environment in which these relationships operate. If trading is disrupted, both the corporate needs and the government objectives will not be met, and turmoil may result. This raises current concerns regarding how managers undertake risk assessment and deploy risk management tools. BCS, The Chartered Institute for IT, has extended its BCS CESG Certified Professional Scheme, for Information Assurance (IA) professionals, and has launched the scheme to the UK private sector, building on what had been previously available to "government employees or those working on government contracts"(http://www.bcs.org/content/conWebDoc/51368). (For information about the UK information assurance community please consult: www.cesg.gov.uk/publications/Documents/uk_ia_community.pdf).

One of the key issues that needs to be addressed is how a new approach to risk management can be developed that is considered holistic and embraces and supports internal working relationships as well as relationships between organizations. Managers that operate on an individual basis (UK cultural value system) view decision-making differently from managers that engage in a collectivist decision-making approach (Korean cultural value system), and because of this, it is possible that cyber attacks are dealt with differently. In order to deal with threats both from internal sources (the insider threat) and the external environment (the activities of organized criminal groups and stated sponsored organizations and which manifest in some sort of computer hacking activity), it is necessary to have a firmer appreciation of how risks can be mitigated. The Information Assurance Advisory Council is aware of the fact that "managing risks involves both technology and human activities", and by developing a meaningful risk assessment and analysis methodology, it will be possible to explain better how risk is perceived and how managers learn about dealing with risk. This means, that we need to rethink how we interpret learning within organizations and most importantly, how we can promote more widely the concept of organizational learning.

Information sharing and organizational learning

The organizational learning concept can be utilized to provide a holistic approach to training; and provide a foundation from which a project liaison team management structure can be built (Lee, 2009, p.189). This being the case, a cyber security culture can be developed that reinforces security awareness; influences the organizational value system and the value system of partner organizations; and encourages managers to be pro-active. By engaging more fully in sharing information and deploying the organizational learning concept, managers can, through improving organizational communication, group work and planning, develop highly relevant cyber security systems and practices that lead to the organization becoming more resilient than is the case at present. The advantage of this is that not only will the organization become sustainable, the main organizational stakeholders will be better informed about the risks involved and will also be more aware of the need to absorb and respond to messages in relation to the communication of risk. A well crafted risk communication strategy can inform partner organizations of what the state of affairs is and the action being taken to rectify the situation. This form of transparent communication is considered relevant as cyber attacks need to be dealt with in real time, if that is, the defensive strategy deployed is to be successful. Transparency is particularly important with respect to building trust within and between organizations, and should be considered vital with respect to developing relationships involving UK and Korean organizations.

The escalation in different forms of social engineering has resulted in various cyber security attack vectors being exploited and as a consequence management need to pay more attention to the behavioural factors of those orchestrating such attacks and employees who may be susceptible to falling victim to this kind of manipulation. Although some corporations have implemented policies that govern the use of BYOD (Bring Your Own Device) to work and have required that employees enter into formal contractual agreements relating to usage and the storage of sensitive data and information, more needs to be done and needs to be done sooner rather than later. Preparing staff to deal adequately with both current (known) and unknown (future) cyber attacks is something that requires fuller attention.

Bearing the above points in mind, we can return to the topic of risk. For example, it is necessary to develop knowledge and working practices that take into account the different ways in which organizational risk is assessed and also, how to link more firmly, emerging bodies of knowledge such as strategic marketing, corporate intelligence with corporate security. By doing so, it is possible that managers within organizations will engage more fully with their counterparts in partner organizations, and in the process develop a joint security approach that views security as a core activity across the partnership arrangement. It is envisaged that research into organizational risk jointly undertaken by UK and Korean researchers, will do much to strengthen relationships between staff in UK and Korean companies as the research findings will be embedded in a culturally focused context.

Further reflection allows us to conclude that there is a need to make explicit the current and future cyber security issues that managers in private and public sector organizations will be confronted with and by focusing attention on horizon scanning activities in relation to how managers can devise cyber security management initiatives, university researchers will be able to devise an appropriate organizational cyber security policy framework that can be made known to managers in various industrial sectors. Work in this area has already been undertaken by Trim and Upton (2013) and can be built on.

Identifying the central issue

A number of issues and challenges have been identified. We assert that the main research question is: How can management use the organizational learning concept in order to produce best cyber security practice that results in the most appropriate protection of the organization's assets?

In order to answer this we need to have an appreciation of the issues that managers are currently concerned with as regards: (i) counteracting current and future cyber security threats; and (ii) devising new approaches to risk management.

Underpinning this way of thinking is a commitment to finding answers to two questions:

How can managers ensure that an organization is resilient?

How can stakeholders be kept informed about events through a well crafted risk communication strategy?

It is envisaged that in order to provide answers to these questions, a number of topics need to be addressed:

(1) Current and future security issues.
(2) Organizational issues in relation to cyber security policy.

(3) Types of social engineering and behavioural factors.
(4) The benefits associated with a collectivist approach to security.
(5) Harnessing the organizational learning concept.
(6) Working with partner organizations in order to develop a joint security approach.
(7) Utilizing the concept of corporate intelligence.
(8) Education, training and staff development.
(9) Best practice and integrated organizational security.

List of recommendations

Recommendation 1: Academics, university researchers and researchers from private and public sectors organizations need to broaden their appreciation of what cyber security involves and engage in interdisciplinary/multidisciplinary research projects.

Recommendation 2: To establish how scenario-based training and the organizational learning concept can promote the collectivist decision-making approach to security.

Recommendation 3: Academics need to liaise with industry and design and market appropriate cyber security training courses that can be extended/made available to university students as part of their educational provision.

Recommendation 4: Research should be undertaken that links cyber security with innovation studies in order to establish how cyber security projects are managed through time.

Recommendation 5: Research should be undertaken to establish what types of security breach are occurring, in different industries and different parts of the world, and how these forms of security breach are changing through time.

Recommendation 6: In order to establish how management in an SME can implement a shared responsibility of risk, research should be undertaken to establish how risk management can be applied across all business functions in SME’s.

Recommendation 7: In order to establish how government agencies can work more effectively with cyber security specialists in the private and public sectors, research should be undertaken to establish how international cyber security partnerships can be developed and maintained.

Recommendation 8: Immediate attention should be given to impact and raising awareness of how social science, and in particular, business and management and computer science vis-à-vis cyber security are linked, hence the need to produce a special issue of academic papers in a reputable academic journal.

Recommendation 9: in order to promote the concept of interdisciplinary/multidisciplinary cyber security research and activities, a summer school, attended by academic, government and industry representatives, should be held in London that promotes the linkage between business and management and computer science vis-à-vis cyber security.

Recommendation 10: Research should be undertaken to establish the existing partnership arrangements between UK and Korean security companies in order to identify future areas of cooperation and market development.

References

BIS. (2013a). *Information Security Breaches Survey*. London: Department for Business, Innovation and Skills.

BIS. (2013b). *Small Businesses: What you need to know about Cyber Security*. London:

CESG. (2012). *Executive Companion: 10 Steps to Cyber Security*. Cheltenham. (The guide was produced by GCHQ, BIS and CPNI).

CPNI. (2012). *Holistic Management of Employee Risk (HoMER): New guidance to help organisations to reduce the risk from their employees.* London: Centre for the Protection of National Infrastructure.

Lee, Y-I. (2009). "Strategic transformational management in the context of inter-organizational and intra-organizational partnership development", pp.181-196 in *Strategizing Resilience and Reducing Vulnerability*, edited by P.R.J. Trim and J. Caravelli. New York: Nova Science Publishers, Inc.

Trim, P.R.J. (2004). "The strategic corporate intelligence and transformational marketing model". *Marketing Intelligence and Planning*, 22 (2), pp.240-256.

Trim, P.R.J. (2005). "The GISES model for counteracting organized crime and international terrorism". *International Journal of Intelligence and CounterIntelligence*, 18 (3), pp.451-472.

Trim, P.R.J., and Upton, D. (2013). *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training.* Farnham: Gower Publishing. ISBN: 978-1-4094-5694-0 and e-book 978-1-4094-5695-7 and Kindle 978-1-4094-7457-9.

Websites

CESG.
Website: www.cesg.gov.uk
UK IA Community Map – CESG.
www.cesg.gov.uk/publications/Documents/uk_ia_community.pdf

Centre for the Protection of National Infrastructure (CPNI).
http://www.warp.gov.uk/background.html

BCS, The Chartered Institute for IT
http://www.bcs.org/content/conWebDoc/51368 (accessed 30th September, 2013).

Department for Business, Innovation and Skills.
www.gov.uk/bis

Information Assurance Advisory Council
http://www.iaac.org.uk/