Cyber security issues, challenges and the way forward

Trim, P.R.J. and Lee, Yang-im

This is a copy of a chapter published in: Trim, P.R.J. and H.Y. Youm (eds.) (2015) Korea-UK Initiatives in Cyber Security Research: Government, University and Industry Collaboration, British Embassy Seoul, Republic of Korea, pp. 11-14.

Paper 2: Cyber security issues, challenges and the way forward

Peter Trim and Yang-Im Lee

Introduction

The material in this paper originated from the discussions that took place during the UK cyber security research network group meeting on 25th November, 2014 (see Appendix 4). The aim of the report was to provide a number of points that would stimulate discussion amongst a wide audience and in due course ideas were put forward regarding how researchers could adopt an interdisciplinary or multidisciplinary approach to studying various aspects of cyber security. The reader will gauge the fact that the topics covered span business, academia and policy, and that cyber security is not defined in a single domain. By adopting a holistic approach to security, it is envisaged that researchers will think in terms of how various aspects of the literature, and especially technological, organizational and psychological aspects of cyber, can make links across separate fields of knowledge and within and between fields of knowledge. If this is the case, solutions should be automatic and in some cases, they may be transferable across national boundaries.

Current thinking

There exists some confusion as regards what cyber covers and more attention needs to be given to defining cyber and placing it within the context of cyber security and the changing environment. As regards cyber security generally, a balance needs to be taken of how the public and private sectors take and share responsibility for eradicating cyber threats. The reason for this is because organizations in the private sector are considered to be ahead of organizations in the public sector with respect to cyber security implementation, however, small companies in particular are not as forward thinking as large and medium sized companies, and as a consequence assumptions must not be made about cyber security provision generally.

Policy makers in particular need to understand better the link between technology and the human factor, and need to understand better how technology is deployed. This is especially important when comparing the UK and Korea, and establishing what the appropriate measures are for establishing commonality between the two nations. Indeed, a holistic approach to security should provide a basis for the technological, organizational and psychological dimensions to be taken into balance and should this be the case, an interdisciplinary/multidisciplinary approach can be taken to solving cyber security problems. By understanding how those set on causing harm and damage think, and what their motives are, it should be possible to take into account the technology-human factor dimensions and how weaknesses in technology and human relationships are exploited, and can be safe guarded.

The way forward

Some industries are more at risk than others or become prone to cyber attack due to a set of events/circumstances, hence more needs to be done for small and medium sized enterprises (SME's) in industries at risk of cyber attack or potentially at risk from cyber attack. For example, more advice and assistance needs to be given to managers in SME's regarding the protection of intellectual property. Part of the solution could be to put in place a framework to

ensure that relevant liaisons transform into working partnerships. It can also be argued that a collectivist approach to decision-making has the benefit of ensuring that the human factor is perceived as important and also, the technological factor can be placed in the context of country specific situations. Attention needs to be given to the use of systems modelling and how it can support an interdisciplinary approach to counteracting cyber security threats. With specific reference to the cyber insurance market, more appropriate risk assessment and risk management are required.

Bearing these points in mind, it can also be suggested that more advice and support is needed with regards to effective cyber security legislation and privacy and this needs to be collectivist in orientation. By having a more collectivist approach to cyber security, international cooperation will be facilitated and made easier, and information sharing across borders will become automatic. A deeper insight into how people are affected by and embrace legislation relating to working practices in the area of cyber security needs to be established. Should this be the case it would be possible to categorize people according to their motives: (i) those that want to engage or feel compelled to engage in cyber crime activity; (ii) those that actually carry out or work with others that are engaging in cyber crime activity; and (iii) those that organize, manage and lead others into carrying out cyber crime activity.

Policy makers and their advisors need to be constantly reminded that there are lots of pockets of cyber crime activity and that sophisticated criminals or hackers are increasing their knowledge and sophistication and will possibly start to join up their attack activities by drawing more on their own resources or by sharing information and resources with other illicit groups. Hence new skills and knowledge will be needed on an ongoing basis to counteract the activities of those involved in cyber crime and also, a more direct approach will need to be made to governments that are involved in state sponsored cyber activity that is focused on economic gain by illegal means. Hence, on the job cyber security training needs to complement class based cyber security training and educational provision. In particular, at the higher end, attention needs to be given to how a specific style of leadership nurtures initiatives to counteract cyber attacks.

Government in cooperation with industry and academia, will need to identify what cyber security skills are needed in the short, medium and long term. Academics, working closely with people in industry, need to develop risk based decision-making models that are used in an objective and real time setting. This is because smart inventions and applications, and the notion of the smart city, will provide cyber criminals with additional attack opportunities. A collectivist or joined up approach needs to ensure that the potential vulnerabilities identified are not exploited in a way that is beyond the capability to make safe and restore.

More attention needs to be given to making managers in a company aware of who to contact in a crisis and evidence needs to be obtained regarding the nodes in the chain of the attack so that there is a joined up or collectivist approach to sharing information and acting on information in real time. In order that law enforcement agencies are not swamped vis-à-vis responding to new forms of cyber crime, it is essential that companies in the private and public sectors engage with law enforcement personnel and cooperate when required and share information so that a problem can be contained and does not escalate. Staff in SME's need to understand that websites will be monitored/should be monitored to a degree and that this is in the interest of all parties concerned, if that is, known forms of cyber crime are to be eliminated/curtailed. Bearing in mind that new risk models will emerge, it is important that

those at the apex of an organization understand, accept and take responsibility for placing adequate cyber security systems and policies in place, which translate into an adequate leadership model that is transformative in nature and which is underpinned by a collectivist decision-making process. Mechanisms need to be established so that data, information, knowledge and expertise are shared and individual managers take ownership of cyber security and in addition, information relating to best practice is not lost but is made available and can be accessed and acted upon in the future.

Government need to ensure that there will be continuity of advice, support and collaboration with respect to dealing with cyber attacks and cyber crime generally, and this means that responsibility and accountability for cyber security at all levels needs to be associated with government departments and agencies. It is important to point out however that people and their right to know need to be weighed against the need for sharing information as there are ethical issues to be addressed. Academics need to think of how they can include aspects of cyber security into the syllabus and adopt where possible an interdisciplinary approach that gives rise to joint research projects. We encourage researchers based in different departments within the same university and those based at different institutions. In addition, researchers need to work together on joint cyber security projects and they also need to think of how the scope of the research can be extended to include industry partners.

A number of recommendations can be put forward.

Recommendation 1: Research should be undertaken to produce case studies that highlight how security involving technological factors and human factors gives rise to best cyber security practice in a country experiencing various forms of cyber attack.

Recommendation 2: Research is undertaken into explaining and identifying how and when an individual is likely to engage in cyber attack activity.

Recommendation 3: Policy advisors need to ensure that empirical data and evidence is available that can be used as a basis to invest resources wisely in the area of cyber skill development and enhancement.

Recommendation 4: A security culture mentality needs to be adopted if that is managers in SME's are to fully understand how cyber attacks are planned and orchestrated, and appropriate people need to be appointed to deal with risk that are capable of undertaking risk management.

Recommendation 5: Research needs to be undertaken into providing evidence of how new types of crime (eg., related to developments such as smart cities and smart city living) are emerging/will emerge and how such crime can be counteracted through public awareness programmes.

Recommendation 6: Cyber security needs to be integrated at all levels (local, national and international), if that is, threat led intelligence is to result in information being shared and cooperation is to be forthcoming.

Recommendation 7: An analysis needs to be made of how Korea and the UK can, possibly with other governments, share cyber security data and information relating to best practice, with the view that it may be possible to adapt working practice, systems and policies, and

thus benefit from informal as well as formal associations and working relations between organizations in both countries.

Recommendation 8: Research should be undertaken to identify patterns to be identified in cyber crime activity and new risk models can be produced that allow policy advisors in the UK and Korea to work together in a forward looking manner (engage in foresight planning) to counteract developments such as the theft of intellectual property.

Recommendation 9: Research needs to be undertaken to highlight how different types and forms of cyber crime are emerging (externally orchestrated crime and internally orchestrated crime) and how preventive measures can be developed and put in place to curtail the actions of cyber criminals.

Recommendation 10: Research needs to be undertaken in order to establish how events in cyber active parts of the world affect the way in which cyber policy is fashioned.

Recommendation 11: Research should be undertaken to establish how terrorist networks are developing a cyber attack capability.

Recommendation 12: Research needs to be undertaken to establish what types of problem occurs at the local level when security is outsourced and how the problems can be eradicated.

Recommendation 13: Research needs to be undertaken to establish how members of society can better understand the actions of cyber criminals and how stakeholders can work together to reduce the vulnerabilities identified.

Recommendation 14: Research needs to be undertaken to establish how the theft of data affects people and what the psychological issues and problems are.

Recommendation 15: Research needs to be undertaken to establish the benefits associated with stolen data and its value.

Recommendation 16: Research needs to be undertaken to establish what role the middle manager plays with respect to prioritizing known risks and implementing security policy.

Recommendation 17: Research needs to be undertaken to establish how industry and government can establish a trust based model for information sharing and cooperation across borders.