Korea-UK Initiatives in Cyber Security Research: Government, University and Industry Collaboration

Report Submitted to the Korean Government and the UK Government March, 2015

Peter Trim and Heung Youl Youm
(Editors)

Korea-UK Initiatives in Cyber Security Research: Government, University and Industry Collaboration

Report Submitted to the Korean Government and the UK Government March, 2015

Peter Trim and Heung Youl Youm
(Editors)

British Embassy Seoul: Republic of Korea.
March 2015.

Dedication

This report is dedicated to global researchers from the public and private sectors and professionals from various industries that are actively engaged in applying cyber security solutions through active partnership arrangements.

Acknowledgements

As in 2013 to 2014, we are indebted to a number of people that have worked closely with us and who have provided advice and guidance during the duration of this project. In particular, we would like to thank the UK Cabinet Office for providing us with the opportunity to undertake the project in the way that we did.

We would like to record a very special thank you to Hyeyoung Kim at the British Embassy in Seoul for the time and effort she put into the project and for the guidance and commitment she showed throughout its duration. We would also like to record a special thank you to various representatives of the UK's Foreign and Commonwealth Office, and in particular thank Gareth Davies for his continued support and also Minji Choo for her patience and support. In addition, we would like to thank the Embassy of the Republic of Korea in London for sending a representative to attend the main cyber security workshop in London. This was the second year running that we had the pleasure of welcoming a member of staff from the embassy and their presence was much appreciated. Many thanks also to Ben Leigh at the Department of Business Innovation and Skills (BIS) for his assistance.

We would also like to record our appreciation to the funders, the UK's Department of Business Innovation and Skills and Korea's Ministry of Science, ICT and Future Planning, and other organizations, for allowing us to work together and to gain knowledge and insights into cyber security in both the UK and Korea. We would like to thank the Korea Information Security Forum and in particular the Korea Internet and Security Agency (KISA) for their all round help and assistance, and for the time their staff made available to the UK cyber security delegation while in Korea.

Peter Trim (London) and Heung Youl Youm (Seoul).
March, 2015

Foreword

As indicated in the first report entitled: *Korea–UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership* (Trim and Youm, 2014, p.8), the rationale, aims and objectives of the research network were made clear. The research project was a co-funded, Anglo-Korean government approved university-business project that focused on *Increasing Cyber Security Provision in the UK and Korea: Identifying Market Opportunities for SME's.* Funding was secured in 2013-2014 and again in 2014-2015. The funding allowed a project to be undertaken that harnessed "the knowledge and expertise of academics, representatives from government, policy advisors and industry experts, to work on a number of initiatives that will strengthen the cyber security provision of both countries" (Trim and Youm, 2014, p.8). The two project leaders, Dr. Peter Trim, Birkbeck, University of London and Professor Heung Youl Youm, Soon Chun Hyang University, were each responsible for organizing a research network in their respective countries that would provide insights into how sophisticated cyber attacks are emerging and how managers in SME's could identify organizational vulnerabilities and implement solutions. In addition, it allowed academics, government representatives and people from industry to come together and discuss cyber security issues, challenges and policy solutions. To assist them in their task, two Korea-UK Cyber Security Research Workshops per year took place in each of the funding periods. The third workshop took place in Seoul on 19th January, 2015 and the fourth workshop was held in London on 23rd February, 2015. During the second funding period, again the workshops represented the mechanism through which the outputs were delivered but in addition a number of visits, group and individual meetings were arranged with key cyber security staff. Visits were arranged to various influential organizations, and two additional research workshops were held. The Korea Internet and Security Agency (KISA) hosted a workshop on 20th January, 2015 and the Korea-UK Cyber Security Applied Research Workshop was held at Birkbeck, University of London on 24th February, 2015. Members of the Korean Cyber Security Research Network also attended a workshop organized by the Information Assurance Advisory Council's Academic Liaison Panel, which took place in the afternoon of 24th February, 2015. The visits and meetings proved most useful as they resulted in new and strengthened relationships between people from the two countries, and resulted in new areas of co-operation between the research network members.

Source: Trim, P.R.J., and H.Y. Youm (Editors). *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership.* British Embassy Seoul: Republic of Korea.

Table of Contents

List of Appendices

Paper 1: Increasing Korea-UK university and industry research collaboration in cyber security

Peter R.J. Trim and Heung Youl Youm.

Introduction

The 2013 to 2014 Korea-UK Cyber Security Research Network was highly successful and the 2014 to 2015 Korea-UK Cyber Security Research Network can be judged to have been equally successful. The overall aim of the project was the same (Trim and Youm, 2014, p.9): to "focus on a number of objectives including establishing ways to make stronger business relations between Korea and the UK, and to establish synergy among companies involved in cyber security provision. In addition, it was to consolidate ties between government representatives and academic researchers". The purpose of the project was defined as: "Increase Korea-UK university and industry research collaboration in cyber security".

The 2014-2015 Korea-UK Cyber Security Research Network built on the organizational visits, workshop presentations, networking discussions, e-mail exchanges and meetings at the 3rd Cyber Space Conference, and the 2014 iMM Cyber Security Conference in London, the IAAC dinner in London as well at the meeting at the NCA in London, during the 2013-2014 period. The cyber security issues and challenges identified, had been discussed at length and the overall objectives had been revisited and recommendations put forward (see Appendix 1). Indeed, the recommendations from the previous report were discussed at several venues and via email exchanges. This allowed current and future partnership arrangements to be established, the aim of which was to establish how specific cyber security problems could be counteracted and national cyber security policies and strategies could be extended across borders. The activities carried out in 2014-2015 strengthened the relationships established in the previous funding period and resulted in various additional Korea-UK academic relationships and knowledge exchange bridges being formed. In addition, increased attention was given to the security provision of small and medium sized enterprises (SME's), government support mechanisms and the transfer of cyber security knowledge from one setting to another.

Placing the project in context

The 2014-2015 project took forward a number of the outcomes of the previous project, namely:

(i) to identify current and future cyber security issues and problems;
(ii) to strengthen existing UK-Korea academic relationships through networking and identifying additional partnership links;
(iii) to develop additional cyber security contacts in both countries; and
(iv) to develop a platform from which new cyber security knowledge and practices can be developed (e.g., especially education and training).

As a result, stronger academic and business links were made between Korea and the UK, and previously established cyber security links were strengthened through immediate collaboration and a future commitment for additional collaboration. The various one to one, group and email discussions throughout the funding periods focused on establishing how training and the organizational learning concept could promote a collectivist decision-making

approach to security. Attention was given to cyber security risk communication, incident management and business continuity planning. In addition, advice was forthcoming regarding counteracting sophisticated cyber attacks and how managers can categorize these attacks and link them with organizational vulnerabilities, and implement solutions. Discussion also centred upon establishing measurements that let policy makers or CSOs learn about the status and competence (readiness or posture) of imminent cyber attacks.

It became clear during the discussions during the two periods covered (2013-2014 and 2014-2015) that cyber security experts in Korea and the UK are in the process of mapping the various links, relationships and procedures in Korea and the UK, and wish to share this knowledge and information with their counterparts in other countries. This can be considered valuable because it will strengthen the knowledge base of the cyber security community and also, support and lead to initiatives in higher education with respect to establishing the differences and similarities relating to organizing and dealing with cyber crime prevention in Korea and the UK, and reinforcing the need for both training and educational provision to be made available to a wide public.

The main deliverable for 2014-2015, as was the case with the previous grant period, was a report for both the UK government and the Korean government, that provides insights into how senior managers in a range of organizations operating in the public and private sectors; and research staff at various universities can work together and form sustainable partnerships to enhance cyber security policy. The main benefit of the project is that it provides cyber security experts in one country with a knowledge of and access to cyber security experts in the other country and this facilities communication between and among the parties involved and strengthens working relationships. The focus of the work has remained the same, basically to create knowledge and expertise relating to how cyber security policies can be formulated and implemented, and more generally, how lessons learned can be made known, in both Korea and the UK. For example, Korea has over the years experienced a range of cyber attacks, some of which are politically motivated and which have specific economic oriented objectives; and the UK is, because it has a leading financial centre (the City of London), a champion of anti-money laundering activities in the form of initiatives such as information sharing that are aimed at counteracting financially oriented cyber crime. All types of cyber crime were given attention at the 3rd Cyber Space Conference in Seoul in October 2013, and it was noticeable that what is being done in the UK is very relevant to other nations. It is pleasing to report that this research project highlighted the similarities between the two countries and established a forum for discussing and outlining how cyber security problems or future problems could be tackled. The Republic of Korea and the UK are committed to working more closely together in the area of cyber crime prevention and the knowledge and intelligence obtained from this project has assisted various policy makers in Korea and the UK to make cyber security more robust. Indeed, at the Korea-UK Cyber Security Applied Research Workshop at Birkbeck, University of London in the morning of 24th February, 2015, Mr. Patrick Curry and Professor Youm facilitated a research meeting with an invited audience which revolved around aspects of PKI (Public Key Infrastructure).

The following people participated in the applied cyber security research workshop at Birkbeck:

Mr. Robert Hann, Trustis.
Mr. Vince Freeman, Metropolitan Police.
Mr. Richard Pharro, The APM Group Limited (to talk about CDCAT).

Mr. Tony Butler, Delphinitum
Mr. Mark King, Broadsail
Mr. Patrick Curry, British Business Federation Authority (BBFA) Ltd
Dr. Peter Trim, Birkbeck, University of London
Dr. Yang-Im Lee, University of Westminster
Professor Heung Youl Youm, Soonchunhyang University
Dr. Jae Hoon Nah, Electronics and Telecommunications Research Institute (ETRI)
Dr. Jaejung Kim, Korea Information Certificate Authority (KICA)
Professor Dae Ha Park, The Cyber University of Korea
Mr. Ki-Woon Lee, Korea Internet & Security Agency (KISA)
Mr. Jae Nam Ko, Soonchunhyang University
Dr. Pilyong Kang, Director, Korea Internet & Security Agency (KISA)

The following action items were discussed or referred to at the Korea-UK Cyber Security Applied Research Workshop:

PKI Federation readiness.
Organisational ID - ROLO Korea.
Cyber information sharing pilots with industry; status info, threat intelligence.
Re-use of KISA capabilities in UK.
DNS Sinkhole.
DDoS Shelter.
Cyber Curing System.
Internet governance and trust overlays.
Trusted cloud.
Age verification.
Industry and government coordination/collaboration, including with developing nations and major supply chains. (Maritime, electronics, aerospace, telecommunications, banking, pharmaceutical). Links to ITU and ETSI.

Prior to the discussions, Mr. Richard Pharro from APMG-International provided a talk relating to CDCAT (Cyber Defence Capability Assessment Tool). The topics covered linked back to some of the issues discussed at the workshop the previous day and helped to integrate the topics discussed at the two workshops.

Due to the fact that the research project consolidated what had been achieved the previous year, the cyber security network in both Korea and the UK was extended so that the necessary platform was created to develop additional cyber security research links in both countries. Please consult Appendices 2 and 3 for a list of the active members of the network. As well as reviewing the recommendations contained in the previous report, the following topics were given attention:

(1) Initiatives in Korea and the UK relating to the protection of critical national infrastructure and critical information infrastructure.
(2) Information exchange in Korea and the UK and the role of Computer Emergency Response Teams.
(3) Cooperation and collaboration in Korea and the UK in cyber security involving the general public, law enforcement agencies and organizations in the private and public sectors.
(4) Evolving cyber security governance requirements in Korea and the UK.

(5) The development of an appropriate international standard relating to cyber security.
(6) The development of joint research teams and international cyber security research projects.
(7) Ways in which to receive support from industry.

By year two of the project, it was clear that a means had been found, through each active network, to provide guidance as to how both governments could engage more strongly with organizations in the private and public sectors and provide direction and guidance as regards future cyber security policy. Specific areas of knowledge were exchanged including: cyber security attacks; critical national infrastructure protection in Korea and the UK; new management and training practices; input into a cyber security standard; and the basis for cooperation in the area of PKI. The main activities of the network are listed below.

Activities:
(1) Meetings of each cyber security research network group in London and Seoul. Prior to the UK group meeting, a meeting took place between Dr. Trim and Mrs. Hyeyoung Kim, to discuss the way forward.
(2) The 3rd Korea-UK Cyber Security Research Workshop in Seoul, which was attended by four UK cyber security group members and three members of staff from the British Embassy in Seoul. Additionally, the following day, there was an organizational visit to KISA that incorporated a research workshop. Four people from the UK attended the presentation at KISA and the research workshop.
(3) The 4th Korea-UK Cyber Security Research Workshop in London, was attended by seven Korean cyber security group members and a representative from the Korean Embassy in London. In addition, the Korean cyber security experts attended a research workshop at Birkbeck, University of London and the IAAC ALP meeting the following day.
(4) Dr. Trim and Professor Youm edited the report for the two governments.
(5) Two brief reports were also produced for the sponsors.

Source: Trim, P.R.J., and H.Y. Youm (Editors). *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership.* British Embassy Seoul: Republic of Korea.

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.

Paper 3: Report relating to the Third Korea-UK Cyber Security Research Workshop

Peter Trim and Heung Youl Youm

A UK delegation of cyber security experts attended the 3rd Korea-UK Cyber Security Research Workshop at the COEX in Seoul on 19th January, 2015, and in addition, on 20th January, 2015, the UK delegation visited the Korea National Biometric Test Center at KISA (Korea Internet & Security Agency), which was also in Seoul. The workshop was the third workshop in a series of Anglo-Korean workshops relating to *Increasing Cyber Security Provision in the UK and Korea*, the purpose of which is to harness the knowledge and expertise of academics, representatives from government, policy advisors and industry experts, to work on a number of initiatives that will strengthen the cyber security provision of both the UK and Korea. (Please consult Appendix 5, which contains a list of the four main cyber security research workshops over the two year funding period). The UK delegation was composed of members from Birkbeck, University of London; the British Business Federation Authority (BBFA) Limited; Dysart Solutions Limited; and Broadsail. Several representatives from the British Embassy in Seoul attended and there were a number of representatives from the Korean government in attendance including representatives from the Ministry of Science, ICT and Future Planning. In addition, a number of organizations and institutions from Korea were represented at the workshop including: Soonchunhyang University; the Korea Internet & Security Agency; the Telecommunications Technology Association; Symantec; FireEye; Korea Telecom; and the Electronics and Telecommunications Research Institute (ETRI). The workshop was opened by Professor Daeha Park from the Cyber University of Korea. Mr. Jin Bae Hong, Director of the IT Strategy Bureau, Cyber Security Policy Division, Ministry of Science, ICT and Future Planning, provided a keynote address. Those attending the workshop were from both the public and private sectors, and in addition, a number of researchers were present. The talks addressed a number of key topics and current challenges including the Korean Government's IoT security roadmap; ways and means to share cyber security information; the role performed by computer emergency response teams; international cooperation; cyber risks and critical infrastructure; the London 2012 Olympic Games; the way in which advanced persistent threats are changing the approach to cyber security; how to protect telecom infrastructure; how to establish sustainable working relationships in cyber security involving government, industry and academia; best practice in information security training; cyber security and critical infrastructure capability; and the information security readiness certification system.

The visit to the Korea National Biometric Test Center at KISA was highly informative and covered various psychological and behavioural aspects, as well as certification. Following the presentation from KISA, a research meeting was held between the UK delegation, KISA, and Professor Youm, concerning public key infrastructure (PKI). The meeting proved valuable with respect to identifying topics of interest with respect to the Fourth Korea-UK Cyber Security Research Workshop, which was held in London on 23rd February, 2015.

The objectives of the workshop

The objectives of the workshop were defined:

> Sharing information about landscapes, activities and policies in cybersecurity and privacy.

Strengthening academic and business relationships and establishing synergy among companies involved in cyber security.

Providing solutions to protect against cyber-attacks and/or where solutions are likely to come from for SMEs.

Identifying problems and ensuring that the timetable for delivery of the project is adhered to (eg., the research plan is actionable).

The primary workshop topics

The primary workshop topics were identified as:

Strategy and policy in cybersecurity and privacy.

Cybersecurity and privacy landscapes.

Best practices in education and training for improving the cybersecurity capability of SMEs.

Business and academic relationships.

Future collaboration items.

Potential applications of collaboration results

There is a shared consensus that much needs to be done to enhance cyber security provision in order to ensure that the necessary security polices and systems are in place, which allow a nation to trade effectively and at the same time create opportunities for sustaining a range of businesses that employ people and help maintain the quality of life. In terms of government to government cooperation, it is clear that greater transparency and cooperation in the area of information sharing to combat illicit cyber activity will allow an appropriate form of leadership to develop, which results in increased forms of governance and compliance. New forms of operating will give rise to new technological applications that result in a range of products and services, in the area of on-line security and supporting systems, that can be developed at speed and which can meet unmet needs. In particular, small and medium sized enterprises will identify market opportunities and develop, either on their own or in partnership, new products and services that enhance cyber security capacity. By utilizing new security products and services, user companies will develop a more appropriate risk management strategy and will be more able to identify possible vulnerabilities and eradicate them, and in the process communicate risk more appropriately. As regards specific areas of cooperation such as public key infrastructure (PKI) for example, there is no doubt that by pooling knowledge and information, better security awareness will be created that gives rise to new security solutions. There will be increased opportunities for industry and academia to work together and this increased cooperation will give rise to stronger working relationships. It will also allow new knowledge to be brought into the teaching environment and thus ensure that those undertaking a degree in cyber security are able to contribute more effectively to organizational security. As the need increases for cyber security experts, so too will the demand for a masters degree in cyber security/degree in security with a cyber dimension. It can also be said that there will be increased opportunities for postgraduate degrees in business/management that have a cyber security module included in the programme of study, and this also represents a market opportunity.

Project outcomes

Joint publication:

Trim, P.R.J., and H.Y. Youm (2014)(Editors). *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership.* British Embassy Seoul: Republic of Korea. Available at: http://eprints.bbk.ac.uk/9561/1/9561.pdf.

Joint research proposals:

The work referred to above is the second project under the Global Partnerships Fund scheme and builds on earlier work. It is envisaged that a grant application will be made for a much more in-depth research project that will be supported by both the UK Government and the Korean Government, and a number of industry partners. Several universities are also expected to cooperate in the research project.

Future expected and/or potential outcomes:

The 4th Korea-UK Cyber Security Research Workshop will be held at the BIS Conference Centre in London on 23rd February, 2015 and it is also envisaged that the Korean cyber security delegation attending the workshop will also visit organizations/institutions of interest on 24th February, 2015.

Website links:

- http://eprints.bbk.ac.uk/9561/1/9561.pdf.
- http://elec.sch.ac.kr/~csw/

Paper 4: A summary of the papers presented at the Third Korea-UK Cyber Security Research Workshop

Peter Trim and Heung Youl Youm

Oliver Hoare was the former head of Cyber Security and Information Assurance for the UK Government Olympic Executive, and talked about the London 2012 Olympic Games, and specifically about cyber security and Critical National Infrastructure. The London 2012 Olympics and Paralympic Games were heralded as the "first digital games" and in addition, London, was considered the first games to be held in a high-threat environment with regard to the terror threat to the UK. The entire Olympic security programme represented the largest peace time security operation in the UK since the Second World War. Mr. Hoare provided insights into how a cyber strategy was threat, risk and intelligence led, using UK government methodologies, and the importance of governance, command and control arrangements across a wide stakeholder community. He made particular reference to protection of Critical National Infrastructure within an Olympic context, and liaison with various bodies, such as the UK Centre for the Protection for Critical National Infrastructure (CPNI), the IOC and sporting bodies, as well as the many private sector contractors, vendors and suppliers.

Peter Trim gave a paper entitled: "Establishing sustainable working relationships in cyber security involving government, industry and academia". He addressed a number of initiatives that can assist the development of sustainable working relationships among stakeholders in the area of cyber security. Particular reference was made to how government, industry and academia can work together, both directly and indirectly, in order to establish a network of national partnerships that promotes cyber security more generally. Reference was also made to a government funded project, which brought into partnership a number of universities and companies from the security sector, and which resulted in the development of a software package that provided enhanced organizational and network security. In addition, the talk highlighted how managers based in small and medium sized enterprises can work with university researchers on highly sensitive projects and develop collaborative research networks with researchers overseas. A number of key areas were addressed including a holistic approach to security; risk management and risk communication; and how an inter-disciplinary or multi-disciplinary approach can help researchers to develop new cyber security knowledge and theory. Dr. Trim drew some of his observations from two government funded research projects he had been involved in and which were cited in two books:

> Trim, P.R.J., and Upton, D. (2013). *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training.* Farnham: Gower Publishing.
>
> Trim, P.R.J., and Lee, Y-I. (2014). *Cyber Security Management: A Governance, Risk and Compliance Framework.* Farnham: Gower Publishing.

Patrick Curry explained how MACCSA (the Multinational Alliance of Collaborative Cyber Situation Awareness) is working with the UN, EU, USA and PACRIM to establish a baseline for collaborative risk management based on cyber controls frameworks. His talked entitled: "Cybersecurity information exchange and the role of the computer emergency response team", outlined how collaborative cyber situation awareness depends on cyber controls frameworks to provide a definition of Normality, against which Abnormality can be detected consistently across communities by CERTs. In addition, he outlined how MACCSA's

approach reflects best practices, such as the US Cybersecurity Framework, and is based on five steps - Identify, Protect, Detect, Respond and Recover. He provided examples of key international activities in each step and identified opportunities for greater UK-Korea collaboration and pilots, particularly for:

- EU and US developments on CERTs and information sharing.
- High assurance PKI federation, particularly across supply chains and for sharing cyber information under control. This included various authentication, signature and encryption functions.
- Identity proofing of people, organisations, devices and software. There is particular interest on Organisation Identification and federated Trusted Platform Module 2.0.
- Security metrics tied to cyber controls frameworks.
- Threat intelligence sharing, including STIX, IODEF and more, and security automation with Governance Risk and Compliance (GRC) applications.
- The possible development of international vulnerability sharing capabilities that could satisfy Patriot Act and other US legal constraints.
- Age verification for compliant organisations and also non-compliant organisations and actors.
- Initial outcomes from EU Project MAPPING - Internet governance, privacy and intellectual property protection for the EU. Potential Korean participation in the next Technical WG in Washington, DC in March 2015.

Mark King provided a talk entitled: "Increasing cooperation through information sharing", and covered a number of key points and provided insights into how opportunities can be created for facilitating the sharing and exchange of information in existing and new fields of inquiry. In addition, reference was made to lessons learned from mistakes, and explanations were provided, which indicate possible constraints that may not be apparent to those concerned. Attention was also given to how individuals can make better decisions through working in groups. By placing matters in a UK context, it was made clear how the UK functions and most importantly, by outlining the peculiarities associated with the government structure in the UK, it became clear as to why decisions are made and implemented in the way that they are. For example, different rules apply to different government departments and this historical context was explained so that a better understanding of the constraints that are in place were known, and which may militate against information sharing and the exchange of information.

Patrick Curry, Oliver Hoare, Mark King and Peter Trim provided a joint talk entitled: "Cyber Security and critical infrastructure capability: Priorities and the way forward". The speakers offered insights into what can be done to improve cyber security provision and increase a nation's critical infrastructure capability. Emphasis was placed on the linkage between security and intelligence, and enhanced cooperation among stakeholders. This line of argument was extended and reference was made to international collaboration and joint working, and in addition, reference was made to how the sharing and exchange of information can be formalized to ensure that sustainable working relations are formed, both at the national and the international level. Reference was also made to how a university can work with external partners in order to become an international centre of research and teaching excellence, and the role that government needs to play in order to ensure this happens.

Mr. Kwangtaek Youn made reference to “Cyber risks to the critical infrastructure” and covered targeted attacks on critical infrastructure. He explained that targeted attacks are motivated by espionage (the theft of IP) and more recently there has been an increase in the number of destructive attacks against certain organizations. The topics of sabotage and espionage driven targeted attacks were covered. Reference was made to Dragonfly, which represents an example of an energy sector targeted attack.

Mr. Hongsoon Jung had as the theme of his talk, “National computer emergency response team and international cooperation”. The speaker introduced the background to national CERT's and the functions carried out, and highlighted the benefits but also the potential barriers relating to CERT cooperations.

The focus of Mr. Hyunjun Kim’s talk was “Security reimagined – Time to detect, time to remediate for advanced persistent threat”. The lessons learned from the APT attack on Sony Pictures and KHNP suggests that the traditional security model cannot provide adequate protection against sophisticated attacks and it is time to reimagine security. Reference was made to how FireEye can provide direction and detect and remediate for new threats in real time.

Mr. Tae Sun Hwang outlined “How to protect telecom infrastructure effectively”. Three key activities for information security in Korea Telecom were covered: protection of personal data; protecting network infrastructure; and providing secure B2B services. Reference was made to large scale data leakage incidents that have happened, and how Korea Telecom is redesigning the information security architecture of systems that have been/are assumed to have been compromised and which require continuous monitoring and remediation.

Mrs. Yoonjeong Kim focused on “Best practice for information security training and the education system for business”, and outlined what training and education programmes are needed for business, and how the K-shield programme at the KISA Academy can assist managers to implement best practice.

Professor Heung Youl Youm gave a talk entitled: “Information security readiness certification system in Korea”, and outlined what had been achieved in Korea since 2014. Professor Youm indicated that the objective was to improve cybersecurity capability for various types of organizations, especially SMEs. He made reference to how the certification criteria is used for assigning one of 5 levels of assurance.

Paper 5: International information sharing

Mark King

Introduction

Various potential pitfalls that come with international information sharing in general need to be explored to make sure that they will not delay nor block progress in the cyber arena. These are not new, and come from the analysis of initiatives that have underperformed as well as current programmes. No immovable barriers have been identified, but research to avoid wasted effort is recommended.

There is an existing forum for collaboration on Cyber Situational Awareness under the follow-up to MNE7, where groups from the UK and Korea were and are participants. There is some danger of confusion and some reluctance to participate; possibly because it is not widely understood that NATO is not just a military alliance, and everyone knows that Korea is not in the North Atlantic.

PKI (Public Key Infrastructure)

Underlying all interoperability is the need to be clear as to whom information is provided to and how it is used. The most urgent progress needed in the infrastructure is level 3 PKI, which was explored in greater detail in a follow-up session with KISA (20th January, 2015).

The world-leading Korean PKI has been:

- copied for the Philippines, Vietnam, Cameroon, Panama and Ecuador,
- is being developed for Rwanda, Kenya, and Costa Rica, and
- is under consideration in Indonesia, Brunei, Iran, Egypt, Morocco, Mongolia, and Kazakhstan.

In each case it is a stand-alone system, so further elaboration is needed to support international trade and multinational organizations.

The UK is well-placed as a partner in moving to a wider international use, offering experience with connecting with the other EU nations, America, and the Commonwealth.
This complements the Korean 'if it's broken, fix it promptly' attitude.

The proposed industry-provided bridge in the UK looks suitable. There is a common template for PKI policy documents, so comparison of the two should be relatively simple, although how to handle the inevitable differences will call for deep thought.

Legal

Different legal systems can cause blocks which may reflect a different cultural approach or simply be out-of-date. Research on issues has been done on this in the STORK programme within the EU, but should be widened, at least covering OECD members.

In particular, the handling of evidence varies from country to country, and needs to be accommodated, and the balance struck between retention for a fair trial and deletion for security or data protection concerns.

Further study will be called for to understand how to make progress despite the different arrangements of government, public and private organisations in different countries, e.g., the protocol for a public body in Korea collaborating with a UK not-for-profit organization. It is encouraging to note that Asia/Pacific CERTS work together despite having significantly different status from country to country, so it clearly can be done.

Labels and formats

A frequent problem when organisations work together in a federation is a difference in the way that information is labelled, made harder both by language differences and by changes over time.

A simple 'traffic-light' system has been established in the CERT community, but this may be insufficient for wider use, especially for any that use or abuse a nationalistic position.
Various UK players could benefit from the Korean experience of handling non-US approaches. There is also a need for more feedback; at present information can appear to fall into a 'black hole', and those providing information stop doing so because they do not get any indication that it has been worthwhile. It has to be remembered also, that information sharing involves trust based relationships which need to be maintained through time.

Alignment of motivation

Even where there is no block, where there is no compulsion there is unlikely to be progress unless the aims of the participants align and there is no significant conflict of interest. Since there are costs in sharing (monetary and various forms of risks), the benefits to each organisation need to be understood at senior level. Just removing barriers will not make data flow; education is needed.

It is normal for at least one party to have an interest in the validity of assertions, but where there is mandation the focus may be on cost rather than correctness. For example, for some age verification cases where neither party want, but the seller may want to offload liability.
The commercial model is just as important as the technical model if progress by industry is needed.

Compulsion

There are notable differences in what is mandated in different countries. There are advantages and disadvantages with compulsion, e.g.,

- it ensures consistency and also makes it clear that there is a defined and measurable market for products and services;
- it removes use as a market distinguisher;
- it makes a 'level playing field' but unless everyone is starting from nothing, could lead to high costs for some to adopt;
- it may induce perverse incentives, e.g., reporting all transactions rather than suspicious ones, then raising privacy risks and adding no value for fear of missing something; and
- it can be a barrier to trade.

Occasionally there are also direct conflicts, e.g., being required and forbidden to hold data

such as religion. The UK position may need to be reconsidered after the forthcoming election.

Standards

The work of standards bodies is slow and not glamorous - even if they meet in what may sound like glamorous locations, and inevitably out of season. For standards, and not mere sectoral guidelines, there should be opportunities for all stakeholders to participate, but both SMEs (small and medium sized enterprises) and those lobbyists concerned with privacy are often inadequately funded. Standards need to be developed and adopted but also maintained, and the UK industry bridge has been designed to allow for phased upgrades that do not require the entire federation to make changes simultaneously. (UK based to satisfy at least UK requirements, but not restricted to UK users or usage.)

US NSTIC has been alerted to practical engineering aspects such as character sets, since limitations such as just using ASCII characters are not going to be acceptable. The UK specifications have not come out, and we can feed in from this session that it would be appropriate to allow for Korean names to be in both Hangul and non-simplified Chinese characters.

The EU data protection regulation is still in draft. The 'subject access requests' are clearly expected to be handled online, and currently apply to individuals without limit. A level 3 certificate would seem a likely requirement. Koreans would have the ability to get such a certificate although there is nothing announced for the UK. Some more infrastructure would be needed to establish practical interoperability.

Privacy

The question of sharing information in the sense of publication and/or monetization of data currently in government databases was raised at the workshop in Korea (19th January, 2015), and there are people pressing for this in both countries, not least to encourage innovation. It was suggested that studying the Swedish position would be instructive, since they started from a position of openness and appear to be heading in the opposite direction. The use of privacy impact assessments is essential for demonstrating that the necessary balances have been struck.

Bearing in mind the above points, the following recommendations can be made:

Recommendation 1: The barrier to trade that stops a UK (or other non-Korean) organization being part of the electronic supply chain for a Korean contract must be addressed, both as a trade policy matter and to assist with infrastructure since without the potential to participate no sharing is likely.

Recommendation 2: The UK efforts to handle European character sets for official identifiers should be extended both to support Asian character sets and to handle multiple official names for one entity.

Recommendation 3: Korean thinking on privacy and data protection should be made more widely known in the UK and Europe.

Paper 6: Summary of the papers presented at the Fourth Korea-UK Cyber Security Research Workshop and the way forward

Peter Trim and Heung Youl Youm

Those in attendance at the 4th Korea-UK Cyber Security Research Workshop were:

Mr. Tony Butler, Delphinitum
Mr. Patrick Curry, British Business Federation Authority (BBFA) Ltd
Mr. Neil Fisher, Foreign and Commonwealth Office
Mr. Robert Hall, London First
Mr. Oliver Hoare, Dysart Solutions Ltd
Mr. Mike Humphrey, National Crime Agency
Dr. Pilyong Kang, KISA
Dr. Jaejung Kim, KICA
Mr. Mark King, Broadsail
Mr. Jae Nam Ko, Soonchunhyang University
Mr. Ki-Woon Lee, KISA
Dr. Yang-Im Lee, University of Westminster
Mr. Austen Okonweze, Department for Business Innovation & Skills (BIS), UK
Dmitry Organ, The Risk Advisory Group plc
Dr. Jae Hoon Nah, ETRI
Mr. YeonHo Pang, Science & ICT Attache, Korean Embassy London.
Professor Dae Ha Park, The Cyber University of Korea
Mr. Alan Shipman, Group 5 Training Limited
Dr. Peter Trim (Chairman of the UK Cyber Security Research Network), Birkbeck, University of London
Professor Heung Youl Youm, (Chairman of the Korea Cyber Security Research Network), Soonchunhyang University

After the opening session, Mr. Austen Okonweze provided a talk entitled: "Supporting the growth of the cyber security sector". Mr. Okonweze made reference to the UK government's cyber security strategy and emphasized the need for collaboration with a range of government and non-government organizations. The UK is in need of upgrading its cyber security skill base and there are actions in place to ensure that this happens. He made reference to the National Cyber Security Programme (£860 million) and indicated that the UK cyber security industry is worth £6 billion and employs about 40,000 people. Of particular interest was the Cyber Growth Partnership, which was a joint initiative between government, academia and industry, the aim of which was to boost the UK's global market position in terms of cyber security products and services. Reference was made to a national programme to increase support for cyber security start-ups and small businesses known as Cyber Connect UK; the development of cyber clusters, drawing on the success of the Malvern cluster; the Innovation Vouchers scheme; and s second Cyber Innovation Summit.

Professor Heung Youl Youm in his keynote address entitled: "Recent Korean security policy for the financial sector", talked about various security challenges involving the leakage of personal data. He outlined how malware was down loaded into a user's computer, how a DDos attack was launched, and how the malware gives rise to a Zombie computer. He went on to outline how it is possible to block an attack by Zombie computers on targeted websites.

Several disruptive attack scenarios were presented and so too were a number of major cyber incident cases in Korea. For example, reference was made to the two cyber terror attacks known as 7.7 (7/7/2009) when 36 websites in Korea and the US were attacked and 3.4 (4/3/2011), which is when 40 websites in Korea were attacked. Professor Youm also provided information about the leakage of personal information in 2011, 2012 and 2014; and the 3.20 cyber terror (29/3/2013) incident involving an attack on three banks and three broadcasting companies in Korea. A scenario was also presented of a typical attack scenario relating to personal data leakage, and this was followed by a data leakage incident involving the credit card industry in 2014. Penalties and countermeasures were made known and it is clear that financial firms in Korea will be held more accountable for personal data protection and also for technical security measures which will be strengthened. The financial consumer's rights will also be strengthened as one would expect.

Dr. Yang-Im Lee presented a co-authored paper entitled: "Working within and across cultures: insights into managing international research projects". She focused on various aspects of culture that are important with respect to communication (both verbal and non-verbal) and how a communication mechanism allows appropriate language to be used to convey messages and knowledge. Dr. Lee cited the work of several academics who had undertaken research into cultural value systems and provided an explanation of why it was important to think in terms of the visible and invisible aspects of culture. In addition, an explanation was provided as to why it is important to think in terms of culture having not one but several layers. She also provided several insights into the link between a national value system and an organizational value system. Various UK and Korean cultural attributes and characteristics were highlighted and compared, and emphasis was placed on making known the key factors determining how group work should be undertaken to ensure that an international research project could be managed effectively.

Professor Dae Ha Park addressed the topic: "Cloud Services Security Countermeasure Criteria for Korean Personal Information Protection Act based on International and Domestic Standards". He outlined the situation before the Korean Personal Information Protection Act came into force and then the situation thereafter. Also, he outlined the hierarchal structure encapsulating the Personal Information Protection Act, mentioned the legal basis, and the safeguards and penalties associated with negligence. Reference was made to the personal information safeguards and these were linked with the articles (internal management plan; access right management; password management; access control system; encryption; access record preservation; security programme; and physical access prevention). Professor Park made reference to a project he was involved in entitled: Research of safeguards for personal information under cloud services, the purpose of which was to develop a revised baseline of personal information safeguards considering privacy related issues from the cloud service environment. He finished by outlining the current status of personal information processing in the cloud service environment; risks and countermeasures in the cloud service environment; and a baseline of cloud personal information safeguards and cloud privacy. On reflection it was most interesting to note the methodological approach used for establishing privacy related risks in cloud computing and how the risks were mapped against the countermeasures.

Tony Butler provided a talk entitled: "Reducing people-risk in organizations". He suggested that "despite being amongst the greatest threats in cyber-space, the human-in-the-system has fewest counter-measures available to combat it and, as we have seen from recent events in commercial, financial, medical and political environments, is capable of causing considerable

damage. Big-data techniques are beginning to make some inroads in identifying anomalous behaviour; however, such defensive capabilities are unproven, expensive to deploy and likely to trigger many false positive indications. The UK's Centre for the Protection of National Infrastructure's Insider Data Collection study (CPNI, 2013) identified 18 characteristics that indicate rogue behaviour but, other than recommending that managers should be aware of such behaviour from their own staff, offered no solutions; tellingly, the same report identified that managers and executives were responsible for more than half of the Insider acts examined in the study. Reliance on technical solutions is additionally flawed in that they are retrospective: after-the-event - a rogue act has already taken place by the time observations may be made and any damage-limitation or post-event forensic investigations initiated. An alternative, axiological, approach, borrowing tools and techniques from coaching and HR disciplines, seeks to address the problem in a different way. Employing a recent development of axiology (branded, where proprietary applications are used, as Axiometrics™), enables the identification of people-risk in individuals and teams. In addition, axiology provides a unique method of measuring an organization's human resource environment which, benchmarked over time, provides a reliable method of measuring the business's culture. The CPNI study identified a dysfunctional working environment as the predominant cause of the consequential rogue acts, the axiological approach will resolve many of the issues that led to the 96% of incidents examined in the report that were instigated by individuals that became 'rogue' during their tenure of employment. A similar approach to recruitment and on-boarding would additionally identify many of the 6% of successful job applicants who join an organisation with intent to commit a rogue act. Fundamentally different in composition and deployment to psychometric equivalents, axiologically derived solutions are rapid to implement, largely automated (therefore, relatively low-cost) and, uniquely, ungameable".

Source: Centre for the Protection of National Infrastructure (CPNI). (2013). *CPNI Insider Data Collection Study: Report of Main Findings.* London (April). Available at: http://www.cpni.gov.uk/documents/publications/2013/2013003-insider_data_collection_study.pdf

Alan Shipman covered the objectives and content of the new International Standard ISO/IEC 27018 in his talk. He suggested that this publication "was produced at the request of cloud service providers, and specifies controls and functionality that should be included in their service provision. When cloud storage is used by organisations, and part of the information they store is information about individuals (e.g. personal data), then the cloud service provider is acting as a 'data processor' on behalf of the organisation (the 'data controller'). For the data controller to meet their obligations under Data Protection legislation, they need to be sure that their data processors work with them to ensure compliance". Mr. Shipman raised a number of relevant and timely questions, and offered insights into legal and ethical considerations.

In addition to providing a most insightful talk, Mr. Shipman also brought to the attention of the audience the report entitled: "A Guide to Using the BS ISO/IEC 27018 Standard: For Data Protection in the Cloud", by Chris Mitchell and John Phillips, which was published on 16th February, 2015. The author's state on page 1: "This guide is intended for two audiences. First, those with personal data to process who want to process it in a public cloud service and second, those who offer a public cloud service with an ISO/IEC 27001 certification who want to process customers' personal data".

“Korean cybersecurity capabilities for UK collaboration” was the theme of Mr. Ki-Woon Lee’s talk. Mr. Lee outlined the cyber security framework of Korea and stated that most of the zombie personal computer incidents in Korea occurred in the private sector and because of this KISA has responsibility for dealing with them. He also provided a glimpse into the Cyber Threat Warning System which is divided into five levels (normal, moderate, substantial, severe and critical), and outlined the reporting links and mechanisms adopted by KISA and also the rapid response process. Organizational issues, tasks and job flows were also cited. In particular, reference was made to how a malicious code spreads and what managers need to know about a DNS sinkhole. The speaker also covered various aspects relating to monitoring, analysis, propagation and recovery. It can be noted that the cyber security system in Korea is both formal and comprehensive and KISA scan in excess of two million websites each day in order to detect malicious code and offer support and assistance.

Mr. Patrick Curry provided a talk entitled: “ISO 29115 - Entity Authentication Assurance Framework - What happens next? Mr. Curry made reference to the fact that information protection requires access control and access control is based on Authentication, Authorisation and Audit (AAA). He went on to outline the assurance levels and talk about risk assessment, and referred to assessing confidence in credential service providers and implementing an Authentication Process. Information was provided as regards an Entity Authentication Assurance Framework and establishing an identity and how credentials are issued. Guidance was provided as regards what was being measured, and attention was also given to what is happening in the EU and the USA in terms of both the citizen/consumer and an enterprise. Distributed cyber risk was covered and priority items for discussion were listed.

Mr. Jae Hoon Nah provided an in-depth analysis and interpretation of “Standardization collaboration on age verification” and introduced conventional solutions, attribute aggregation models and attribute based access control. Reference was made to a number of issues and topics and as well as explaining and placing in context both identity and Authentication, attention was given to how the Internet is used and the problems that arise concerning age verification. He explained why it was important to pay adequate attention to current identity federation standards. A number of scenarios were put forward and compared, and a detailed explanation was offered as regards: (1) the Identity Provider (IdP) Mediated Models; (2) Service Provider (SP) Mediated Models; and (3) Entity-Mediated Model.

Oliver Hoare’s talk entitled: “Cyber security in relation to the 2018 Winter Olympic Games in Pyoeng Chang”, drew on knowledge gained from the London 2012 Olympic and Paralympic Games and also raised a number of ‘what-if’ questions. Mr. Hoare explained that the organizers of the London 2012 games witnessed a number of cyber incidents during the Games and although they were well prepared, managing the risk associated with a cyber-attack such as a sports event is complex. He stated that the attack surface is unique and “that there are shifting geopolitical considerations, requiring analysis of threat actors, their capabilities and intentions, and above all the need for good intelligence”. Mr. Hoare discussed potential threats and countermeasure strategy against cyber-attack during an Olympic Games, with particular reference to the next Winter Olympic Games being held in Pyenog Chang in South Korea.

Mr. Hoare stated: “Recent North Korean hackers’ attack on Sony Entertainment has obviously demonstrated the gravity and seriousness with which, senior world leaders consider cyber-attack. Cyber-security is likely to dominate the international security agenda for

sometime, however, this particular incident, along with other recent cyber-attacks in South Korea, gives rise to a potentially serious threat to South Korea and its hosting of the 2018 Winter Olympic Games. There has been a series of cyber-attacks on South Korean financial and media companies between 2011 and 2013 by North Korean hackers, and most recently in December 2014 there has been an attack on a nuclear power plant (although origins of the attack have not been made public, and the attack is reportedly on the non-critical operations). These incidents along with rising political tensions with the North, is likely to put the 2018 Pyeong Chang Olympic Games at risk of cyber-attack. It is generally accepted that hacking as an asymmetric military threat is the most economic way to attack an enemy nation. It has also an advantage to offer a cyber-shelter until the concrete evidence indicates who the offender is/might be. In addition, judicial disparity and application of different laws interrupt the rapid response to a cyber-attack. The Olympic and Paralympic Games is a live event that will be broadcast to an international audience of billions (London 2012 saw 4.8 billion viewers), it cannot be rewound like VOD, and therefore must be well protected in real-time.

The link between the Olympics and sporting events with terrorism is widely known to the general public, from the Munich Olympics to the more recent Boston marathon. However, those terrorists used guns and explosives, whilst in contrast, future terrorists may consider cyber-attack, or cyber enabled attack as a means of conducting terrorist atrocities. Particularly, in the new era of the Internet of Things (IOT), where the attack surface is so much wider and interconnected, that offers greater opportunities for the terrorists to disrupt the games and cause loss of life. Rapid development of digital technology and greater proliferation of cyber-attack tools will increase the risks, which therefore require much more advanced security countermeasures against sophisticated cyber-attacks. The concept that "prevention is more important than cure" should be the watchword for the Olympic cyber-security professionals".

Reflecting on Mr. Hoare's comments, it is useful to re-evaluate the concept of security and to rethink the subject of risk management. As regards the type of potential threat actors that exist, it is important to think in terms of what type of attack might materialize, because to some degree, those carrying out an attack are looking to gain the maximum publicity for what they do and at the same time wish to recruit people to their cause. They also know that they can try something unique and use proxies to disguise what they have done.

Mr. Jaejung Kim provided insights into: "Key elements for PKI federation", and talked extensively about the status of PKI in Korea and the PKI Federation Model, as well as the role that KICA plays. Reference was made to the number of Internet users in Korea and also how accredited certificates are issued. The PKI scheme in Korea was given attention and it was made clear what the responsibilities are regarding the Ministry of Science, ICT & Future Planning (MSIP), which has and specific responsibilities and exercises those responsibilities. The framework for registration was outlined and the lessons learned were cited. It is clear that the Korean government is providing strong leadership with regards to PKI and that in order to avoid duplication of effort, it is anticipated that there will be a single root certification authority. Interoperability is placed in the context of international interoperability and also, discussions are under way with the Asia PKI Consortium which is expected to produce positive results. In order to be effective however, there needs to be mutual recognition of the standards used and also an appreciation that the world wide web is an open environment that needs to be underpinned with a reliable Authentication system. The relevance of this work can be seen from the type of organization that is involved in the different types of market operation and also, how the certificate issuance process works.

Dmitry Organ provided a number of insights into why more attention should be given to help SME's develop their understanding of Cloud computing. He referred to an organization's size, the resources available to it and the skill set required. With specific reference to Cloud adoption vis-à-vis small and medium sized enterprises (SME's), he suggested that the evidence suggests that there has been a steady growth in cyber-attacks on reputable providers, and as a consequence managers have been concerned about trustworthiness and security. He made reference to the fact that trust is a central element in technology acceptance and that trust can be enhanced through certification of Cloud services to security standards. It is important to acknowledge that the standardisation authority acts as a trust mediator. It also has to be remembered that SMEs have their own specific needs and because of this it is not possible to generalize. Managers will form their own view as regards what trust represents, what adoption decisions involve and the value of certification. Although certification is seen as relatively useful for building trust, the perception towards its importance largely depends on the type and industry in which an SME operates. Mr. Organ's talk highlighted the lack of awareness and understanding of security standards by managers and also indicted that managers in SME's may not be fully aware of what Cloud certification means. Because of this collaboration is needed between certification bodies, government and SME's. The recommendations he put forward for the Cloud stakeholders, should improve intelligibility of certification for non-experts and build stronger links between SMEs, service providers and certification bodies. Should this be the case, relationship marketing can play a definite role.

As regards the talk entitled: "The Korean information security certification", Professor Heung Youl Youm incorporated the work of Professor Dae Ha Park and Mr. Jae Hoon Nah, and provided an overview of the two types of management systems in cyber security in Korea: K-ISMS and PIMS. The legal background was explained and most interestingly, the organizational structure relating to both K-ISMS and PIMS were outlined. The duties of the certification committee, the certification authority and the assessment team were all explained. Building on the first part of the talk, information was then provided about the information security readiness scheme and specific references were made to SMEs and their capabilities. As regards the assessment model, which was developed by MSIP/KISA and transferred to the Korea Federation of ICT organizations in 2014, it can be noted that two functions need to be fulfilled. First, a clear statement of the basic controls that organizations should implement to mitigate risk from common threats is needed; and second, a mechanism for organizations to demonstrate to customers, investors, and insurers and other stakeholders that they have taken essential precautions with regards to cybersecurity measures is needed. Much detail was provided and comparisons were made with other management systems in Korea. The talk concluded with evidence from recent security policy changes and a case was made for continuing to improve the cyber security capability of organizations. Another concluding remark reiterated the fact that education and training, though different, are essential with respect to improving the management process vis-à-vis technical controls.

Mr. Robert Hall, before he chaired the session entitled: "Collaboration and Cooperation in Cyber Security and Personal Information Protection", informed the audience that because cyber attacks occur across boundaries, it is essential for nations to cooperate in cyber security and ways need to be found to fund research projects and programmes so that the work that has been started can continue and produce additional cyber security outputs. Owing to the fact that 80% of the critical national infrastructure in the UK is owned by the private sector, it is essential that all the stakeholders come together and share knowledge and find solutions to a range of cyber security problems. In addition, companies need more support from government and need to know who to turn to when they encounter an attack/cyber related

problem. This means that certain government funded cyber security policies and programmes need to be promoted more widely.

Additional presentation

Prior to the discussions at the Korea-UK Cyber Security Applied Research Workshop at Birkbeck, University of London on 24th February, 2015, Richard Pharro from APMG-International provided a talk relating to CDCAT (Cyber Defence Capability Assessment Tool). Mr. Pharro indicated that CDCAT is a management tool that can be used to help managers establish an organization's cyber defence preparedness. It does this by identifying and highlighting gaps and weaknesses, and thus allowing mitigations to be applied. Being able to assess an organization's risk appetite and risk tolerance in uncertain times is something that senior management are focusing on. Because the methodological approach of CDCAT draws on government and industry controls, once a threat/vulnerability has been identified, a control can be put in place to eradicate it. Managers can use the tool to establish the value of specific data/information to the organization and invoke a situational analysis which can then be presented to the board. The scoring system used means that the tool can help managers compare the impact associated with a specific risk with the costs of an improvement plan. It also has the advantage of getting management to think in terms of adopting a holistic security approach as opposed to a narrow or stovepipe approach that militates against a collectivist and inclusive decision making approach to security.

It is clear that managers in a range of industries are concerned with identifying and eradicating corporate weaknesses and need to deploy tools and systems that can harness and utilize cyber security knowledge. Flexible tools and systems allow managers to think in terms of dealing with dynamic risk and dealing with a problem before it escalates out of control.

The way forward

The workshop proved valuable with respect to identifying topics of interest with respect to the Korea-UK Cyber Security Applied Research Workshop, which was held at Birkbeck, University of London the following day. The focus of the workshop was to take forward the discussion relating to research in the area of PKI federation.

By undertaking a joint research project/set of projects in the area of cyber security, it will be possible for Korea and the UK to enhance cyber security awareness and devise and implement specific education and training programmes that enable people to develop the necessary cyber security skill set and put in place appropriate cyber security safeguards.

In terms of government to government cooperation, it is clear that by developing a number of sustainable industry to industry, university to university, and industry to university partnership arrangements, increased cooperation will occur across industry sectors and will give rise to additional cooperation in the area of information sharing to combat illicit cyber activity. It is also envisaged that new technological applications will emerge and result in new cyber security products and services.

There is no doubt that more needs to be done to assist managers in small and medium sized enterprises to develop management systems to counteract the actions of those engaging in cyber crime activity. A major Korea-UK research project/set of projects will help to establish

valuable partnership arrangements that enhance cyber security capacity and offer a more robust defence against those engaging in cyber attacks.

It is envisaged that once research collaboration commences between Korea and the UK, there is likely to be increased activity in the area of cyber security and one of the advantages of collaboration is that new cyber security knowledge will be produced that is then included in undergraduate and postgraduate degree programmes. This will ensure that there is strong cooperation between industry and academia in the area of cyber security knowledge transfer, and the strong working relationships that evolve are expected to provide a basis upon which further cooperation and collaboration will manifest in teaching, and research and development. Ultimately, new market opportunities will arise and products and services will be available to meet the needs of various customers in various markets worldwide. The project outcomes are cited below.

Joint publications:

- Trim, P.R.J., and H.Y. Youm (2014)(Editors). *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership.* British Embassy Seoul: Republic of Korea. Available at: http://eprints.bbk.ac.uk/9561/1/9561.pdf.
- Trim, P.R.J., and H.Y. Youm (2015)(Editors). *Korea-UK Initiatives in Cyber Security Research: Government, University and Industry Collaboration.* British Embassy Seoul: Republic of Korea.

Joint research proposals:

- The work referred to above stems from the second phase of funding in relation to the Global Partnerships Fund scheme and builds on the work carried out in 2013 to 2014. It is envisaged that a grant application will be made for a much more in-depth research project that will be supported by both the UK Government and the Korean Government, and a number of industry partners. Several universities are also expected to cooperate in the research project.

Future expected and/or potential outcomes:

- The existing cyber security research networks (Korea and the UK) will be maintained and expanded.
- An annual Korea-UK cyber security research workshop will be held in Seoul or London.
- A major Korea-UK cyber security research project/set of projects will be undertaken.
- Increased collaboration between industry and academia will materialize and opportunities will be identified for joint research projects, joint academic courses and the exchange of staff.
- Enhanced cyber security provision for small and medium sized enterprises in Korea and the UK will result and will be promoted more widely than is the case at present.

Next project activity:

- The writing of a major research proposal.

Website links:

- http://eprints.bbk.ac.uk/9561/1/9561.pdf.

Paper 7: Trust through certification in SME Cloud adoption

Dmitry Organ

Cloud adoption shows steady growth among small and medium sized enterprises (SMEs), however, recent cyber-attacks on reputable providers, such as iCloud and Dropbox, highlighted concerns about trustworthiness and security. Trust is a central element in technology acceptance. This paper explores the idea that trust can be enhanced through certification of Cloud services to security standards, where a standardisation authority acts as a trust mediator. Various types of SMEs have their own specific needs, which influence the perception of trust, adoption decisions and the value of certification. Although certification is seen as fairly useful for building trust, the perception towards its importance largely depends on the type and industry in which the SME operates. The paper highlights the lack of awareness and understanding of security standards by managers and draws recommendations for Cloud stakeholders, such as the need to improve intelligibility of certification for non-experts and build stronger links between SMEs, service providers and certification bodies, in which relationship marketing can play a definite role.

Introduction

There are an estimated 4.9 million SMEs in the UK, 99.2% of these are micro businesses (Rhodes, 2014) for which information technology is a critical success factor and a key driver for growth. Increasingly SMEs vote in favour of Cloud solutions thanks to minimal upfront expenditure, scalability and ease of implementation. IBM suggests that 85% of new software today is being built for the Cloud (Bort, 2014), this means, in the future businesses will not have much choice but to embrace this new technology. For example, the leading CRM platform Salesforce, is only available as a Cloud application. The Cloud technology is still rapidly evolving (Gartner, 2013), which illuminates various challenges in its adoption by SMEs, such as service security, quality and reliability. Lack of trust and transparency prevents SMEs from utilising the Cloud to its full potential, to make things worse smaller businesses are not seeking much needed professional help in an attempt to minimise financial expenditure (Young, 2013, p.14).

The government responded with increased amounts of advice about online compliance, however, it is not always aimed at micro enterprises that require support most. Active promotion of voluntarily certifications to security standards for both Cloud services and the SMEs is another area actively explored by industry policy makers as part of the assurance mechanisms (Sunyaev and Schneider, 2013, p.412). Despite the fact there is currently a growing effort aimed at marketing of Cloud attestation and development of simplified adoption recommendations, little is known about their practical benefits for small enterprises. It is unclear if managers are able to assess existing adoption frameworks and certification standards, and integrate them into their business models.

This study offers a comprehensive literature review and obtains practical information from in-depth interviews with senior SME managers in order to investigate the relationship between two features of Cloud computing: certification and trust. It also explores how both of these elements affect Cloud adoption. Furthermore, the value of Cloud certification for both SMEs and Cloud providers is looked at in order to produce managerial recommendations for Cloud stakeholders.

SME competence as a determinant of Cloud adoption

SMEs are heterogeneous in size and profits, they aggregate different business needs that are shaped by the client base and the sector in which they operate. Research by the Danish Technological Institute suggests that an SMEs competence level can act as a determinant of the Cloud adoption paradigm (Laugesen, 2012, pp.6–7). Three types have been identified: the lowest segment (52%) is characterised by basic skill level and no international exposure, e.g., start-ups; the middle segment (35%) has an average dynamic skillset, potential for growth and international expansion; and the top segment (13%) includes globally competitive firms which comprise cutting-edge innovation and high potential for growth.

The same research found that the segment with the lowest skillset most frequently adopted off-the-shelf, SaaS public Cloud products – often free rudimentary tools every business requires, like email and word processing. The drive towards the Cloud is dictated by cost savings, quick adoption and ease of use, whereas obvious vulnerabilities are in the lack of IT competence, financial constraints, inability to assess associated expansion risks, and regulatory requirements (Blackburn, 2012, p.5). The intermediate segment demonstrates more specific Cloud needs. As more financial resources become available, Cloud adoption involves better planning and professional advice, such as ROI evaluation. SaaS systems include more business specific applications, e.g., CRM. Depending on the SME industry, PaaS and IaaS are used for Web hosting, Cloud storage, databases or remote desktop terminals, especially for hi-technology companies and the financial sector (Badger et al., 2012, p.43). Potential for growth makes these SMEs more likely to consider engaging with certified Cloud providers to foresee future regulatory and clients' demands, certifications such as ISO 27001 are often seen as a means of gaining competitive advantage (Brophy, 2008, p.7). The top 13% have all the finances needed to employ top experts in ICT and security, thus, Cloud adoption is likely to be assessed using "best practice" frameworks and with the help of consultants. In Taiwan SMEs with high IT capability are known to significantly boost Cloud adoption intention due to improved ability to forecast outcomes and manage unpredictable turbulences. The requirements of such SMEs can be extremely complex, and a heavy reliance on ICT prompts attention to cyber security and corporate resilience, and certification compliance is often enforced by regulators or trading partners (Hsu et al., 2014, p.484).

Influence of SME size on Cloud adoption

SME size plays a pivotal role in perception and attitude towards IT adoption, organisational structure and culture, availability of resources and skills. Larger firms can afford to take greater risks when deploying new IT models. They increase profits faster, export twice more than micros and are 55% more likely to seek external expert advice than micros and better invest in staff training and equipment (Lomax, 2013, p.62). Despite evidence that professional guidance from the outside has a positive influence on growth, small and micro enterprises are typically managed in an autocratic way by the owner, who makes business decisions singlehandedly (Blackburn, 2012, pp.17–21). Lord Young's (2013) report on growing micro-businesses in the UK exposed the fact that small firms tend to undervalue the significance of external advice, and are reluctant to invest in expert help during a difficult economic climate. Matters are only made worse by government advice which is either too simplistic and fragmented, or aimed at the corporate sector and is difficult to navigate through (Young, 2013, p.25). As a result, "do it yourself" is a prevailing ICT approach in organisations with 1-9 PCs, whereas larger firms usually employ professionals. Free

subscriptions for web based SaaS applications, become almost a "default" solution for micros. The use of multiple decentralised free Cloud accounts (e.g., Dropbox) poses a ticking bomb for many businesses, making their IT unmanageable as demands grow. Unlike larger SMEs, micros rarely perform thorough ROI calculation, which is likely to result in overspending due to poor managerial decisions.

Role of SME industry in Cloud adoption

Belongingness to a certain industry largely determines the way in which an SME operates, establishes an attitude to security, attestation and corporate governance, e.g., financial services and law firms have more focus on ICT and how it is implemented, than micro retail businesses (Tan and Lin, 2012, p.10). SMEs working in customer relationship management, finance or e-commerce are more than twice as likely to use the Cloud, than those across all industries on average (Diamadi et al., 2011, p.5). Industries, such as e-commerce, imply strict requirements as regards the handling of electronic data, which must be reflected in the decision making process about Cloud adoption. Such requirements include whether data can be sent overseas, how long it needs to be retained, and for what purposes it can be used. Breaching the Data Protection Act 1998, for example, will result in a criminal offence or a personal liability of a director (Bange and Hann, 2012, pp.2–7). As a result certification becomes especially relevant: e.g., moving some or all data to the certified Cloud provider significantly simplifies the auditing process, as the auditors can be pointed in the direction of the Cloud provider for some of the answers about cyber security.

Technology adoption frameworks

Technology adoption by micro and small firms greatly differs from larger businesses. In micro firms choices are predominantly made by one individual based on their limited competences (Blackburn, 2012, pp.17–21). Decision making in such a scenario is well explained by the Theory of Reasoned Action (TRA), which focuses on beliefs and attitudes as determinants of consumer buying, TRA assumes that individuals will make rational choices at the best of their abilities, based on the information available to them (Ajzen and Fishbein, 1980). Managers rarely have a good understanding of Cloud technology, and because of this their reasoning will be limited to the information available to them, their level of education and to their ability to evaluate information, all of which makes managers' choices dubious. The TRA concept was used to develop a Technology Acceptance Model (TAM). It uses variables of perceived usefulness and perceived ease of use of technology to determine attitude and intention to use the technology (Davis, 1989, p.320). TAM applies especially well for firms which use free Cloud services, as this model does not take cost factors into account. Lucas and Spitler (1999) further elaborated this model and see social norms as "more important in predicting the use of technology than are users' perceptions of the technology" (Lucas and Spitler, 1999, p.304), such social factors would take into account manager's trust and confidence in technology alongside with other factors. Trial can also become a key to the purchasing decision, previous experience using a free Cloud service, may prompt to upgrade to a paid account. Such a transition would also reduce the fear of the unknown and act as a trust catalyser. Prior positive experience of a similar technology, as well as its effective implementation by competitors, are likely to fill managers with confidence and enthusiasm towards such services (Lippert and Forman, 2005, pp.363–381). Following a social trend can be another behavioural choice determiner, e.g., desire to certify to ISO 27001 because everyone else in the industry is doing so (Li, 2005, pp.2–5). Larger SMEs with a high skillset are likely to use sophisticated Cloud adoption frameworks, taking

into account technical suitability, usability, economic value, control, security and reliability, issues of trust and compliance (Saripalli and Pingali, 2011, p.320). The problem is, most of these frameworks are extremely complex and are aimed at the corporate sector, this makes practical application of such adoption models questionable for small firms.

Dimensions of trust in the Cloud

In any business interactions trust is reciprocally related to reputation and success, this is especially relevant to intangible e-commerce and Cloud products. In the technical literature, such as ISO/IEC, trust is sometimes linked to trustworthiness and assurance. For example, the whole section of the ISO/IEC 15408 certification standard is devoted to the issue of trust, where it is observed under the prism of "so called evaluation assurance levels" (Osterwalder, 2001, pp.33–39). Trust is a multidimensional construct and can be approached from institutional, behavioural, intentional and dispositional perspectives. Institutional trust is essential for the Cloud as it implies structural assurance, which "gives confidence and belief that protective structures, that are conducive to situational success, are in place" (McKnight and Chervany, 2001, p.44). When choosing the Cloud provider such structural assurance is backed by SLA guarantees, clear procedures, certification and compliance. "These with low trusting intention tend to want to formalize their agreements", therefore, there is a probability that certification can boost trust in Cloud computing (McKnight and Chervany, 2001, p.44). Certification also "provides historical or missing experiential information about a seller or a product, thus providing a potential mechanism to increase trust" (Corritore et al., 2003, p.752). Reputation systems play a similar role, e.g., rating portals, such as Passify.it and professional discussion boards. Certifications, though, prove to be more reliable and escape bias that rating portals and publications may suffer. Cloud providers often make alluring promises about the quality of their products, but before the decision can be made, managers in an SME prefer to verify that the statements are valid. One of the easy ways for both marketers and the consumers to achieve this, is by "borrowing" trust from accreditors who are seen as trustworthy, and therefore, acting as an alternative control mechanism (Huang and Nicol, 2013, p.7).

Trust relationships between the SME and the Cloud provider

The established view in marketing theory is that relationships play an important role in shaping trust between businesses. Well managed relationships have great potential to generate belief in a partner's honesty, integrity and benevolence, give sense of equality and create tolerance to failure, all of which shapes trust (Geyskens et al., 1998, pp.226–229). Today when Internet facilitates social networking and explosion of CRM systems, managers understand that building customer loyalty and product differentiation is impossible without deeply understanding and tailoring the company's products to consumer needs, this encouraged a 'consumer centric approach', in which users are often encouraged to co-create products (Zbuchea, 2009, p.305). Relationship Marketing, which aims to establish a network of financially beneficial sustainable relationships, brings transparency to the communication process between organisations by simplifying the consumption of information, and making the whole process more efficient (Zbuchea, 2009, p.306).

In the context of Cloud computing, relationship marketing can help to address a number of issues. Firstly, the difficulty SMEs have in communicating with Cloud giants during planning, adoption and at post-implementation stage, when unforeseen problems may arise, is well known. Whereas it may be a manageable task for SMEs with internal IT departments,

the rest may rely on the experience of IT consultancies and Cloud brokers. Montoya et al., (2010, p.81) empirically proved that post-implementation intervention by the Cloud provider may build or restore trust to a company. Another issue is the incompetence of SME managers, which prevents them from making the best choices about information technology, this can be aided by seeking external help, or by educational marketing. Finally, there is a lack of understanding of risk, certification and security standards and their benefits for a particular SME. While this is being tackled by governments in a form of online advice about 'best practices', the information given is either too simplistic or even misleading to bring noticeable value, (e.g., advice to always install software updates) are often aimed at selling security products, or too complex and time consuming to understand (Young, 2013, pp.14–15, and p.49). Cloud providers place an increasing amount of effort into promoting security standards and their meaning to the end user by setting dedicated security portals. Google established a 'trust' portal, which covers the topics of reliability, security, privacy, compliance and transparency (Google Inc., 2014). The title of Salesforce domain speaks for itself – it reads 'success is built on trust', this Internet resource covers every possible aspect of trust and security in great detail, potential users are welcome to ask questions and engage in discussion online (Salesforce.com, Inc., 2014).

Cloud brokers can play a vital role in building and maintaining trust relationships. They act as an intermediary between SMEs and Cloud providers and create close personalised relationships with SME managers. Importantly, Cloud brokers possess in-depth knowledge of Cloud products and have the ability to appreciate strengths and limitations of each one of them, which can be especially valuable in complex scenarios, when a mix of different products is required. "Moving to the Cloud means buying from Cloud providers who do not always provide a transparent view into the inner workings of their infrastructure. While the exact nature of the issues vary depending on the type of Cloud service" (Hyek, 2011, p.18). Cloud brokers save time during implementation, and provide subsequent support, which adds extra confidence for managers and provides a safety net in case something goes wrong. In some cases there is opposition in IT departments about moving to the Cloud, "because different skills are required, existing IT staff will likely need to be retrained or replaced. Organisations face a conundrum: if they attempt the Cloud transition with existing staff they will likely meet internal resistance, but new staff would lack knowledge of company processes" (Hyek, 2011, p.7). PWC highlights changes for CIOs within organisations: "the CIO must lead IT into a new era in which the role of the IT department will shift from an emphasis on technical skills to abilities in managing relationships with service providers and internal business units. Given the complexity of Cloud implementations, it's not surprising that brokers are gaining favour among CIOs. According to Gartner, by 2015 brokers will handle at least 20% of all Cloud services, up from less than 5% today" (PWC, 2011, pp.9–10).

Cloud certification: benefits and challenges

Leading European cyber-security organisations, ENISA, CERT-UK and CSA, call policy making and certification critical in creating trust in the Cloud. Directed by the EU Commission, ENISA has embarked on creating the Cloud Certification Schemes List (CCSL) to help mitigating risk and boost trust in the Cloud (ENISA, 2014, p.2). Based on the marketing-induced research by Grayson et al., (2008), trust to Cloud providers largely depends on trust to the industry, known as 'narrow scope trust'. In turn, narrow scope trust is dependent on the endorsement by government bodies ('broad scope trust'). This implies that the Cloud industry could see benefits in partnering and investing in certification bodies and

promoting certification and compliance. If Cloud providers choose to opt out from collaboration with such government institutions, it may reduce the burden of bureaucracy and regulation for providers, but also decrease trust in the Cloud industry (Grayson et al., 2008, p.252).

There is a clear demand for certification and compliance: 55% of respondents of the 'Boardroom Cyber Watch Survey 2014' indicated their business allies inquired about corporate security arrangements 50% more frequently than a year earlier and showed an increased interest in standards such as ISO/IEC 27001 (Calder, 2014, p.7). This is understandable, as certain industries are legally obliged to comply with various certifications, e.g., Cloud provider offering tools for supporting card payment transactions is likely to require a PCI – DSS attestation (ISO, 2014). It is not unusual that companies wishing to move to a public Cloud, which lacks the "right" certification, get stuck because of issues with their auditors (Emison, 2013). For a Cloud provider, certification may help to improve security, enhance customer satisfaction, increase sales, and provide competitive advantage; for organisations - optimise operations, improve resilience and open up new markets.

Even in a traditional IT environment, certification is complex enough by its nature, in the fluid and dynamic Cloud environment, ensuring security compliance will remain challenging. The sheer ocean of certification schemes may become overwhelming for non-expert SME managers only adding confusion, instead of acting as a navigational beacon. Just the standards recommended by ENISA, count to as many as 12 (Dekker and Liveri, 2014, pp.6–7):

ISO 27001/2
ISO 20000 (ITIL)
CSA Open Certification Framework
EuroCloud Star Audit
SOC 1-2-3
PCI – DSS
Europrise
FISMA
Cloud Industry Forum Code of Practice
ISACA COBIT
Security Rating (Leet Security)
TUV certified

Different standards are governed by independent certification bodies around the globe without necessarily cooperating with each other. Some of the best known are NIST, OCC (USA); ETSI, ENISA, SIENA (Europe); KCSA, CFF (South Korea); OGC, GICTF, CBA (Japan) and ISO/IEC JTC1, IEEE (Global) (Sakai, 2011, p.2). Despite developments in EU legislation which aims to consolidate data protection rules within the EU, data compliance is facing sometimes unresolvable cross-border legal challenges, for example, when a different law applies to data protection in various counties. Another serious issue is that it is time consuming, labour-intensive, expensive and involves a repetitive auditing process which many cannot afford. Continuous efforts to simplify a certification process by means of software automation, which reduces the role of the auditor are on-going, but have not been very successful mainly because the 'certificating machine' needs to be constantly updated to understand the latest security protocols, vulnerabilities and adapt to emerging Cloud products, but also provide assurance that the certifying software has not been tampered with

in a malicious way. The issues above are well known and improvements are constantly being developed. The question is, what effect do these points have on the minds of SME managers, on their confidence in certification, their ability to make decisions, and their trust in the certification schemes?

Interview outcomes and discussion

During the course of the research, 5 in-depth interviews with senior SME managers were conducted to elicit practical views on the topic. Semi-structured interviews were chosen to allow more freedom in collecting data, so that new ideas could be drawn. The candidates included: 1) a CIO of a law firm; 2) a director of an IT consultancy; 3) a senior IT manager of a non-profitable organisation; 4) the head of a risk management firm; and 5) the owner of a small Cloud provider.

The summary of the interview responses revealed that key factors that shape trust in the Cloud are: reliability, ease of use, data security and privacy, this agrees with TAM theory and the findings of Huang and Nicol (2013). Interestingly, the respondents indicated that interruption in service delivery would be a lot more harmful, than the potential breach of confidentiality – not something found in the literature. The interviewees confirmed that transparency about data handling and ability to elicit detailed information about the internal workings of the Cloud provider, play a significant role in shaping trust judgments and adoption decisions, this is aided by information from online communities, and word of mouth, as mentioned by Lippert and Forman (2005). What is peculiar, is that none of the interviewees mentioned the use of any of the Cloud adoption frameworks, as outlined by Greenwood et al., (2010, p.456) or Marks and Lozano (2010, p.113), despite the fact that three of the respondents occupied a senior IT role in a highly skilled SME, one of which was an IT consultancy. This raises serious questions about the practical usefulness of such adoption models. Certification is seen by interviewees predominantly as an indicator of whether the Cloud provider is worth dealing with, nonetheless, certification was not found to create a directly strong impact on trust on its own, largely due to a lack of understanding of the technicalities of the scheme. Certifications were compared with professional qualifications when hiring new staff, it gives a point of reference as to what the candidate is professionally capable of, but managers always prefer to interview the contender to find evidence of expected skills. Reputation was said to have more value, than attestation, besides, in case of reputational damage, certification may become a powerful instrument to rebuild trust. At the same time, interviewees unanimously agreed, that loss of the certification by a Cloud provider would affect a SME's trust. Such a scenario instantly raises questions about trust to the supplier, regardless of the fact of whether it was a conscious decision to drop certification, or it was a result of a security breach or due to financial constraints. This can be explained by the theory of trust constructs where in the case of certification withdrawal, 'structural assurance' will be broken (McKnight and Chervany, 2001, p.44).

Among the drawbacks, managers point out that it is often impossible to precisely understand the meaning of ISO 27001 without seeing the statement of applicability, which spells out what exactly is covered by the security standard. Certification standards are criticised for being rather "flexible", commercialised and their reliability was occasionally described as "questionable". Complexity and lack of clarity also depreciates certification as a trust validation tool. Overall, the interviewees are a lot less enthusiastic about the effect of certification on trust, than it is portrayed by accreditation bodies. Respondents have accentuated, that the need of SMEs to comply with government regulations defines the

significance of Cloud certification for SME managers more than anything else: stock brokers and equity dealers are as such FCA regulated, these companies want to cover themselves in case of a data loss or any other breach of security, and they want to relay this responsibility onto a Cloud provider. Regulated firms are likely to adopt Cloud products covered by the same type of security standard, in order to simplify their auditing process, some are happy to outsource their entire infrastructure to a Cloud provider, as long as that provider is ISO compliant, they by default become ISO compliant. On the contrary, micro enterprises and start-ups often disregard the attestation element in their decision making process, since their decisions are driven predominantly by cost efficiency and time to market. All interviewees universally agreed that managers have little or no understanding of certification standards. Even when they do consider it important, it is mainly because they were advised so, or under the influence of marketing. There is a lot of buzz about certification, and for certain categories of people it might sound quite appealing even though they have no understanding of what it actually means. In summary, respondents acknowledged that promoting certifications is far less efficient than building strong trusted relationships with the client.

The interview data demonstrates that the characteristics of SMEs play a pivotal role in shaping attitudes towards the importance of Cloud certification. Among the essential features, respondents pointed out 1) industry type, 2) SME competence, as well as 3) turnover and 4) size of the enterprise. This mirrors the findings in the literature outlined above. Most get certified either because they are required to, or because all their competitors have it. For those companies that are not regulated, and do not have the requirement, certification will not make any positive difference. Two of the respondents criticised public sector organisations for requiring certifications from their partners, whereas they themselves preferred to remain uncertified.

The value of stored data is another factor that was brought up during the interviews: if the loss of data will cause a devastating effect on the firm, certification of the provider will be highly desired. Managers agree that micros and start-ups frequently choose whatever is cheaper or free, certifications is not something they think of. The director of the IT consultancy admitted they had two or three instances, when things went wrong as a result of the implementation of such free solutions.

Implications for managers in SMEs

Managers need to appreciate the benefits and limitations of the Cloud. Like any other IT system, it is never entirely secure. Revelations by Edward Snowden and WikiLeaks exposed the fact, that no certifications or security protocols can prevent governments from acquiring personal data (Greenwald and MacAskill, 2013). Cloud providers remain vulnerable to hacking attacks which either exploit unrevealed technical vulnerabilities, or are socially engineered, recent iCloud and Gmail intrusions present the latest examples (Love, 2014; Stone, 2014). Certifications can provide only a degree of confidence that the Cloud is safe, reliable and the provider will adhere to the promises made. It is assumed that the holistic assessment of the Cloud service (details of data handling and security, internal culture, reputation, consumer feedback) would be more appropriate, than blind reliance on certification. Managers also need to be vigilant when considering IT certifications as a ‘seal of confidence’ and understand that security standards have limitations. The interview data indicated that a certified Cloud provider is not guaranteed to be better, but will almost certainly, be more expensive. Heavily regulated firms will see more benefits in certification, outsourcing IT to a certified Cloud provider can lower the burden of auditing and reduce

costs. Micro enterprises will see little or no benefits, unless they are required to comply to security standards.

Choosing the right Cloud paradigm is critical for any SME. Start-ups can get great value from free SaaS products at the 'proof of business concept' stage. However, once they achieve sustainable growth and expansion, they need to rethink their approach to IT, in order to prevent potential Cloud chaos. It is doubtful owners of SMEs will be able to make optimal Cloud choices alone. Cloud brokers and consultancies are vital for expert advice on implementing the right IT service(s). Although they involve extra cost, brokers are likely to generate return by assisting with product trial, migration and providing post-implementation support. Relationship marketing theory suggests that brokers may act as a trusted partner between the SME and the Cloud provider, and facilitate the development of lasting and mutually beneficial business relationships.

The success of a major organisational change, such as Cloud adoption, is impossible without support of senior management or the owner. Managers need to be aware of the possible resistance of staff in the internal IT department to migrate to the Cloud, explained by fears of job insecurity and the need to acquire new skills. Cloud brokers can reduce the risk of uncertainty and help to re-build trust based relationships. From an internal marketing perspective, Cloud brokers may "assist in staff training, which should be user-centric as opposed to technology-centric. Effective training by the Cloud broker should be service oriented, focused on the user needs and concerns about the new system with respect to employees' job roles/functions" (Montoya et al., 2010, p.80). Cloud often relays more control over data handling to end users (e.g., Google Drive), therefore, appropriate security mechanisms must be put in place, such as 2-factor authentication and monitoring for external data exposure (i.e., file sharing via Web links). Employees must be made aware of the possible implication of systems mishandling.

Implications for Cloud providers

Cloud providers spend vast amounts of resources to achieve compliance to security standards, therefore, it is of paramount importance for them to ensure that certification will convert into a source of competitive advantage. Large providers like Amazon or Google are almost always certified, as they have a huge customer base, some of whom will inevitably require certification. For smaller providers, it is a lot harder to justify significant expenditure on certification, as well as hurdles of regular auditing and increased bureaucracy. The research data shows, that the only incentive for small providers to acquire certification, is when their business model is orientated at customers, who are legally obliged to conform to a certified service. The SME managers interviewed stated that explicit information about the provider and the service, as well as willingness to share this information, has a lot more weight when it comes to signing a contract. It is suggested that for a smaller provider certification may become a competitive disadvantage, due to increased cost and possible decrease in service quality as a trade-off. For some small providers security risks can be mitigated by storing and processing all their data in the Cloud infrastructure (IaaS) of another certified vendor.

It would be, possibly, counterproductive for Google or Saleforce to excessively advertise security of their offerings, as psychologically it might achieve quite the opposite effect from what is desired. It is deemed to be more efficient to engage marketing and communications in such a way, where security information is unobtrusively made available to the consumer in a clear and transparent manner (Salesforce.com, Inc., 2014). Small providers can leverage an

advantage from having a narrower customer base, and by placing emphasis on building close, personalised and lasting relationships with the SMEs, and react quicker to emerging consumer demands. Such relationships are likely to facilitate a fluid exchange of knowledge, and forge a higher degree of trust. Essentially, in such a scenario, this removes the need for Cloud brokers, which may become a source of competitive advantage on its own, as suggested by relationship marketing theory.

Recommendation 1: Cloud providers need to put in effort to safeguard the trusted image of the Cloud industry, this can be achieved by partnering with certification bodies and regulators, and also invest energy into clarifying the meaning of certifications and embedding them into the evoked set of the consumer.

Implications for standardisation authorities

There is mounting pressure on government institutions like ISO and ENISA to promote Cloud security, without overcomplicating its delivery. Certification bodies like ISO depend on their integrity and credibility. Trust in these authorities is ultimately transferred into their security standards. However, providers like Amazon who conform to multiple security standards become vulnerable to a recent 'Heartbleed' encryption security breach (Curtis, 2014). The interviewees pointed out, this became damaging not only for the reputation of Cloud providers, but also for the certification industry. Technology giants such as Google, Facebook and Cisco urged collaborative schemes to improve security of open standards, certification authorities need to actively engage in improving relationships with technology providers and demonstrate they are leaders and not laggards in this initiative. Broad acceptance and implementation of their security standards is vital for their success, however, SMEs are reluctant to make huge investments into internal auditing and compliance and rarely see competitive advantage in doing so. In particular, the reluctance of the public sector, e.g., councils, schools and hospitals, to undergo formal accreditation undermines the message of the government of the need of certification for SMEs. SME managers find it absurd that the public sector is expecting their commercial partners to be accredited without feeling the need to undergo certification themselves.

Recommendation 2: The government need to identify core IT certifications for the public sector and strongly encourage organisations to implement them. This can motivate the private sector to follow the trend and facilitate the creation of trusted links between the private and public sectors. Streamlining 'best practices' in the public sector may also return savings due to the reduction of human error and downtime of IT systems.

Recommendation 3: Certification bodies need to create ways to reduce the cost of auditing, while preserving the consistency of assessment quality, automation may bring certain benefits. Development of free of charge interactive and user intuitive step-by-step online guides for different types of SMEs, based on their needs and capabilities may help to tackle managers' incompetence in IT certification schemes and improve awareness.

Recommendation 4: The government should be extra vigilant when giving oversimplified cyber-security advice, which is at times misleading, e.g., HM Government Cyber Street campaign recommends that 'You should always download and install software updates immediately when they appear on your computer, phone or tablet' (HM Government, 2015). Such advice can be counter-productive as blind deployment of updates can sometimes cause undesired effects and even hinder devices from operating properly (Hern, 2014).

Recommendation 5: Standardisation institutions across different countries need to double their efforts to increase compatibility of various standards to exclude unnecessary replication.

Conclusion

The discussion set out in the above attempted to establish the role of Cloud certification with regards to trust, in the context of SME Cloud adoption. The research drawn upon has shown that certification plays an important role in shaping trust in the Cloud – it offers a unified way of evaluating numerous Cloud attributes across the industry, which reduces uncertainty. The interviews undertaken with IT managers revealed, that the perception of certification is not homogeneous: it depends on the industry in which the SME competes, the size, and the level of competence of the firm. In cases where SMEs have to abide by strict data protection rules, certification is seen as a useful tool to retain trust, it also allows data protection responsibilities to be shared between the firm and the Cloud provider. Certification is also seen as an instrument, which can be used by IT managers to convince an organisation's executives to migrate to the Cloud. On the other hand, the study revealed that micro enterprises and start-ups see little or no benefits in certification, due to a lack of understanding, severe financial constraints, and shortage of time for planning their IT. Smaller enterprises, which are themselves Cloud providers or IT consultancies, refrain from acquiring certifications due to the cost factor, and also because of worries that lapse of certification may cause reputational damage. It appears that standardisation organisations, like ENISA, are moving in the right direction, attempting to simplify and unify security standards. However, they may need to invest more energy into building closer relations with leading technology providers and SMEs, to improve the image of trustworthiness and integrity across the industry. ENISA could better target non-experts by creating jargon-free easy to read guides, designed specifically for micro and small enterprises.

Recommendation 6: Further academic research is needed to explore how relationship marketing can establish trust based relationships between Cloud stakeholders.

References

Ajzen, I., and Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behaviour*. Englewood Cliffs, NJ: Prentice Hall.

Badger, L., Grance, T., Patt-Corner, R., and Voas, J. (2012). Cloud Computing Synopsis and Recommendations. [online]. Available from: http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf [Accessed August 10, 2014].

Bange, V. and Hann, G. (2012). An Overview of UK Data Protection Law. [online]. Available from: http://www.taylorwessing.com/uploads/tx_siruplawyermanagement/NB_000168_Overview_UK_data_protection_law_WEB.pdf [Accessed August 10, 2014].

Blackburn, R. (2012). Segmenting the SME Market and Implications for Service Provision. [online]. Available from: http://www.acas.org.uk/media/pdf/2/6/Segmenting-the-SME-Market-and-Implications-for-service-provision-accessible-version.pdf [Accessed August 19, 2014].

Bort, J. (2014). Why Cloud Computing is Such a Game-Changer. *Business Insider*. [online]. Available from: http://www.businessinsider.com/this-chart-from-ibm-explains-why-cloud-computing-is-such-a-game-changer-2014-4 [Accessed August 29, 2014].

Brophy, M. (2008). ISO 27001 Global Survey. [online]. Available from: http://www.d1073625-1.blacknight.com/format/ISO27001GlobalSurvey.pdf [Accessed August 20, 2014].

Calder, A. (2014). Boardroom Cyber Watch Survey: 2014 Report. [online]. Available from: www.itgovernance.co.uk.

Corritore, C.L., Kracher, B. and Wiedenbeck, S. (2003). On-line Trust: Concepts, Evolving Themes, a Model. *International Journal of Human-Computer Studies*, 58(6), pp.737–758.

Curtis, S. (2014). 'Heartbleed' Bug in Web Technology Threatens User Data. [online]. Available from: http://www.telegraph.co.uk/technology/internet-security/10754169/Heartbleed-bug-in-web-technology-threatens-user-data.html [Accessed September 19, 2014].

Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), pp.319–339.

Dekker, M. and Liveri, D. (2014). *Certification in the EU Cloud Strategy*. ENISA. [online]. Available from: https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy [Accessed August 10, 2014].

Diamadi, Z., Vora, A., Dubey, A., and Pleasance, D. (2011). Winning in the SMB Cloud: Charting a Path to Success. [online]. Available from: http://www.mckinsey.com/~/media/McKinsey/dotcom/client_service/High%20Tech/PDFs/Winning_in_the_SMB_Cloud.ashx [Accessed August 10, 2014].

Emison, J.M. (2013). Cloud Security: Why Auditors Are Part Of The Problem. *InformationWeek*. [online]. Available from: http://www.informationweek.com/global-cio/compliance/cloud-security-why-auditors-are-part-of/240160567 [Accessed July 30, 2014].

ENISA. (2014). *Benefits, Risks and Recommendations for Information Security*. ENISA. [online]. Available from: doi:10.2759/44445 [Accessed July 21, 2014].

Gartner. (2013). Gartner's 2013 Hype Cycle for Emerging Technologies Maps Out Evolving Relationship Between Humans and Machines. [online]. Available from: http://www.gartner.com/newsroom/id/2575515 [Accessed August 25, 2014].

Geyskens, I., Steenkamp, J. and Kumar, N. (1998). Generalizations About Trust in Marketing Channel Relationships Using Meta-analysis. *International Journal of Research in Marketing*, 15(3), pp.223–248.

Google Inc. (2014). How Google Handles Your Data. *Google for work: Trust*. [online]. Available from: https://support.google.com/googleforwork/answer/6057301?rd=1 [Accessed September 1, 2014].

Grayson, K., Johnson, D. and Chen, D.-F.R. (2008). Is Firm Trust Essential in a Trusted Environment? How Trust in the Business Context Influences Customers. *Journal of Marketing Research*, 45(2), pp.241–256.

Greenwald, G. and MacAskill, E. (2013). NSA Prism Program Taps in to User Data of Apple, Google and Others. *The Guardian*. [online]. Available from: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [Accessed September 11, 2014].

Greenwood, D., Khajeh-Hosseini , A., Smith, J.W., and Sommerville, I. (2010). The Cloud Adoption Toolkit: Addressing the Challenges of Cloud Adoption in Enterprise. *CERN Document Server*. [online]. Available from: http://cds.cern.ch/record/1254484 [Accessed August 2, 2014].

Hern, A. (2014). iOS update: Apple Apologises for Breaking New iPhones. *The Guardian*. [online]. Available from: http://www.theguardian.com/technology/2014/sep/25/ios-update-apple-apologises-breaking-new-iphones [Accessed October 2, 2015].

HM Government. (2015). Cyber Street. [online]. Available from: https://www.cyberstreetwise.com/software-updates.

Hsu, P.-F., Ray, S. and Li-Hsieh, Y.-Y. (2014). Examining Cloud Computing Adoption Intention, Pricing Mechanism, and Deployment Model. *International Journal of Information Management*, 34(4), pp.474–488.

Huang, J. and Nicol, D.M. (2013). Trust Mechanisms for Cloud Computing. *Journal of Cloud Computing*, 2(1), pp.1–14.

Hyek, P. (2011). Cloud Computing Issues and Impacts. [online]. Available from: http://www.ey.com/Publication/vwLUAssets/Cloud-computing_issues_and_impacts/$File/Cloud_computing_issues_and_impacts.pdf [Accessed August 20, 2014].

ISO. (2014). ISO and SMEs. *About ISO*. [online]. Available from: http://www.iso.org/iso/home/about/iso-and-smes.htm [Accessed August 9, 2014].

Laugesen, N.S. (2012). *Cloud Computing Cyber Security and Green IT: The Impact on e-Skills Requirements*. European Commission. [online]. Available from: http://ec.europa.eu/enterprise/sectors/ict/files/eskills/e-skills_and_cloud_computing_final_report_en.pdf [Accessed August 10, 2014].

Leet Security.
http://www.leetsecurity.com/

Li, L. (2005). A Critical Review of Technology Acceptance Literature. [online]. Available from: http://www.swdsi.org/swdsi2010/SW2010_Preceedings/papers/PA104.pdf [Accessed August 20, 2014].

Lippert, S.K. and Forman, H. (2005). Utilization of Information Technology: Examining Cognitive and Experiential Factors of Post-adoption Behavior. *IEEE Transactions on Engineering Management*, 52(3), pp.363–381.

Lomax, S. (2013). SME Business Barometer: February 2013. [online]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/197450/bis-13-p75a-sme-business-barometer-february-2013.pdf [Accessed August 10, 2014].

Love, D. (2014). The Nude Celebrity Photo Leak Was Made Possible By Law Enforcement Software That Anyone Can Get. *International Business Times*. [online]. Available from: http://www.ibtimes.com/nude-celebrity-photo-leak-was-made-possible-law-enforcement-software-anyone-can-get-1677314 [Accessed September 11, 2014].

Lucas, H.C. and Spitler, V. K. (1999). Technology Use and Performance: A Field Study of Broker Workstations. *Decision Sciences*, 30(2), pp.291–311.

Marks, E.A. and Lozano, B. (2010). *Executive's Guide to Cloud Computing*. John Wiley and Sons.

McKnight, D.H. and Chervany, N.L. (2001). Trust and Distrust Definitions: One Bite at a Time. In R. Falcone, M. Singh, & Y.-H. Tan, eds. *Trust in Cyber-societies*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 27–54. [online]. Available from: http://link.springer.com/chapter/10.1007/3-540-45547-7_3 [Accessed August 7, 2014].

Montoya, M.M., Massey, A.P. and Khatri, V. (2010). Connecting IT Services Operations to Services Marketing Practices. *Journal of Management Information Systems*, 26(4), pp.65–85.

Osterwalder, D. (2001). Trust Through Evaluation and Certification? *Social Science Computer Review*, 19(1), pp.32–46.

PWC. (2011). The Next Generation of Cloud Computing: How CIOs Can Help their Organizations Prepare for the Business of Tomorrow. [online]. Available from: http://www.pwc.com/en_US/us/increasing-it-effectiveness/assets/next-generation-cloud-computing.pdf [Accessed August 12, 2014].

Rhodes, C. (2014). Business Population Estimates 2013. [online]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/254552/13-92-business-population-estimates-2013-stats-release-4.pdf [Accessed August 11, 2014].

Sakai, H. (2011). Standardization Activities for Cloud Computing. *NTT Technical Review*, 9(6), pp.1–6.

Salesforce.com, Inc. (2014). Success is Built on Trust. *Salesforce.com: Trust*. [online]. Available from: www.trust.salesforce.com [Accessed September 1, 2014].

Saripalli, P. and Pingali, G. (2011). MADMAC: Multiple Attribute Decision Methodology for Adoption of Clouds. In *2011 IEEE International Conference on Cloud Computing (CLOUD)*. 2011 IEEE International Conference on Cloud Computing (CLOUD). pp. 316–323.

Stone, J. (2014). 5 Million Gmail Usernames, Passwords Hacked and Posted To Russian Bitcoin Forum: Report. *International Business Times*. [online]. Available from: http://www.ibtimes.com/5-million-gmail-usernames-passwords-hacked-posted-russian-bitcoin-forum-report-1684368 [Accessed September 11, 2014].

Sunyaev, A. and Schneider, S. (2013). Viewpoint: Cloud Services Certification. *Communications of the Acm*, 56(2), pp.33–36.

Tan, M. and Lin, T. (2012). Exploring Organizational Adoption of Cloud Computing in Singapore. In 19th ITS Biennial Conference 2012. Bangkok: Econstor. [online]. Available from: http://hdl.handle.net/10419/72509.

Young, Lord. (2013). *Growing Your Business: A Report on Growing Micro Businesses.* London: Department for Business, Innovation & Skills. [online]. Available from: https://www.gov.uk/government/publications/growing-your-business-a-report-on-growing-micro-businesses [Accessed August 22, 2014].

Zbuchea, A. (2009). Relationship Marketing - The New Marketing Approach. In *Business Excellence*. 4th International Conference on Business Excellence. Romania: INFOMARKET publishing house.

Paper 8: Pyeong Chang Winter Olympic and Paralympic Games 2018: Cyber risk and mitigation.

Oliver Hoare

Introduction

This paper discusses the potential risks, and mitigations, against cyber attack and information risk to the South Korean 2018 Pyeong Chang Winter Olympic and Paralympic Games. It draws heavily on experience from the London 2012 Olympic and Paralympic Games, as well as previous Olympics. The paper considers recent developments in cyber global threat trends, including geo-political and technical developments, including the activities relating to Islamist terrorism and the wider middle east conflict, but moreover, the actions of state actors, such as North Korea, China and Russia, and the use of so call Advanced Persistent Threat (APT) methods. Equally of interests to Olympic organisers should be the considerations of criminal and hacktivist groups, but above all is the blurring of these threat actors, and threat groupings, with tacit and covert state sponsored support and the proliferation of APT style tactics.

The Olympic movement promotes international peace and mutual understanding, but sadly the Olympic Games has long been associated with protest and terrorism, perhaps most starkly demonstrated by the terrorist attack in 1972 at the Munich Games by the Palestinian militant group, Black September. Sporting events have long been used as a platform for political protest and violent acts; 1996 Atlanta Olympic bombing (protest against abortion); 2008 Beijing pre-Olympics unrest (Islamic separatists); 2009 Sri Lankan cricket team gunned down in Pakistan (Lashkar-e-Jhangvi militants); and most recently the 2013 Boston marathon bombing (Islamist extremism). Such violent events, particularly considering the wider context of international political violence and the steady spread of Islamist terror, as most recently represented by the shocking terror attacks in Paris (January 2015), are highly likely to continue in the future. Therefore sporting events will need to be policed judiciously, and increasingly this includes consideration of cyber security.

Of course the Beijing 2008, London 2012 and Sochi 2014 Games were successfully staged without any major security disruptions, although the financial cost was very high, and also consistently underestimated – the final security budgets for Beijing was US$3bn and London was US$1bn. Sochi's security budget is not so easy to define, but as the most expensive Olympics ever staged (including Summer Olympic Games), at an estimated US$51bn, it is certain that the tight security lockdown in Sochi, due to troubles in the Caucasus, eclipsed both London and Beijing's security budgets combined. But what of the digital threats to the Games, what are the likely trends for the future?

Both London and Beijing experienced cyber attacks – it has been widely reported that Beijing recorded some 12 billion security 'events', whilst London logged 2.35 billion security system messages. Such numbers need to be viewed with some caution however, there are no agreed metrics or benchmarking here, moreover, cyber 'security events', are likely to include systematic and repeated blocks of attacks at the firewall, or even routine user password changes. London did however experience two significant denial of service attacks against the Olympic website on the day of the opening ceremony (successfully blocking some 200mn malicious connection requests, one at 11,000 requests per second). On the same day, London simultaneously witnessed a suspected 'lone-wolf' cyber threat to the power infrastructure

supporting the Olympic park, which sparked a full national security COBR response (COBR being the UK highest authority for national crisis), and pre-tested procedures were enacted, although in retrospect the emergency was considered a non-credible threat. There were also some serious attacks against digital broadcast systems, all of which were successfully dealt with. In the run up to and during the London Games, DDoS attacks were seen against numerous 'establishment' type targets and Olympic sponsors were also targeted. The Government's 24 hr multi-agency (with private sector assistance) Olympic Co-ordination Centre Team (OCCT) raised some fifty actionable response 'tickets', aka cyber events which required some level of intervention and response. London saw spoof websites for fake 'Olympic' merchandise, tickets, accommodation and travel, but again the response was robust; under Operation PODIUM the Police took down numerous websites and made over one hundred arrests for online crime. In addition to the online threat, cable/fiber and high-value component theft had the potential to cause disproportionate disruption to networks, but good resilience measures were taken, particularly regarding critical Olympic systems.

London received significant intelligence prior to the Games to suggest that it would be targeted by Hacktivist groups, such as Anonymous and Lulzsec - for example would-be cyber attackers were encouraged to join Anonymous' "Operation #TheDDOSOlympics". Similarly, the Sochi games saw the establishment of 'Anoymous Caucasus', a group who claimed "the Sochi games infrastructure was built on the graves of 1 million innocent Caucasians who were murdered by the Russians in 1864". Prior to Sochi the US government's Computer Emergency Response Team, US-CERT, issued a notice warning of high levels of cyber criminality, as well as suggesting that those physically attending the games "will likely have their communications monitored".

Of the twenty-three strategic cyber risks identified by the London 2012 Olympic Strategic Safety and Security Risk Assessment (OSSSRA) and Strategic Risk Assessment (SRA), twelve were realized, all were dealt with, and critically, no *un*identified risks were realized.

In regard to 'cyber-terrorism' London assessed at the time that it was of low probability due to lack of capability by credible threat actors, and moreover, due to the absence of 'threat-to-life' systems. There was however considerable concern that a cyber attack might precede, facilitate or in some way support a terrorist attack - for example digital reconnaissance, or a breach of the security or accreditation pass systems to launch an actual physical attack. As a result considerable Information Assurance (IA) activities were undertaken, including a specific government programme to protect the Critical Olympics Supporting Infrastructure, known as the COSI programme.

Of course each Olympics must be seen within the context of international politics and tensions of the time, particularly during the proceeding months to the games, including the torch-relay, and during the events itself), but also from the perspective of the nation's own threat profile, including its global political/military posture, regional influence and local geo-political controversies and issues. In addition, within the cyber realm, technological advances and vulnerabilities also need to be considered, although motivation for attack should have primacy of consideration. So what are the threats against South Korea? And moreover what are the global Cyber threats trends, both politically and technologically? Before considering this it should be noted that the Winter Games, in comparison to the Summer Games, is considered a lower profile event. That said, it may be then seen as a softer target, and therefore more attractive to would be attackers - as a rule terrorists tend to shy away from hardened and well-defended targets. However, from a cyber perspective this matters less, as

cyber attacks can generally take place with little fear of reprisal. Moreover, cyber threat actors can continue to persistently probe and research for vulnerabilities until they are found, if they are determined enough. Key to these considerations of risk, and ultimately in order to develop an effective and proportionate cyber protection programme, is good planning and intelligence.

South Korea is a modern highly successful western-style nation, which historically has been supported heavily by the United States, militarily, economically and politically, this in itself would make Korea a target for a number of middle eastern terror groups. In addition Korea committed troops to Iraq in 1991 and 2003, and more recently has supported sanctions against Iran. Moreover, Korea has of course been subject to numerous cyber attacks over recent years, and it noisy neighbour in the north, is more than likely to be the source of many of such attacks – although methods may well be shared across Chinese and Russia threat groups. Below is a brief survey of the major attacks on South Korea, (with special thanks to Professor Heung Youl Youm (2015) of Soonchunhyang University for much of this detail).

- July 7, 2009, The first large-scale DDoS attack; 36 websites in Korea and the USA were targeted, including the Korea Blue House and USA White House.
- March 4, 2011, Second largest DDoS attack 40 websites in Korea, again the Blue House, governmental ministries, financial organizations, and ICT services.
- July 26, 2011, major portal breached 35 million online users leaked, including names, phone numbers, email, resident registration numbers and passwords.
- November 26, 2011, personal information leakage of game site with 13.2 million subscribers, including passwords, resident registration number. It is very likely the malicious code emanated from the North.
- July 16, 2012, Major cellular operator breached, personal data of 8.73 million subscribers leaked.
- March 29, 2013 So called "DarkSeoul" A major APT style attack targeting economic and critical national infrastructure, including breaching three major banks and three broadcasting companies (KBS, MBC, YTN). Use of Trojan Horse malware to destruct the master boot record and use of Patch Management Systems (PMS) to then disseminate malicious code laterally.
- March 6, 2014, Network operator's website breach loss of 9.81 million pieces of personal data leaked between August 2013 and February 2014. Insider arrested and company fined by Korean authorities.
- December 2014 an attack on non-critical elements of Korea Hydro and Nuclear Power Company (KHNP). Note: this was an attack against the administrative, rather than operational network, but many argue that the jump between two such systems, if connected, is entirely possible.

It is interesting to note the diversity and progression of attack techniques and targets, particularly the "DarkSeoul" event, which was a typical APT style of attack (e.g., sophisticated, targeted and persistent, and targeted against national infrastructures and social fabric). The widely publicized Sony Corporation hack, considered as retribution for Sony's film comedy, 'The Interview', based on the assassination of North Korean leader, Kim Jong Un, whilst is not a South Korean target, but rather a Japanese/US target, used similar APT tactics. This attack has been squarely laid at the feet of the North Korean state by the US administration, and has provoked an unprecedented response by the US, both politically and technically, with new sanctions enforced on North Korea and Internet blackout occurrences,

although the latter is not formally acknowledged by the US. Interestingly, the Sony attack was committed under the guise of a 'hacktivists' or criminal gang, the so called "Guardians of Peace", which is either a direct cover for, or at the very least is a group sanctioned by, the North Korean State.

Mandiant/FireEye, widely recognised as one the most experienced and advanced cyber-security firm, has recently published its global trends annual report, "M-Trends". This report shows the recent proliferation of APT style tactics and the blurring of criminal and nation state threat groups. Mandiant's (2014b and 2014c) previous and widely renowned reports on Chinese (APT1) and Russian (APT28) cyber threat groups, provide clear evidence of state involvement in large industrial scale espionage operations and support for quasi-criminal groups.

> 'Our investigations over the past year have confirmed an emerging trend: ***cyber criminals are stealing a page from the playbook of APT actors, while APT actors are using tools widely deployed by cyber criminals***. As these actors' tactics merge, discerning their goals becomes critical to gauging the impact of incidents and building a risk-informed security strategy.'

Source: Mandiant/Fireeye, *M-Trends* (January, 2015)

> 'There may be ***overlaps between groups caused by the sharing of malware or exploits they have authored, or even the sharing of personnel***. Individual threat actors may move between groups either temporarily or permanently. A threat actor may also be a private citizen who is hired by multiple groups. Multiple groups, on occasion, compromise the same target within the same timeframe.'

Source: Mandiant/FireEye, *APT 28* (December, 2014c)

(Author's bold italics).

Another worrying trend is the rise of middle-eastern cyber groups such as the Syrian Electronic Army (SEA), who support the repressive Assad regime. Since at least 2011 SEA has been conducting cyber attacks, including DDoS, phishing email attacks and even more sophisticated methods by compromising service providers. SEA have successfully attacked externally facing websites and hacked social media accounts of at least forty organisations, with a specific focus on western news agencies. Attacks included the Washington Post, New York Times, Linked-in, Forbes, BBC, Skype and many others. Most notoriously in April 2013 SEA hacked Associated Press, accessed their Twitter account where they falsely claimed the White House had been bombed and President Barack Obama had been injured. This led to a US$136.5 billion dip on the S&P 500 index.

Similarly, in recent years Iranian based cyber threat groups have surfaced, although the focus of their attacks seems to be critical national infrastructure. An Iran sponsored group is widely believed to behind the August 2012 attacks against oil and gas companies, Saudi Aramco and Qatari RasGas, rendering at least 30,000 computers useless. This was considered as a direct response to the Stuxnet virus, which succeeded in stalling the Iranian nuclear enrichment programme, and is commonly thought to be the work of the US and Israeli governments.

With the rise in middle eastern cyber groups it does not take a great leap of imagination to foresee some form of cyber-assisted terror attack, or even a direct cyber-terror attack, particularly, as sophisticated nation's critical infrastructure, and day-to-day operations, are more and more reliant on networked IP based technology, as well as the public's appetite for a plethora of digitally enabled devices - the so called Internet of Things (IoT).

In comparison to other forms of terror attack, cyber-attacks can be low cost, provide relative anonymity and immunity from prosecution, can be conducted globally from a local base, which can be easily dispersed and reassembled elsewhere, and can have a disproportionate impact on digitally sophisticated societies. Moreover, cyber reprisals, against less digitally matured states and non-state threat actors generally have a negligent effect, and as suggested it is quick and easy for the attackers to set up again from a new location. In short cyber attacks offers an asymmetric strategy for disaffected groups of all types. It is perhaps worthy of note that "Jihadi John" the ISIS executioner of numerous hostages, including most recently Japan's Haruan Yukawa and Kenji Goto Jogo, has been named as Mohammed Emwazi, a computer science graduate who went on to be a computer programmer. How likely then is cyber, or cyber-assisted, terror attacks likely to be in the future?

Conclusions

So what are the real risks to the Pyeong Chang Olympics and how can it be protected? The Olympics is often seen as an opportunity to show case a nation's offerings, South Korea is clearly a tech driven digital based economy, arguably its best known global company is Samsung, the communications giant and seemingly the only real rival to Apple's global dominance. Korea like so many developed nations is becoming increasingly reliant on underlying technology to run the country and its critical national infrastructure, as well as the economy. However, the Olympics is as much about reputational risk, and therefore certain aspects and systems become critical to protect. For example Olympic specific systems such as timing and scoring, ticketing, accreditation/pass and security systems need to be protected, but also health and safety systems need to be robust (if compromised a venue or even the Olympic Park maybe deemed not safe for the public and deemed out of action). Then there are critical supporting infrastructure networks, power, transport, water, utilities etc., and perhaps above all from a reputational viewpoint, is broadcasting. The increasing move to digital and online mediums renders broadcast increasingly vulnerable to cyber attacks – losing broadcast during an Olympics will result in serious reputational damage, lose of revenues, fines and likely legal proceedings. Similarly, Olympic sponsors will require protection and can be seen as a very likely reputational target. The 'insider threat' can be a critical component to a cyber attack, as Korea experienced with the 6 March 2014 attack (see above), therefore personnel security, as well as physical security measures should not be forgotten. Cyber-crime and cyber enabled fraud against the games should be taken as a given – a quick two-minute domain name search came up with the following domain names: 2018Pyeongchang, Ticketspyeongchang, 2018olympictickets, 2018pyeongchangtickets, olympictickets2018, winterolympics2018. Of course the official website domain name is Pyeongchang2018, so what is the likely use of these other domains?

A cyber-security strategy is required, this needs to be proportional and well informed; the key to protecting the Games, is understanding the risks, which requires a sound methodology, evidence, and intelligence. Moreover, employment of the private sector and specialists is critical, as well as good governance, processes, clear responsibility, leadership and due diligence. And perhaps above all is to have a well devised testing and exercising programme.

Recommendations

The South Korea government should consider developing the following:

Recommendation 1: A cyber security programme for the protection of the Winter Olympic Games: including: commissioning a cyber security risk assessment – with a view to developing a proportionate and robust mitigation and cyber-security action plan.

Recommendation 2: A Cyber strategic risk assessment should be seen within the context of an overall security risk assessment.

Recommendation 3: Create an intelligence led model and machinery, leveraging existing capability and developing new intelligence where required.

Recommendation 4: Governance structures – with a central government lead with access to highest authorities and senior ministers, this should include a multi-agency and private sector partnership approach.

Recommendation 5: Appointment of an Olympic Information/Cyber Risk Owner.

Recommendation 6: Multi-agency Olympic CERT/SOC.

Recommendation 7: Consider the appointment of a strategic cyber adviser from the private sector.

Recommendation 8: Gain international support early – to source intelligence, expertise and CERT support.

Recommendation 9: Develop a cyber testing and exercise programme.

Recommendation 10: Ensure that cyber learning and legacy benefits are realized to build on national cyber capability.

Bibliography

BBC News Website (2013). "*The 'cyber-attack' threat to London's Olympic ceremony".* BBC News Website, Gordon Corera, Security Correspondent (July).
www.bbc.co.uk/news/uk-23195283

CyberSecurity Ventures. (2015). *CyberSecurity 500 (top 500 global cyber security firms),* (February).
http://cybersecurityventures.com/cybersecurity-500/

Hoare, O. (2014). *London 2012: Cyber Security, Sharing our Experiences.* Presentation to Japanese Information-Technology Promotion Agency (IPA) (January).
www.ipa.go.jp/files/000039004.pdf
http://www.ipa.go.jp/files/000037535.pdf

Levkowitz, A. (2013). *South Korea's Middle East Policy.* (December). The Begin-Sadat Center for Strategic Studies, Bar-Ilan University.

Mandiant/FireEye. (2014a). *M-Trends 2014: Beyond the Breach.* (January). Mandiant/FireEye Annual Trend Report.

Mandiant/FireEye. (2014b). *APT1: Exposing One of China's Cyber Espionage Units*, Mandiant Intelligence Center Report.

Mandiant/FireEye. (2014c) *APT28: A Window into Russia's Espionage Operations*, Mandiant Intelligence Center Report. (December).

Mandiant/FireEye. (2015). *M-Trends 2015: A View from the Front Lines. (*January). Mandiant/FireEye Annual Trend Report.

The Institute of Engineering and Technology. (2011). *Delivering London 2012: ICT Enabling the Games.* The Institute of Engineering and Technology.

The Institute of Engineering and Technology. (2013). *Delivering London 2012 (Part 2): ICT implementation and operations.* The Institute of Engineering and Technology.

Trim, P.R.J. T., and Youm, H.Y. (Eds.)(2014). *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership*. *Report submitted to the Korean and UK governments*, British Embassy Seoul (March).

Youm, H.Y. (2015). *Recent Korean Security Policies for the Financial Sector.* Presentation by Professor Youm at the 4th Korea-UK Cyber Security Research Workshop, Department of Business, Innovation & Skills, London (23rd February).

Paper 9: Cyber security in supply chains

Emma Philpott

There is a growing awareness of the importance of Cyber Security in supply chains. Large organisations are increasingly being targeted through the smaller and more vulnerable companies in their supply chain. This can be seen in high profile attacks such as the Target breach in late 2013 as well as many more which are not publicised.

Encouraging small companies to adopt secure information assurance and technical controls is difficult. This is partly due to the perceived complexity and cost of the subject. However, it has been seen that significant improvements in security can be gained by implementing simple, low cost processes and controls.

If a company spends the time and resources to adopt secure working practices and good technical controls, they need a recognised certification and badge to show this and give them a competitive advantage over the companies who have not done this. As long as the standard is suitable for small companies to achieve at reasonable cost and effort, the supply chain contracts can reasonably request that a company be certified to this before a contract is granted.

Benefits to supply chain

Such a scheme benefits the supply chain by raising the level of cyber security beyond a recognised minimum. It also takes away the necessity for every company to develop and assess their own cyber security questionnaire/requirements.

Benefits to small companies

The scheme benefits the small companies because, once they have achieved certification to this recognised standard, they will meet the requirements of a number of supply chains without needing to complete additional questionnaires and audits every time they apply for a tender with a new customer. They can also use the badge to gain competitive advantage, especially as awareness of the importance of cyber security grows.

IASME standard

The IASME standard allows the companies in a supply chain to demonstrate their level of cyber security and indicates that they have taken steps to properly protect their customers information. Available either as a self assessment or assessment by an independent auditor, IASME is a realistic and affordable way for all companies to prove that they are following best practice.

Benefits of IASME

Due to the complexity of most cyber security standards, the majority of companies do nothing and have minimal protection. This means that the data they hold, including Intellectual property, personal and commercial information is wide open to international theft.

The number of cyber attacks are increasing and currently 80% are defeated by simple technical and governance controls. It is also increasingly common for larger companies to be attacked through targeting the smaller companies in the supply chain. By implementing the IASME standard through a supply chain, the security of that company's data is increased significantly.

Background to IASME

The IASME standard was developed over several years during a UK Government funded project to create an achievable cyber security standard for small companies. The standard, based on international best practice, is risk-based and includes aspects such as physical security, staff awareness, and data backup. The IASME standard was recently recognised as the best cyber security standard for small companies by the UK Government when in consultation with trade associations and industry groups. The audited IASME certification is also accepted as showing compliance to ISO27001 by an increasing number of companies, including HP.

The international standard, ISO27001

The international standard, ISO27001, is comprehensive but extremely challenging for a small or medium sized company to achieve and maintain.

Cyber Essentials Scheme

The Cyber Essentials Scheme focuses on the five most important technical security controls. It was developed by the UK government with the IASME Consortium after examining the recent successful cyber attacks. If these controls were in place in all companies then 80% of those recent cyber attacks would not have been successful. The Cyber Essentials requirements are already embedded in the IASME standard. If the UK Government expands the Cyber Essentials scheme to other countries, the countries which implement the IASME standard will already be set up to administer the Cyber Essentials certification with little, if any, need for new practices.

Proposal to rollout IASME in Korea

We propose to roll out IASME, in partnership with any similar standard already in place within Korea.

Development Phase

The IASME team will work with local expert organisations to develop a bespoke version of IASME for Korea. This will involve changing aspects of the standard to reflect local laws and practices and any other specific requirements of the region. During this phase the team can work in partnership with local organisations expert in information assurance standards and also align with any standard already used in this sector.

Training Phase

Once the bespoke version of IASME has been agreed, the IASME team will work with local experts to select a number of cyber security organisations to become the first Korean IASME

Certification Bodies. IASME will then work with these organisations to train their staff to be IASME assessors or to be able to offer consultation to organisations that need help to work towards the IASME standard.

The IASME team will also assess and certify these pathfinder organisations to the standard themselves which is a prerequisite to becoming a Certification Body. Once trained and certified, the Korean Certification Bodies will start assessing local organisations. The IASME team will initially support them in this until they become confident.

Deployment Phase

Korea will have a growing stable of local, high quality, proficient organisations able to certify companies to the IASME standard. If the UK Government chooses to expand the Cyber Essentials Scheme to other countries, Korea will be ideally placed with pre-trained Certification Bodies to roll out the scheme immediately. Equally, even though the Cyber Essentials certification cannot be issued initially, the companies will be assessed to the same level because the Cyber Essentials requirements are embedded within the IASME requirements.

Longer term advantages

As the awareness of IASME certification as being a realistic and understandable certification for small companies spreads, the level of cyber security awareness and protection will increase within the general population and supply chains.

The technical controls of Cyber Essentials within the IASME certification will, alone, prevent a significant number of cyber attacks. The governance requirements in the rest of IASME will ensure those aspects are sustainable.

Paper 10: Korea-UK collaboration: Strategic drivers, collaborative capabilities and pan-industry requirements

Patrick Curry

Every organisation, nationally and internationally, faces increasing internal and external cyber threats to their information, their ability to operate and to citizens, consumers and employees. In an increasingly connected but distributed world, organisations have to collaborate to thrive; they also have to collaborate to address shared risks and ensure their mutual defence. Cybercrime and identity fraud are increasing. Isolated organisations are becoming particularly vulnerable.

Both Korea and the UK have requirements to share cybersecurity information between each other and as part of various international communities, to ensure their national digital capabilities (industry, government and societal) can develop and provide benefit without threat. However, the global ability to share sensitive information under control within and across different communities is in its infancy. Organisations in Korea and the UK are active and at the forefront of the development of international standards, business cases and implementation. Discussions have highlighted much common thinking and also opportunities for synergy and collaboration.

The UK and Korea are well positioned to work together and with allies (particularly the USA and the EU) and major industry partners to be at the forefront of developments in collaborative cybersecurity, and to promote interoperability.
To understand the opportunities afforded by Korea-UK collaboration requires a wider understanding of:

- The strategic drivers and developments in internet governance, cyber assurance, collaborative cyber situational awareness (CCSA) and identity management;
- The collaborative capabilities within Korea and UK government and wider industry;
- The requirements of industry sectors, governments and international organisations, which have the need and are already creating early adoption.

Strategic drivers and developments

As use of the internet grows with more devices, more services, more applications and more people will avail themselves of the products and services on offer. So the 'attack surface' is increasing. Unfortunately, most parts of society are so focused on immediate benefits that they remain unaware of the opportunities this creates for fraud, cybercrime and industrial espionage for example. Identity fraud remains the top international enabler for crime, according to Europol and US agencies; damaging nations, business and human lives. Governments are responding with increasing regulation, particularly the USA, creating legal instruments, standards and technology that, at the same time, set the bar for other nations and also drive the development of technologies and the markets.

It can be argued that 9/11 was the compelling event. The inability of organisations to collaborate with each other and trust each other, in the real and cyber worlds, was worse than anyone had anticipated. It resulted in several Presidential Directives, including HSPD 12 to standardise identity management across all Federal organisations. The resulting standards, including FIPS 201, SP800-63 and Personal Identity Verification – Interoperability (PIV-I)

created technologies and a market that has extended internationally and also fed into the creation of ISO, ITU-T and IETF international standards. These, particularly the ISO 27000 series (Information Security Management Systems) and ISO 29115 (Entity Authentication Assurance Framework), have been embraced in industry sectors, particularly aerospace, defence and pharmaceuticals, as well as some governments, police, military and air traffic management. Unfortunately, the international awareness of these capabilities and the speed of their development is not geographically consistent. International organisations are unable to keep pace with differing developments in the developed and developing worlds. Consequently, international collaborative organisations like MACCSA are being created to track international developments and enable the implementation of collaborative mechanisms for Collaborative Cyber Situational Awareness (CCSA).

Amongst the several national and international activities, four major strategic activities stand out:

- The US Cybersecurity Framework mandated by Presidential Executive Order 13636. The Framework is supported by several major standards, particularly SP800-53. The US Government has announced a number of Executive Orders regarding cybersecurity, identity management and information sharing, which are forcing implementation and also creating cybersecurity developments in technology, supply chain behaviours and executive accountability in organisations.
- The EU Cybersecurity Framework, which is supported by new laws and regulations for identity management, incident notification, information sharing, cloud computing and organisational responsibilities. The EU is coordinating with NATO to enable interoperability and re-use for member states.
- The development of new US Federal Acquisition Regulations (FAR) for cyber assurance across supply chains, based upon the US Cybersecurity Framework for example.
- EU Project MAPPING, which is to provide guidance to the Council of Europe on internet governance, privacy and protection of intellectual property. MAPPING is also to consider whether a new international treaty is needed for the Internet and to recommend model law.
    - MAPPING links to other projects ranging from smart surveillance to consent mechanisms. MAPPING is coordinating with US on its FAR developments and also with other nations outside the EU.
    - MAPPING is gradually forming an initial view that the Internet will evolve to have a series of trusted overlays on the Internet; these overlays provide the trust mechanisms that any community needs to be able to operate, and they require identity or partial anonymity as defined in ISO 29191. Anonymity is not permitted in a trusted overlay.
    - Interpol and 11 nations are partners in MAPPING. BBFA is the UK partner.

Collaborative cybersecurity capabilities

MACCSA was created as a result of Multinational Experiment 7 (MNE7), a two year experiment by the military of 15 nations and HQ NATO, with the objective, "to ensure access to the global commons of sea, space and cyberspace". UK and Korea MODs participated. UK MOD led the cyberspace activities and they brought in a UK expert, who edited the Information Sharing Framework (ISF) for Collaborative Cyber Situational Awareness (CCSA). At the end of MNE7 in December 2012, the national leaders decided that the ISF should be implemented and tasked the UK MOD to run transition workshops to involve the

non-military government, industry and international organisations and to make information sharing real. Absent were any agreed suitable organisation, it was decided to create a new neutral organisation to take this forward – MACCSA was formed as a UK company, in a meeting in Incheon in Oct 2013. MACCSA is slowly expanding its activities and relationships with other communities, particularly in North America, Europe and Asia.

MACCSA's Information Sharing Framework requires participants:

- To have an approach of collaborative risk management, including dynamic risk, for risk identification, assessment and treatment (by mitigation, transfer or acceptance).
- To have a risk mitigation strategy based on a cyber controls framework and Levels of Assurance e.g. ISO 27002+, US SP800-53, DE BSI 100, EE ISKE or ES Magerit. Participants in a community can use the framework to define Normality across the community – this ensures consistent mutual defence and, most importantly, a consistent detection of Abnormalities.
- To have a time-based security approach. Protection must provide time for detection and response. $t_{protect} > t_{detect} + t_{respond}$.
- To operate five major functions, which reflect the leading cybersecurity frameworks, including USA:
    - Identify. The identification of enterprise and collaborative risks.
    - Protect. Protection control measures to mitigate risks. This includes dynamic vulnerability management and threat detection.
    - Detect. Monitoring and detection capabilities inside and outside the organisation to detect abnormalities and security events.
    - Respond.
        - To contain and defeat the attack or incident, and;
        - to ensure the continued operation of core business functions.
    - Recover. To restore Normality – normal operation and behaviours.
- To be capable of incident management and information management.
- To be trustworthy and capable of Level of Assurance 3 (High) or 4 (Very High) PKI federation in accordance with ISO 29115 and agreed Common Policies. <u>This provides the basis for trust, which facilitates information sharing</u>.
- To use an appropriate standards-based taxonomy and protocol for sharing threat intelligence and incident information. STIX/TAXII and IODEF/RID are two common examples.

MACCSA recognises that industries and government organisations in the UK and Korea each have capabilities and best practices that, by cooperation, could create greater and faster benefit for the UK and Korea, other nations and international industries. At the workshop in Korea , MACCSA proposed six major activities for further collaborative exploration and development by the UK and Korea. These areas are already happening, driven by international developments and requirements, so the UK and Korea will have to move with momentum and agility, if it is to deliver tangible benefits. If not, a new UK/Korea arrangement should be considered.

The six major activities are:

1. Development of PKI Federation for collaborative identity management, based on existing international and national capabilities, and the latest developments.
    a. The central part of this federation activity would be cross-certification between:

i. The Public Korea PKI Root Certificate Authority (CA) operated by KISA, with its five government-approved credential issuing CAs.
ii. The UK PKI Bridge Root CA operated by BBFA, with at least five compliant issuing CAs. (BBFA – British Business Federation Authority)

b. KISA provided a presentation "The Status of the Korean PKI", which includes an overview, PKI policy, PKI business models, certificate promotion and future work.

Next steps. KISA and BBFA agreed to work together to:

i. Conduct an initial comparison of relevant Certificate Policy documents.
ii. Assess the technical feasibility; and,
iii. identify communities of stakeholders who wish to participate.

2. Participate in one or more CSSA pilots for information sharing, or develop a new one. Options could include Korean industry and government participation in the UK's Cybersecurity Information Sharing Partnership (CISP) (based on XMPP), the Financial Services Intelligence Sharing Analysis Centre (FS-ISAC) and other emerging industry-specific capabilities. Any pilot should be based on the ISF for CCSA, e.g., they could include federated access control, redaction and partial-anonymisation mechanisms for source protection, STIX/TAXII or IODEF/RID with security automation.

   Next steps. To develop a plan of collaboration at the meetings of 23rd to 24th February, 2015 in London (BIS Conference Centre and Birkbeck, University of London).

3. Re-use of KISA best practice capabilities for protecting citizens and organisations. Although the UK government has no plans for such capabilities, there is interest in industry to provide such capabilities within a collaborative governance model. The four of interest are:
   a. The Cyber Curing System (described in the Forum meeting in March 2014).
   b. The DNS Sinkhole (ditto).
   c. The DDoS Shelter System (ditto).
   d. The Information Security Readiness Scheme, ISMS, PIMS and PIPL.

   Next steps. To develop a plan at the next meeting (23rd to 24th February, 2015 in London (BIS Conference Centre and Birkbeck, University of London)).

4. ROK involvement in international developments in Internet governance, particularly:
   a. EU Project MAPPING and Cybersecurity Strategy activities. These activities are coordinated with UN and NATO.
   b. US Cyber Assurance across supply chains.

   Next steps. For BBFA to arrange an invitation for Korean participation in the EU MAPPING & US Legal/Technical Workshop taking place in the Delegation of the EU Commission in Washington DC, on 23-25 March, 2015.

5. Trusted Cloud. As organisations face increasing threats and regulatory requirements to protect their own and shared information, many large organisations have the resources and capabilities to operate their own cloud services securely. However, Small and Medium Enterprises (SMEs) do not. SMEs, particularly in large supply chains, seek trusted cloud services to protect their information and ensure regulatory

compliance. But no agreed standards and assurance schemes exist to define trusted cloud. Cloud providers are beginning to work together to develop practical capabilities that will meet the US FEDRAMP, US SP 800-53, EU Code of Conduct for Cloud Providers, and leverage emerging standards. Korean involvement would be welcomed to assist in development, requirements input and encouraging adoption.
Next steps. To discuss at the next meeting, with one or more cloud providers.

6. Age verification. There are many national and international requirements for age verification (young and old), based on the use of attribute-based credentials (ABC). The Korean National Body (Prof Youm) in ISO JTC1 SC27 is leading a Study Period on Age Verification that will report at the next SC27 meeting in Kuching, Malaysia in May 2015. This should lead to the creation of a new ISO International Standard. BBFA provides a co-rapporteur for the Study Period. It is also co-authoring briefing material on Age Verification for UK Members of Parliament after the election in May 2015, and it is working with:
    a. Industries to develop a practical approach to age verification in the UK.
    b. EU MAPPING and Interpol to develop an approach to address age verification where service providers are non-compliant e.g. on the TOR network.

    Next steps. To discuss at the next meeting.

Pan-Industry international requirements

7. Engaging industry. All industry sectors are increasingly at risk and looking for mitigating solutions that are interoperable, reusable, agile and affordable. The EU defines 23 industry sectors. Some sectors are much further ahead than others:
    a. leading sectors include: aerospace, defence, energy and banking;
    b. sectors that need to improve and to collaborate include telecommunications, IT manufacturers, information service providers, pharmaceuticals, food, transport, shipping & maritime, health, construction, retail, counter-fraud, law enforcement, child online protection.

    Next steps:
    a. To develop a plan at the next meeting.
    b. To identify stakeholder industry communities for early engagement and to be champions for others to follow.
    c. To assist/work with leading bodies in the maritime industry that are responding to the International Maritime Organisation requirements for maritime cybersecurity and the development of an approach to be discussed at Maritime Safety Committee (MSC) 95 in London in June 2015. MACCSA is already engaged. It will find out the names of the Korean representatives and pass them to Korean colleagues in this Forum.

8. Organisational Identification.
    a. Other matters were discussed during the visit, notably the situation in Korea on the identification of all types of organisations that do business on the internet. All entities in cyberspace bind to an organisation. Fake organisations are a global challenge.
    b. Internationally, a new kind of organisational register is required that meets the requirements of cyberspace for the identification of organisations, their trustworthiness (Level of Assurance), the validity of their attributes and all this

to an accuracy of 24 hours or less. The generic ROLO (Register of Legal Organisations) specification is contained in the draft ISO 29003 WD3. The ROLO specification has been taken by 4 nations (including UK and USA) and more nations are interested.

c. ROLO should be the trustworthy near real-time Authoritative Source for an organisation at a given Level of Assurance, accurate to less than 24 hours. ROLO is a real time Authoritative Source for some attributes and a Corroborative Source for others. The Korean business register includes all types of organisations, including charities, and is overseen by the Supreme Court.

Next Steps. If possible, to plan at the next meeting.

9. Communication. An increasing number of Korean and UK organisations are showing an interest in the above work and also in the D5 Group of ROK, UK, Estonia, New Zealand and Israel.
(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386290/D5Charter_signed.pdf).
There is a requirement for communication and coordination.
Next steps. To discuss at the next meeting.

Conclusion

Based on shared interests and views, those attending the workshops in Korea recognised the opportunities for Korean and UK organisations to consider for collaboration and future development. Further planning and discussions at the next meeting in London on 23rd and 24th February, 2015 should develop some of these opportunities into activities that could provide real benefit and enable wider progress, and be resourced accordingly.

Paper 11: Korea-UK Collaboration: Meeting of 24th February, 2015 at Birkbeck, University of London.

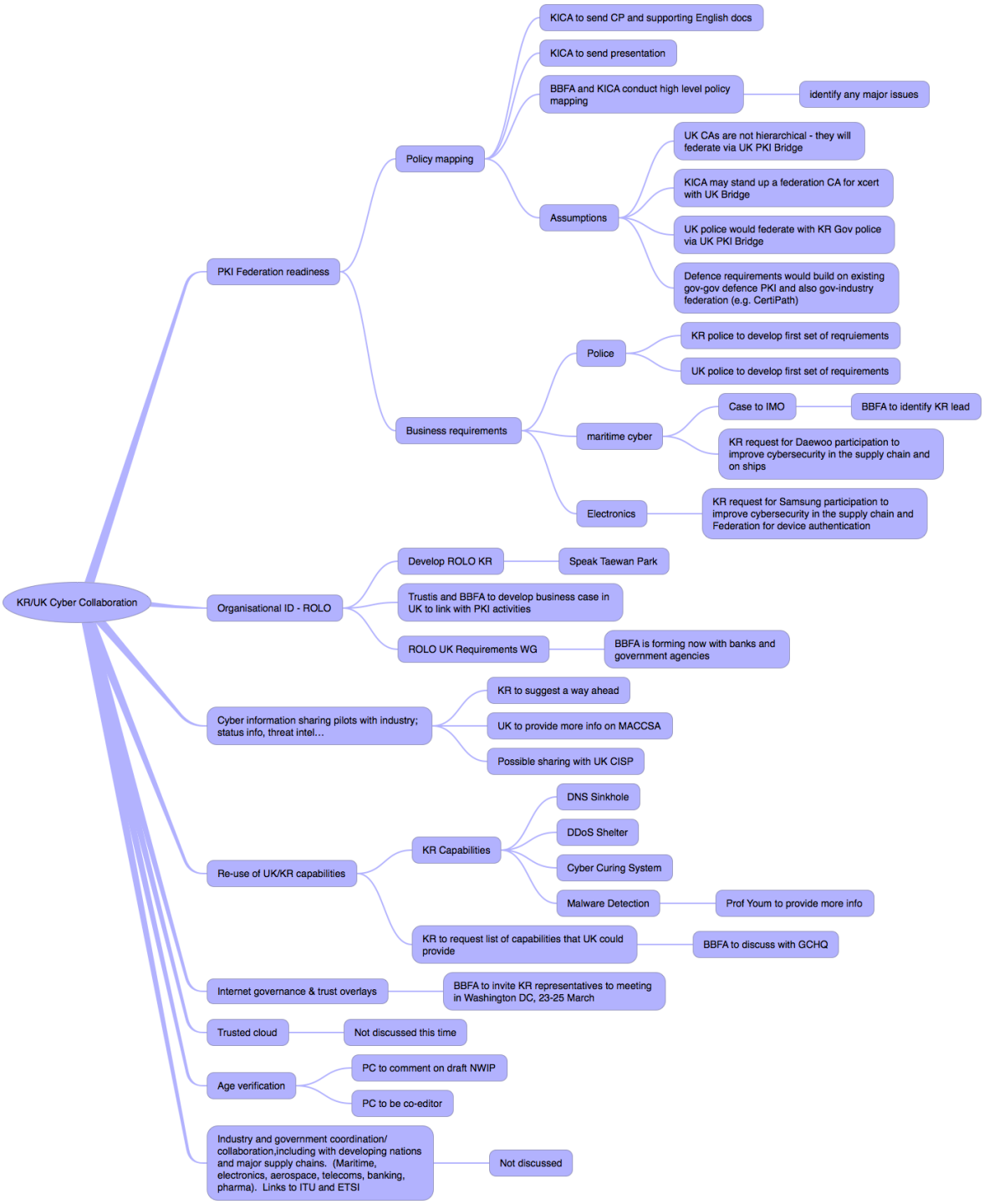
Heung Youl Youm and Patrick Curry.

The points and actions from the meeting are outlined below.

- PKI Federation readiness
    - A way forward was confirmed: policy mapping, analysis of technical elements, and the business requirement.
    - MoU between KICA and BBFA to promote this PKI federation.
    - Policy mapping:
        - KICA to send CP and supporting English documents.
        - KICA to send presentation material.
        - BBFA and KICA to undertake a high level policy mapping:
            - identify the/any major issues.
        - Assumptions
            - UK CAs are not hierarchical - they will federate via UK PKI Bridge.
            - KICA may set up a federation CA for xcert with UK Bridge.
            - UK police would federate with Korean Government and police via UK PKI Bridge.
            - Defence requirements would build on existing government to government defence PKI and also government - industry federation (e.g. CertiPath).
    - Technical elements
        - KISA and BBFA to propose technical elements for federation.
    - Business requirements
        - UK and Korea to identify business needs from their perspective.
        - Police:
            - Korean police to develop first set of requirements (e.g., information sharing for preventing serious cybercrimes, e.g., information about UK sites for cyberattacks).
            - UK police to develop first set of requirements (e.g., information sharing for preventing serious cybercrimes, e.g., information about UK sites for cyberattacks, for the PyeongChang 2018 Olympic Games, online child protection, and counterfeit good protection).
        - Maritime cyber:
            - Case to IMO.
                - BBFA to identify Korean lead.
            - Korean request for relevant Korean industries (e.g., Daewoo) participation to improve cybersecurity in the supply chain and on ships.

        - Electronics:
            - Korean request for relevant Korean industries (e.g., Samsung) participation to improve cybersecurity in the supply chain and federation for device authentication.
- Organisational ID - ROLO
    - Develop ROLO Korea.
        - Speak to Taewan Park to follow up discussion with Supreme Court.
    - Trustis and BBFA to develop business case in the UK to link with PKI activities.
    - ROLO UK Requirements working group.
        - BBFA is discussing this now with banks and government agencies.
- Cyber information sharing - pilots with industry; status information and threat intelligence for example.
    - Korea to suggest a way ahead.
    - UK to provide more info on MACCSA.
    - UK to identify benefits for sharing this knowledge and information.
    - Possible sharing with UK CISP.
- Re-use of UK/Korean capabilities
    - Korean Capabilities:
        - DNS Sinkhole.
        - DDoS Shelter.
        - Cyber Curing System.
        - Malware Detection.
            - Professor Youm to provide more information.
    - UK to identify organizations (e.g., government agencies or GE) who are interested in operating these capabilities for UK citizens).
    - Korea to request list of capabilities that UK could provide.
    - UK to recommend list of capabilities that Korea may use.
        - BBFA to discuss with GCHQ.
- Internet governance and trust overlays
    - BBFA to invite Korean representatives to the meeting in Washington DC, 23-25 March, 2015.
- Trusted cloud
    - Not discussed this time.
- Age verification
    - Patrick Curry to comment on draft NWIP.
    - Patrick Curry to act as co-editor.
- Industry and government coordination/collaboration, including with developing nations and major supply chains. (Maritime, electronics, aerospace, telecommunications, banking, pharmaceutical). Links to ITU and ETSI
    - Not discussed.

The activities outlined are mapped below.



Paper 12: Issues that managers need to consider when undertaking research relating to the cyber environment

Peter Trim and Yang-Im Lee

Introduction

The aim of this paper is to highlight the need for managers in a range of organizations to engage more fully in research relating to the cyber environment and in particular, to help them to undertake research to improve their understanding of what cyber threat intelligence involves. Attention is given to how managers and academic researchers can work together and engage more fully in social science cyber security research.

It is hoped that academics, researchers and managers in a variety of organizations will find this paper of interest as it makes explicit a number of factors that govern partnership arrangements involving supplier organizations, retail organizations and distributors. Furthermore, attention is given to such issues as partnership development in the context of making the organization more robust and better able to put in place policies and procedures relating to counteracting the growing number of cyber threats.

Background

With reference to a cyber risk report featured in Management Today (2014), it is clear that insider crime is an issue and managers are aware of DDos attacks, the work of hackers and the threat posed by viruses and malware. Indeed, one-third of incidents can be attributed to malware that has been designed to steal data and because of this greater attention needs to be given to situational awareness across industrial sectors, cooperation between organizations throughout the public and private sectors, and information sharing across borders (Gibson, 2014). What needs to be remembered is that malware can be in a system for 200 days or more before it is detected (Jopling, 2014). Another key point to note is that there are a large number of tools that can be downloaded and used to commit cyber attacks and in addition, there are a lot of people that have the ability and/or intent to use these tools (Bach, 2014). With regards to rapid change that is shaping the business environment, it is clear that academic researchers need to undertake research that allows them to better explain the complexities that are giving rise to new business models and which require new forms of decision-making to be deployed. When a cyber attack is launched upon an organization, it is likely that the impact will have an effect both upon the organization itself, partner(s) organizations, and various customer groups. If the impact is severe and a major disruption occurs, senior management must ensure that the image and the reputation of the organization and its partner(s) is restored as soon as possible. Hence it is essential that a risk communication strategy is in place. Indeed, ENISA (2011: 3) make clear the fact that an organization's risk management strategy encompasses a communications policy that is embedded within the management of risks approach.

According to Trim and Lee (2014: 80-81), "A risk communication strategy must therefore be grounded in the business continuity management planning framework and if an impact does occur, the recovery process can be as rapid as possible owing to the fact that the procedures are adequately documented and those in charge or associated with the recovery process are competent to ensure that it goes ahead as planned".

Key issues and challenges for managers

The process of internationalization has focused the attention of managers on a range of important activities including environmental scanning; the changing landscape of retailing; and in particular, how retailers formulate and implement strategies (Akehurst and Alexander, 1995; Howe, 1998, p. 215). This brings to the surface a number of issues such as the type of business; the location of the business; how goods are to be selected, distributed, and displayed; and how channel partners are managed (Walters, 1979, p. 215; Lewison and DeLozier, 1986, p. 45 and p.63; Lewison, 1997, p. 8; Morganosky, 1997, p. 269; Martin et al., 1998, p.114; Siguaw et al., 1998, p. 99). The concept of reciprocal relationships vis-à-vis channel partners has received attention (Sparks, 1995), and so too has technology utilization. As regards the latter, managers in the retail sector are becoming increasingly aware of how connectivity and interactivity between organizations is facilitating business relationships and how strategic management intelligence decision-making needs to take into account cyber threat activity. What is important to note, is that the cyber environment in which organizations compete and form cooperative working relationships with other organizations, is undergoing constant and rapid change and forcing managers to think in terms of managing risk and uncertainty more pro-actively than they did in the past. Indeed, the range of threats and the problems associated with inadequate security systems, is forcing managers to think more about putting in place a corporate security system that incorporates counterintelligence. The reason why managers need to give this attention is because employees are increasingly engaging in remote working and as a consequence criminals will have more opportunity to steal sensitive information (Jones, 2014). This is a highly relevant observation bearing in mind that managers are confronted with the challenge of managing the due diligence process in association with third parties and supply chain activities (Jones, 2014). The problem becomes more complex in the sense that a large amount of data that employees handle is no longer stored in the company's data centre and also, it is known that "52 per cent of workers use 3 or more devices daily" (Hardy, 2014). Selman (2014) is clear that a structured cyber security model has a number of advantages and has highlighted risk assessment, supplier profiling, supplier assurance and compliance, and this can be considered widely and placed in the context of a partnership arrangement involving companies from both the private and public sectors. One way forward is for senior management to engage more deeply in threat intelligence and this means that managers need to collect and analyse data and information from a number of different sources, and to formulate policy to deal with these threats (Samtani, 2014). This can be facilitated by placing data/information in an active cyber defence cycle (incident response, threat and environment manipulation, threat intelligence consumption, and asset identification and network security monitoring) (Samtani, 2014). What managers need to be aware of is that "individual threats have multiple vectors" and because of this they need to formalize the process of identifying threats and classifying threats, so that all the points of attack are covered (Tailor, 2014). By adopting a more focused view as to what strategic intelligence represents (Trim and Lee, 2007), it should be possible for senior managers to think in terms of making the organization more resilient (Trim and Lee, 2008a). This can be achieved through the development and deployment of strategic cyber security management models, frameworks and software packages.

What needs to be noted, is that the cyber environment in which organizations carry out their daily operations, is witnessing a different degree of interdependency materialize. For example, global operations require that management put in place a technically proven and tested iGRC (integrated governance, risk and compliance) framework and system, which incorporates outsource contracts information and operational analysis necessary to operate

the controls and metrics necessary for sustained iGRC management in a cyber environment that will increasingly become dependent upon adaptive risk management (Trim and Lee, 2010, pp.1-2). Hence the need for management to engage in cyber intelligence. According to Mattern et al., (2014: 704): "Cyber Intelligence seeks to not only understand network operations and activities, but also who is doing them, why, and what might be next … …… Cyber Intelligence should drive the cybersecurity mission. Intelligence-led operations require (a) a proactive security posture, (b) a thorough, accurate, timely understanding of the threat environment, and (c) a commitment to decisions based on data".

Strategic cyber security management models

What is focusing the interest of academic researchers is the increasingly complex and integrated network structures that are evolving, which are resulting in a higher degree of interdependency between organizations. Of concern to managers are longer lead times and shorter product life cycles, and if additional factors such as governance, risk and compliance are included, it becomes increasingly obvious that risk assessment and risk mitigation need more attention. In order to manage risk more adequately during periods of increased uncertainty, most notably changes in market dynamics (Trim and Lee, 2010, pp.1-2), it is necessary for managers to adopt a more pro-active approach to studying threats in the external environment and to devise an adequate SLEPT (Social, Legal, Economic, Political and Technological) analysis that can be used by strategists to put in place a strategic cyber security management model that will counteract various cyber threats.

The substitutability of suppliers; their indispensability; and common interests all need to be taken into consideration (Krapfel et al., 1991), if that is the organization's risk appetite is to remain at an acceptable level. Siguaw et al., (1998) have empirically examined the effectiveness of suppliers' marketing orientated behaviours on channel relationships and have produced a conceptual model. They have also focused attention on a distributor's marketing orientation approach, and have covered such important topics as trust, cooperative norms, commitment and satisfaction. Siguaw et al., (1998, pp.106-107) have provided research findings which indicate "that a supplier's market orientation affects the distributor's market orientation, and commitment to the relationship". Baker et al., (1999) support this view and suggest that commitment is very important, and is based on perception and cooperative norms. Distributors adopt the supplier's marketing orientation approach, because managers based in the distributor are committed to achieving higher financial returns, the outcome of which is increased levels of satisfaction.

It is worthwhile at this point to reflect upon advice given and acknowledge the fact that a cyber attack can come from a number of sources. Although the necessary controls may be in place, it may not prevent an attack getting through because the controls have not been implemented effectively (Clelland, 2014). It is sound advice therefore for management to test each control and ensure that it performs to the level required (Clelland, 2014).

Partnership related issues and research

At this point, it is useful to reflect and to suggest that during the initial stage of a partnership's development, a governance mechanism helps to integrate the various decision-making processes but needs to be viewed as flexible. This is due to the complexity of the socio-cultural environment and the business conditions that prevail and which are subject to change. Another point that should be noted is that senior managers may contemplate

establishing a hybrid organizational partnership culture that embraces national cultural traits, however, in the context of the cyber environment, it is most likely that because of the high degree of Internet linkage, technology itself becomes the greatest influencer as regards organizational configurations as opposed to an individual organization's value system and power oriented relationships.

It is obvious, therefore, that the concept of partnership needs to be placed in a wider context than is the case at present, and a partnership arrangement needs to be viewed from the perspective of mutuality. This being the case, the term partnership will become increasing understood as a method for fostering continual learning as staff in partner organizations adopt a pro-active, adaptive and risk sharing approach to doing business. Trim and Lee (2008b, p.223) have provided a useful interpretation of what a partnership arrangement constitutes: "An all embracing mutually oriented mechanism that allows staff within an organization to identify, devise and implement a legal instrument that results in combined ownership, an integrated management model that is underpinned by a hybrid organizational culture, which gives rise to a clearly defined mission statement and marketing strategy".

Business intelligence

A host of factors can be identified by managers that shape retailing landscapes, but speed of new product development and marketing mix considerations (Walters, 1979) are considered to be very important. Managers will, because of the level of complexity, need to avoid falling into the trap of thinking in terms of traditional retailing methodology and instead, need to adopt a forward thinking marketing approach that focuses on identifying and satisfying unmet needs. Meeting customer expectations is central to a retailing strategy being successful, however, establishing mutually oriented channel partnership arrangements that embrace facilitating technology are at the heart of the situation. Managers will need to embrace the strategic marketing concept (Aaker, 1984) more fully and also, develop a better appreciation and understanding of the role that marketing intelligence officers play (Trim and Lee, 2005; Trim and Lee, 2007). Another point that needs emphasising is that marketing intelligence officers need to possess analytical and interpretive skills. They also need to be aware of and have an appreciation of what business intelligence (BI) is and can deliver. For example, Maguire and Suluo (2007, p.21) state: "The future of retail BI will be defined by the retailers that have figured out how to maximize customer satisfaction and profitability with the right combination of quality products, friendly and efficient service, unique value, a differentiated shopping experience, and a business model that truly serves its community-locally and globally. This will be accomplished by starting with understanding the customer and then linking that insight into every decision that is made, from merchandising to marketing to distribution to store operations to finance, so that retailers can predict how to best serve their customers' ever changing needs and desires".

Managers, strategists, marketing intelligence officers, marketing researchers and organizational specialists concerned with business continuity need to be involved in identifying future cyber threats. Hence research needs to be undertaken to link firmly with corporate intelligence activities. This means that managers need to authorize industry forecasts and engage in scenario planning. As regards an organization's vulnerability, Sheffi (2005) has highlighted a useful and some would argue necessary approach to resilience and what emerges from the discussions is that there are several ways to reduce an organization's level of risk. One way is to identify and select trustworthy business partners that avoid opportunistic behaviour, and this may support the argument for a collectivist approach to

decision-making. Hence business-to-business relations can be viewed from the stance of "mutual market responsibility" (Walters, 1979, p. 214) and should this be the case, managers can implement what is known as an integrated systems approach that relies upon up-to-date marketing intelligence that incorporates an ethical approach to data collection and usage (Carrigan and Kirkup, 2001, pp. 415-435).

Partnership development

By ensuring that each organization in the partnership arrangement has a recognizable mission statement and also, that each of the mission statements is underpinned by a set of similar values, managers can reduce each of the organization's level of vulnerability. Managers in retail organizations do evaluate existing business relationships, negotiate new partnership arrangements, and deal effectively with local government (Lowe and Wrigley, 1996, pp. 13-16; Christopher and Juttner, 2000, p. 119; Porter et al., 2000, pp. 24-25 and pp.29-35), however, in the years ahead it will become even more important than it is at present to undertake a Cyber Security SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis. This is because staff based in the Corporate Intelligence function need to relate better to staff based in the other departments and functions if that is a more appropriate governance framework is to be implemented (Trim and Lee, 2010, p.2).

Owing to the fact that change in the business environment means that a partnership strategy locks partner organizations into a location strategy (Wrigley, 1994, p.7; Alexander, 1996, p.24 and p.26), managers need to possess the mindset to negotiate with local government representatives and various other interested stakeholders (Trim, 1999). They can be aided in their efforts by in-house and external researchers who, working in unison with marketing staff and staff from other business functions, identify issues and concerns of importance to senior management, and undertake research and intelligence studies that are aimed at providing answers to recurring problems (both cyber and non-cyber). Researchers will be called upon to identify and then interview industry experts in order to establish key industry drivers; undertake studies to validate the predictions of industry analysts; and organize a number of in-house seminars, workshops and focus groups that are aimed at validating or identifying trends in consumer buyer behaviour for example. By working closely with marketing intelligence officers, strategists and competitive intelligence officers, it should be possible for researchers to outline how changes in government regulatory policy results in new market opportunities.

The degree of integration between a retail organization and its suppliers is strongly influenced by the way in which each organization participates in the business relationship and the how managers exercise their responsibilities within the partner organizations. A high level of customer service is closely related with the issue of how retail organizations can create fitness through internal and external harmony. Hence a continuous relationship building process is perceived as essential (Beckett-Camarata et al., 1998, p.78). This can be interpreted from the stance of achieving a sustainable competitive advantage and refocuses the strategy-structure debate. One can think in terms of appropriate organizational design (Germain and Droge, 1997), and how the sharing of information results in a cost advantage. Cost related information is normally classified as confidential and sensitive and can be a source of strategic risk because of the vulnerability aspect (Christoper and Juttner, 2000, p.119). However, information sharing is necessary for developing trust and may be considered a key aspect of doing business (Trim and Lee, 2006). Selecting appropriate channel members is important with respect to an organization achieving vertical marketing

integration and ultimately a sustainable competitive advantage (Cespedes, 1995; Kumar et al., 1995; Weitz et al., 1995; Siguaw et al., 1998).

Trust in the context of a partnership arrangement

Doney and Cannon (1997, p.36) have built on Ganesan's (1994, pp.3-4, and p.15) work; and the work of Kumar et al., (1995); and have provided useful definitions of trust. It is clear, that trust is composed of two components: one is perceived credibility (which refers to the ability to perform satisfactorily a given task) and the other is benevolence (which requires that short-term benefits are given-up for a long-term relationship and mutual benefits). It can be suggested, therefore, that trust is a pivotal element in the strategy process when two or more organizations attempt to build a strong, continuous relationship. Krause and Ellram (1997, p.30) have examined some of the key elements of trust building (such as two-way communication, top management involvement in the development of relationships, the role of liaison teams, and the volume of purchasing from partner suppliers), and have indicated that managers in retail organizations must invest in training and education programmes. Managers in supplier organizations can show that they are committed to partnership development by investing in up-to-date equipment, and training and education programmes that improves the skill and knowledge base of their employees (Ganesan, 1994, p.13; Doney and Cannon, 1997, p.47).

According to Mattern et al., (2014: 704): "A proactive posture relies on well thought out and dynamic defenses, informed by intelligence, to address both actual and potential threats. Ideally, this approach relies on the full spectrum of an organization's capabilities-from network defense, to public relations, legal efforts, and other business operations. Proactive positioning also relies on a comprehensive and accurate understanding (and in as near real time as possible) of one's own network, and the ability to collect and integrate information sources outside of that network to fully assess the threat environment". Possibly a transformational as opposed to a transactional form of leadership is required. Trim and Upton (2013: 53) have stated: "A transformational leader places a high emphasis on trust and trust-based relationships, and considers that employees need to be in harmony with the organization's objectives. This can be interpreted as an individual employee having the same value system as their peers (and other employees) and that there is a match between the employee's value system and the organization's value system, hence internal mutuality".

Engaging in research

Managers operating in the international business environment are involved in a range of data and information gathering exercises relating to market structure; how legislation affects retailing operations; how local retailers can explore product-market opportunities; and how cultural knowledge can aid promotional activities. McAuley (2004) has acknowledged the importance that culture plays in consumer decision-making and suggests that marketers need to be politically aware. Managers can choose between a number of market entry strategies when launching new business ventures abroad. This has resulted in opportunities for retail organizations (Davies and Fergusson, 1995, p. 104) and to some degree changed the emphasis of business-to-business relationships. What can be deduced is that as market opportunities evolve, business relationships are both stimulated and nurtured. However, managers engaged in research seldom authorize ethnographic studies of any kind and this is regrettable because this type of research, which can be placed in a socio-cultural context, can provide evidence relating to how personal relationships are formed; how individuals can be

motivated to develop and maintain personal bonds; and how trust between managers in different organizations can be maintained in times of uncertainty. Ethnographic research can also provide insights into how peer group decisions are made and can highlight the important characteristics of non-formal human interaction (socializing activity). Ethnographic research has the added advantage of providing insights into how the role of power within an organizational setting influences and shapes relationships and organizational activities (both within and between departments) and how power struggles, shape business policy. A partnership arrangement is affected by power struggles from time to time and this needs to be recognized in order that risk reduction is achieved. The role that power plays in relationship building has been addressed by Hingley (2005, pp.66-75) and it can be argued that power play activities and politicking can have consequences vis-à-vis organizational vulnerability.

Methodological approach: fitness for purpose

As regards acquisition strategy, Burt and Limmack (2001, p.18) suggest that takeover strategies do not always meet the expectations of the various stakeholders, and issues such as related versus unrelated diversification spring to mind. Pre-acquisition strategy activity can be researched using qualitative research methods. Both observational research and an attitudinal research survey can be undertaken to explain the activities of the parties involved. It is relevant to note, however, that a great deal of pre-acquisition activity is of a secretive nature and not open to outside scrutiny. Turning to the external environment, although economic analysis is useful it is not always appropriate vis-à-vis understanding the structure of retailing, and the impact that legislation has on business operations (Dawson, 2000; Davies and Itoh, 2001). Another point that has been recognized as influential in retailing, is the role played by small and medium-sized retail organizations. The conceptual framework put forward by Hutchinson et al., (2005, pp.162-168) is useful with respect to exploring the international marketing strategies of small and medium-sized retail organizations and covers a gap in the body of knowledge. The in-depth personal interview method can be used to establish how senior managers in small companies make the decisions that they do and can be used to provide evidence of multi-tasking activity.

It is generally agreed that the qualitative research paradigm provides researchers with a means to obtain insights into various management issues and problems, and Easterby-Smith and Thorpe (1997, p.51) are right to suggest that the qualitative research approach provides an opportunity to understand better the processes associated with management learning.

The grounded theory approach allows the concepts derived from the primary data collection process to be analyzed and the results compared with the theoretical ideas/concepts contained in the relevant literature. It is this flexibility that is not only intellectually stimulating, but enables researchers to think in terms of developing theory, adding to what exists in the form of inductive theory-generating research (Orton, 1997, p.421) and extending the life of a research project.

We are of the view that the grounded theory approach is an acceptable theory building/theory development, methodological approach that involves a number of steps: ‘open coding’, ‘axial coding’, and ‘selective coding’ (Strauss and Corbin, 1990; 1998). Suddaby (2006) is supportive of this view and points out that when using the grounded theory approach, researchers need to be as transparent as possible about the methodological approach itself. We consider the research approach justified as it provides a basis for understanding a complex and interesting phenomenon (Suddaby, 2006, p.636). Indeed, grounded theory can

be viewed as complex, for example, during the axial coding process, the following paradigm model should be adopted: "(A) Causal conditions → (B) Phenomenon → (C) Context → (D) Intervening conditions → (E) Action/interactional strategies → (F) Consequences/outcomes" (Strauss and Corbin, 1990, p.99). One of the advantages of the paradigm model is that it represents a logical approach, which allows researchers to think systematically about establishing causal conditions and thus provides a basis for understanding how a set of relationships are linked. It also allows researchers to add density and precision and these can be considered additional strengths.

Conclusion

Managers in public and private sector organizations need to think about undertaking various forms of qualitative research and quantitative research, on a regular basis, in order to collect data relating to the cyber environment in order to keep up with cyber threats and their possible impacts. Joint research projects can be undertaken with university researchers, and ways can be found to cooperate across industry sectors.

There is no doubt that developments in digital marketing and online payment systems will fashion the way in which business is conducted, and because of this, research needs to be undertaken into how now business models are evolving and what this means for customers and society. By adopting a pro-active approach to researching aspects of the cyber environment, it should be possible to identify immediate and future areas of concern and add to the security and intelligence body of knowledge. It should also allow managers to identify skill gaps and how these gaps can be eradicated through training and educational programmes.

List of recommendations

Recommendation 1: Managers in various organizations need to engage in research with academic researchers to establish the effects (eg., reputational damage) that are caused by cyber security impacts.

Recommendation 2: Managers based throughout a business partnership arrangement need to undertake research into a hybrid organizational culture and establish how such a culture influences the development of a particular business model.

Recommendation 3: Managers in various organizations need to undertake research to establish how staff can engage in and contribute to research projects that study the link between how workers interface with technology.

Recommendation 4: Managers in various organizations can undertake research that studies the adaptive and risk sharing approach to doing business, and link the research findings with the organizational learning concept.

Recommendation 5: Managers can undertake research into how senior managers design a strategic partnership arrangement and how cyber security knowledge transfer occurs that results in a high level of organizational resilience.

Recommendation 6: Organizational staff can undertake qualitative and quantitative research that identifies how individual managers relate to each other in a cross-cultural setting and how a particular business model is formed, implemented and evaluated through time.

Recommendation 7: Studies can be undertaken on a regular basis to establish how effective security policy is implemented with respect to staff working practices in relation to the company working environment, and in particular, what employees do when they take home company owned laptops or use alternative devices to undertake their work.

Recommendation 8: Working with academic researchers, managers can undertake research into developing strategic partnership arrangements with other organizations and establish how a strategic cyber security management model can be developed that promotes and reinforces the concept of mutuality, which gives rise to information sharing.

Recommendation 9: Managers can undertake research into how certain types of cyber attacks should be dealt with and how this can result in a company wide, holistic view of security being implemented.

Recommendation 10: Research can be undertaken that establishes how an organization can be made more resilient through the development and deployment of strategic cyber security management models and frameworks, and cyber security software packages.

Recommendation 11: Research can be undertaken that focuses attention on improving a partner organization's cyber security strategic intelligence capability in relation to new product launches, timely market entry strategies and defensive retaliatory actions against competitors for example.

Recommendation 12: Managers need to think more deeply about security breaches and the wider impact that these might have on customers and society.

Recommendation 13: Research needs to be undertaken in the area of cyber security awareness in order to establish how security training and security education, can be enhanced and how sustainable working relationships can be established between private sector and public sector organizations.

Recommendation 14: Research can be undertaken to establish how managers can undertake risk management and how individuals in organizations can be held accountable for the risk management process, and what type of leadership style is appropriate for managing risk.

Recommendation 15: Management should undertake, on a regular basis, studies relating to cyber security situation(al) analysis and establish how business impact analysis can be formalized.

Recommendation 16: Research can be undertaken to establish what senior management need to do in order to put in place a risk communication strategy and how a communication policy is to be coordinated across business functions. (The risk communication process needs to include all the stakeholders: suppliers, external organizations (eg., design companies), manufacturers, wholesalers and retailers for example).

References

Aaker, D.A. (1984). *Strategic Market Management.* Chichester: John Wiley and Sons.

Akehurst, G., and Alexander, N. (1995). The internationalization process in retailing. *The Service Industries Journal*, 15 (4), pp.1-15.

Alexander, N. (1996). International retail expansion within the EU and NAFTA. *European Business Review*, 96 (3), pp.23-35.

Bach, R. (2014). Government's response to the evolving threat. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Baker, T. L., Penny, M. S., and Siguaw, J. A. (1999). The impact of supplier's perceptions of reseller marketing orientation on key relationship constructs. *Journal of the Academy of Marketing Science*, 27 (1), pp.50-57.

Beckett-Camarata, E. J., Camarata, M. R., and Barker, R. T. (1998). Integrating internal and external customer relationships through relationship management: a strategic response to a changing global environment. *Journal of Business Research*, 41, pp.71-81.

Burt, S., and Limmack, R. (2001). Takeovers and shareholder returns in the retail industry. *The International Review of Retail, Distribution and Consumer Research*, 11 (1), pp.1-21.

Carrigan, M., and Kirkup, M. (2001). The ethical responsibilities of marketers in retail observational research: protecting stakeholders through the ethical 'Research Covenant'. *The International Review of Retail, Distribution and Consumer Research*, 11 (4), pp.415-435.

Cespedes, F. V. (1995). *Concurrent Marketing: Integrating Product, Sales and Service.* Boston, Massachusetts: Harvard Business School Press.

Christopher, M., and Juttner, U. (2000). Developing strategic partnership in the supply chain: a practitioner perspective. *European Journal of Purchasing and Supply Management*, 6 (2), pp.117-127.

Clelland, J. (2014). Why are businesses breached following successful security audits? *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Davies, G., and Itoh, H. (2001). Legislation and retail structure: the Japanese example. *The International Review of Retail, Distribution and Consumer Research*, 11 (1), pp.83-95.

Davies, K., and Fregusson, F. (1995). The international activities of Japanese retailers. *The Service Industry Journal*, 15 (4), pp.97-117.

Dawson, J. (2000). Viewpoint: retailer power, manufacturer power, competition and some questions of economic analysis. *International Journal of Retail and Distribution Management*, 28 (1), pp.5-8.

Doney, P. M., and Cannon, J. P. (1997). An examination of the nature of trust in buyer-supplier relationships. *Journal of Marketing*, 61 (April), pp.35-51.

Easterby-Smith, M., and Thorpe, R. (1997). Research traditions in management learning. In: Burgoyne, J., and Reynolds, M. (Eds). *Management Learning: Integrating Perspective in Theory and Practice*. London: Sage Publications, pp.38-53.

ENISA. (2011). *Risk Management*. European Network and Information Security Agency, pp.1-108. Source:http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-process [accessed 27 February, 2011]

Ganesan, S. (1994). Determents of long-term orientation in buyer-seller relationships. *Journal of Marketing*, 58 (April), pp.1-19.

Germain, R., and Droge, C. (1997). Effect of just-in-time purchasing relationships on organizational design, purchasing department configuration and firm performance. *Industrial Marketing Management*, 26, pp.115-125.

Gibson, C. (2014). Improving the UK's cyber resilience. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Hardy, A. (2014). Endpoint security for the modern enterprise. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Hingley, M.K. (2005). Power imbalance in UK agri-food supply channels: learning to live with the supermarkets? *Journal of Marketing Management*, 21 (1-2), pp. 63-88.

Howe, W. S. (1998). Vertical marketing relations in the UK grocery trade: analysis and government policy. *International Journal of Retail and Distribution Management*, 26 (6), pp.212-224.

Hutchinson, K., Quinn, B., and Alexander, N. (2005). The internationalization of small to medium-sized retail companies: towards a conceptual framework. *Journal of Marketing Management*, 21 (1-2), pp.149-179.

Jones, N. (2014). The changing cybercrime and fraud landscape. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Jopling, P. (2014). Areas to address in cyber security. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Krapfel, R., and Salmond, D., and Spekman, R. (1991). A strategic approach to managing buyer-supplier relationships. *European Journal of Marketing*, 25, pp.22-37.

Krause, D. R., and Ellram, L. M. (1997). Critical elements of supplier development: the buying-firm perspective. *European Journal of Purchasing and Supply Management*, 3 (1), pp.21-31.

Kumar, N., Scheer, L. K., and Steenkamp, J-B. E. M. (1995). The effects of supplier fairness on vulnerable re-sellers. *Journal of Marketing Research*, 32 (February), pp.54-65.

Lewison, D. M. (1997). *Retailing.* Englewood Cliffs, New Jersey: Prentice-Hall, Inc.

Lewison, D. M., and DeLozier, M. W. (1986). *Retailing*. Columbus, Ohio: Merrill Publishing Company.

Lowe, M., and Wrigley, N. (1996). Toward the new retail geography. In: Wrigley, N., and Lowe. M. (Eds). *Retailing Consumption and Capital*. Harlow: Longman Group Limited, pp. 3-30.

Maguire, S., and Suluo, H. (2007). Chapter 2: Business intelligence: Benefits, applications, and challenges. In Xu, M. (Ed). *Managing Strategic Intelligence*. Hershey, PA: Information Science Reference , pp.14-34.

Management Today (2014). Are you ready for a cyber attack? *Management Today* (September), pp.28-29.

Martin, D., Howard, C., and Herbig, P. (1998), The Japanese distribution system. *European Business Review*, 98 (2), pp.109-112.

Mattern, T., Felker, J., Borum, R., and Bamford, G. (2014). Operational levels of cyber intelligence. *International Journal of Intelligence and CounterIntelligence*, 27 (4), pp.702-719.

McAuley, A. (2004). Seeking (marketing) virtue in globalisation. *The Marketing Review*, 4 (3), pp.253-266.

Morganosky, M. A. (1997). Retail market structure change: implications for retailers and consumers. *International Journal of Retail and Distribution Management*, 25 (8), pp.269-274.

Orton, J.D. (1997). From inductive to iterative grounded theory: zipping the gap between process theory and process data. *Scandinavian Journal of Management*, 13 (4), pp.419-438

Porter, M. E., Takeuchi, H., and Sakakibara, M. (2000), *Can Japan Compete*? Houndmills, Basingstoke: Macmillan Press Ltd.

Samtani, T. (2014). Cyber security – The most important business priority. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Selman, D. (2014). Defence cyber protection partnership – Working together to better protect defence information. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Sheffi, Y. (2005). *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage.* Cambridge, Massachusetts: The MIT Press.

Siguaw, J. A., Penny, M. S., and Baker, T. L. (1998). Effects of supplier market orientation on distributor market orientation and the channel relationship: the distributor perspective. *Journal of Marketing*, 62 (July), pp.99-111.

Sparks, L. (1995). Reciprocal retail internationalization: the Southland Corporation, Ito-Yokado and 7-Eleven convenience stores. *The Service Industry Journal*, 15 (4), pp.57-96.

Strauss, A., and Corbin, J. (1990). *Basics of Qualitative Research.* Newbury Park, CL: Sage Publications.

Strauss, A., and Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. London: Sage Publications.

Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of Management Journal*, 49 (4), pp.633-642.

Tailor, A. (2014). Hiding in plain sight – What's really happening on your network. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Trim, P. R. J. (1999). The corporate intelligence and national security (CINS) model: a new era in defence management. *Strategic Change*, 8 (3), pp.163-171.

Trim, P.R.J., and Lee, Y-I. (2005). The role of marketing intelligence officers in strategic formulation and implementation. In: Coate, P. (Ed). *Handbook of Business Strategy, 2006.* Bradford: Emerald Group Publishing Limited, pp,125-130

Trim , P.R.J., and Lee, Y-I. (2006). Vertically integrated organizational marketing systems: a partnership approach for retailing organizations. *Journal of Business and Industrial Marketing*, 21 (3), pp.151-163.

Trim, P.R.J., and Lee, Y-I. (2007). Chapter four: A strategic marketing intelligence framework reinforced by corporate intelligence. In: Xu, M. (Ed). *Managing Strategic Intelligence*. Hershey, PA: Information Science Reference, pp.55-68.

Trim, P.R.J., and Lee, Y-I. (2008a). A strategic marketing intelligence and multi-organizational resilience framework. *European Journal of Marketing***,** 42 (7/8), pp.731-745**.**

Trim, P.R.J., and Lee, Y-I. (2008b). A strategic approach to sustainable partnership development. *European Business Review***,** 20 (3), pp.222-239.

Trim, P.R.J., and Lee, Y-I. (2010). A security framework for protecting business, government and society from cyber attacks. *5th IEEE International Conference on System of Systems Conference (SoSE): Sustainable Systems for the 21st Century*, Loughborough University, 22nd to 24th June (pp.1- 6).

Trim, P.R.J., and Lee, Y-I. (2014). *Cyber Security Management: A Governance, Risk and Compliance Framework.* Farnham: Gower Publishing.

Trim, P.R.J., and Upton, D. (2013). *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training.* Farnham: Gower Publishing.

Walters, D. (1979). Manufacturer/retailer relationships. *European Journal of Marketing*, 13 (7), pp.179-222.

Weitz, B. A., Castleberry, S. B., and Tanner, J. F. (1995). S*elling: Building Partnerships.* Chicago*:* Richard D. Irwin.

Wrigley, N. (1994). After the store wars: towards a new era of competition in UK food retailing. *Journal of Retailing and Consumer Service*, 1 (1), pp.5-20.

Appendix 1: The 2013-2014 future objectives and recommendations

Objective 1: Sustaining the Korea-UK Cyber Security Research Network through identifying Korean-UK collaborative projects.

Objective 2: Establish how various government funded projects (e.g., smart cities) in both the UK and Korea were giving rise to market opportunities.

Objective 3: Establish how joint research projects could be managed.

Objective 4: Establish how the Korean Government and UK Government were increasing the cyber security skill base in their respective countries and how organizations were responding to the challenge.

Recommendation 1: Establish a centre that fosters cooperation between Korea and the UK. It would be possible to expand the envelope of cooperation between Korea and the UK beyond cyber security and related areas, and engage more widely with academia and industry in both Korea and the UK. Such a centre would complement existing centres of excellence and would allow additional networks to develop. Additional research networks would help promote and coordinate current and future industry-university partnership arrangements.

Recommendation 2: Those involved in the Korea-UK cyber security research network need to take into account how the outputs/research findings reinforce the content of the workshops/conferences and how the recommendations can be applied in practice. In particular, the *2013 Information Security Breaches Report*, which was commissioned by the Department for Business, Innovation and Skills (BIS) and conducted by PwC was considered useful as an example of relevant information relating to both small and large organizations that could be utilized and developed further.

Recommendation 3: A monitoring system/process needs to be established to ensure that the outputs/research findings are applied in a logical way by a range of organizations across all industry sectors.

Recommendation 4: When promoting the research network and its activities, reference needs to be made to the fact that it is a partnership arrangement involving government, industry and academia. Useful organizational contacts include: Information Assurance Advisory Council (IAAC); IET (The Institution of Engineering Technology); National Crime Agency; Centre for the Protection of National Infrastructure (CPNI); Department for Business, Innovation and Skills (BIS); BCS The Institute for IT; e-skills UK; the Cabinet Office; the Foreign and Commonwealth Office; the British Business Federation Authority; MACCSA (Multinational Alliance for Collaborative Cyber Situational Awareness); Ministry of Science, ICT and Future Planning; Korea Internet & Security Agency (KISA); National Information Society Agency (NIA); Electronics and Telecommunications Research Institute (ETRI); the Korea Police Cyber Terror Response Centre (CTRC); and various other public and private sector organizations and universities in Korea and the UK.

Recommendation 5: The aims of the research network need to be made clear and endorsed by additional members of the network who join through time. In other words, the research network members need to be aware of the level of work involved and need to be committed to the success of the network.

Recommendation 6: The members of the research network are in possession of relevant knowledge already or are able through their association with other members of the network to obtain knowledge and insights. It is expected that people will share relevant knowledge and help extend the network of members so that additional knowledge in relation to meeting the objectives stated in the national cyber security strategy benefit a wide audience.

Recommendation 7: By working on cyber security projects, the knowledge acquired will help to consolidate our understanding of cyber security as a stand alone body of knowledge that has links with other bodies of knowledge and this will help to establish a consolidated but integrated body of cyber security knowledge.

Recommendation 8: Attention should be given to extending the cyber security research network to include other geographical areas of the world. (It can be noted that there was a representative from Japan in the cyber security research network).

Recommendation 9: The Korean government and the UK government should hold an annual or biannual cyber security workshop(s) to enable cyber security experts and researchers, and interested parties from the private and public sectors, to engage in information sharing and exchange, relating to security provision in general and cyber security policies and changing threat landscapes in particular, to compare best practice associated with dealing with ways and methods to counteract the risks posed by the ever increasing sophisticated forms of advanced persistent threats (APTs)**.**

Recommendation 10: 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 11: To establish how scenario-based training and the organizational learning concept can promote the collectivist decision-making approach to security.

Recommendation 12: 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 13: Research should be undertaken that links cyber security with innovation studies in order to establish how cyber security projects are managed through time.

Recommendation 14: 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 15: 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 16: 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 17: 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 18: 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 19: 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.

Recommendation 20: Research needs to be undertaken into how social engineering and human behavioural factors are placing an organization at risk.

Recommendation 21: Research needs to be undertaken into how the concept of corporate intelligence can be used to provide more appropriate risk management in the context of SME's.

Recommendation 22: Research needs to be undertaken in order to establish how managers based in SME's can work with partner organizations in order to develop a joint cyber security approach.

Recommendation 23: Research needs to be undertaken in order to establish how managers based in SME's can address current and future security issues and devise initiatives such as an organizational cyber security policy that is underpinned by the organizational learning concept.

Recommendation 24: Research needs to be undertaken in order to establish how managers based in SME's can develop internship programmes, with support from universities and colleges, and support academia in developing and operating customized cybersecurity curriculum, so that a cyber security profession is established.

Recommendation 25: Research needs to be undertaken in order to establish how managers based in SME's can develop relevant cyber security training material that utilizes table top exercises and supports training in cyber security more generally so that the skill base of the employees is improved.

Recommendation 26: Research needs to be undertaken in order to establish how managers based in SME's can develop a cyber security research culture and improve cyber security awareness within the organization.

Recommendation 27: Research needs to be undertaken in order to establish how managers based in SME's can work with relevant stakeholders to improve cyber security training and educational provision and how employers can work with educational institutions and

professional organizations to ensure that the education and training provided, whether in-house or contracted-in, is of an appropriate standard.

Recommendation 28: Research needs to be undertaken in order to establish how managers based in SME's can work with government representatives to ensure that information security practitioners reach a defined level of competency and they comply with organizational and legal requirements.

Recommendation 29: Research needs to be undertaken in order to establish how managers based in SME's can work with various stakeholders to ensure that a cyber security culture is embedded in a holistic security management culture.

Recommendation 30: Research needs to be undertaken in order to establish how managers based in SME's can work with various stakeholders to ensure that scenario-based training is underpinned by a collectivist approach to security.

Recommendation 31: Research needs to be undertaken in order to establish how managers based in SME's can develop a cyber security policy, so that they have their own customized cyber security policies.

Recommendation 32: Research needs to be undertaken in order to establish how managers based in SME's can implement risk management, so that they manage security risks that may have a negative effect on the organization's business objective(s).

Recommendation 33: Research needs to be undertaken in order to establish how managers based in SME's can deploy cyber security solutions, so that they implement effectively the organization's cyber security policies.

Recommendation 34: Research needs to be undertaken in order to establish how managers based in SME's can measure their competency and preparedness, so that they respond to existing or emerging cyber security threats.

Recommendation 35: Research needs to be undertaken in order to establish how managers based in SME's can deploy forecasting methods in order to establish what type of cyber security threats are emerging on an industry by industry basis.

Recommendation 36: Research needs to be undertaken in order to establish what national, regional and international standards need to be developed and/or made in order to address emerging cyber threats.

Recommendation 37: Research needs to be undertaken in order to to establish how organizations measure their competency against advanced emerging threats in order to improve the level of cyber security provision deemed necessary to ensure that the organization is considered robust.

Recommendation 38: Research needs to be undertaken to explain how a virtual cyber security emergency planning simulation can be used to train cyber security professionals and those undertaking a training and/or educational programme in the area of cyber security.

Appendix 2: Korea-UK Cyber Security Research Network Group Members 2013 to 2014

Mr. John Austin, CSC Global Cybersecurity
Dr. Jong-hyun Baek, Korea Internet Security Agency
Hugh Boyes, Warwick University
Kevin Brear, J.P. Morgan
Mr. Bruno Brunskill, Information Assurance Advisory Council (IAAC) & Trusted Management Ltd.
Dr. Kyugon Cho, CEO for Fasoo.com and was a former president of KISIA, a Korean industry association in the information security area.
Mr. SiHaeng Cho, a former CTO for AhnLab, Korea.
Dooho Choi Electronics and Telecommunications Research Institute (ETRI)
Dr. Kyugho Chung, a Vice President of KISA.
Nick Connor, Assuria
Patrick Curry, Multinational Alliance for Collaborative Cyber Situational Awareness Ltd (MACCSA).
Kim Du-Hyun, National Information Society Agency (NIA)
Dr. Godfrey Gaston, Queen's University Belfast
Dr Robert Ghanea-Hercock, BT Technology, Service and operations (TSO)
Professor Hugh Griffiths, University College London
Mr. Oliver Hoare, Dysart Solutions Ltd.
Ms. (Elly) IL young Hong, Supreme Prosecutors' Office of Korea.
Mr. Mike Humphrey, National Crime Agency
Dr. Inkyung Jeun, a director of KISA.
Mr. Nigel Jones, UK Defence Academy, Cranfield University,
Professor Jina Kang, Seoul National University
Professor Beomsoo Kim, Yonsei University.
Dr. Du-Hyun Kim, National Information Society Agency (NIA)
Hyeyoung Kim, Science & Innovation Manager, British Embassy Seoul, Republic of Korea.
Ms. E.J. Kim, previously employed by the British Embassy in Seoul.
Professor Kyung Hoon Kim, Changwon National University
Dr. Tae Kyung Kim, Computer and Information Center at Seoul Theological University
Dr. Young Wha Kim, a Director of the TTA (Telecommunication Technology Agency).
Professor Eunju Ko, Graduate School of Yonsei University
Mr Jae Nam Ko, Soonchunhyang University
Professor Kyungho Lee, Korea University
Dr. Sang Woo Lee, ETRI.
Dr. Yang-Im Lee, University of Westminster
Professor Dae-Ha Park, The Cyber University of Korea
Dr. DeaWoo Park, Hoseo Graduate School of Venture
Soon Tae Park, Korea Internet & Security Agency
Tony Proctor, University of Wolverhampton
Dr. Peter Trim, (Chairman of the UK Cyber Security Research Network), Birkbeck, University of London (Email: p.trim@bbk.ac.uk)
Professor David Upton, University of Oxford
Professor Tim Watson, University of Warwick
Dr. David J. Weston, Birkbeck, University of London
Professor Heung Youl Youm, (Chairman of the Korean Cyber Security Research Network), Soonchunhyan University (Email:hyyoum@sch.ac.kr)

Professor Hyeon Yu, Korea Police Investigation Academy
Dickie Whitaker, Financial Services Knowledge Transfer Network

International Group Member
Professor Hironobu Nakabayashi, Meiji University

Observers
Ms. Rhian Jones, Cabinet Office, UK
Mr. Austen Okonweze, Department of Business Innovation and Skills, UK

Appendix 3: Korea-UK Cyber Security Research Network Group Members 2014 to 2015

Mr. Tony Butler, Delphinitum
Mr. Patrick Curry, MACCSA (Multinational Alliance for Collaborative Cyber Situational Awareness Ltd) and British Business Federation Authority (BBFA) Ltd
Mr. Vince Freeman, Metropolitan Police
Mr. Robert Hall, London First
Mr. Robert Hann, Trustis
Mr. Oliver Hoare, Dysart Solutions Ltd
Mr. Mike Humphrey, National Crime Agency
Mr. Tae Sun Hwang, Korea Telecom
Nigel Jones, UK Defence Academy, Cranfield University
Mr. Hongsoon Jung, Korea Internet & Security Agency
Dr. Kyugho Chung, a Vice President of the Korea Internet & Security Agency (KISA)
Dr. Pilyong Kang, Korea Internet & Security Agency (KISA)
Mr. Ki-Woon Lee, Korea Internet & Security Agency (KISA)
Dr. Pilyong Kang, Korea Internet & Security Agency (KISA)
Mrs. Hyeyoung Kim (British Embassy, Seoul)
Mr. Hyunjun Kim, FireEye, Korea
Dr. Jaejung Kim, KICA
Mrs. Yoonjeong Kim, Korea Internet & Security Agency
Mr. Mark King, Broadsail
Mr. Jae Nam Ko, Soonchunhyang University
Mr. Ki-Woon Lee, Korea Internet & Security Agency (KISA)
Dr. Yang-Im Lee, University of Westminster
Mr. Dmitry Organ, The Risk Advisory Group plc
EurIng Dr. Richard Overill, King's College London
Dr. Jae Hoon Nah, Electronics and Telecommunications Research Institute (ETRI)
Professor Dae Ha Park, The Cyber University of Korea
Mr. Richard Pharro, The APM Group Limited
Dr. Emma Philpott, IASME Consortium Limited
Mr. Alan Shipman, Group 5 Training Limited
Dr. Peter Trim (Chairman of the UK Cyber Security Research Network), Birkbeck, University of London (Email: p.trim@bbk.ac.uk)
Professor Tim Watson, University of Warwick
Professor Heung Youl Youm (Chairman of the Korean Cyber Security Research Network), Soonchunhyan University (Email:hyyoum@sch.ac.kr)
Mr. Kwangtaek Youn, Symantec, Korea

Observers
Ms. Rhian Jones, Cabinet Office, UK
Mr. Austen Okonweze, Department for Business Innovation & Skills (BIS), UK

Appendix 4: Agenda and Minutes of the UK Cyber Security Research Network Group

Agenda

The meeting will be held in room 224 at 43 Gordon Square (Birkbeck College) on Tuesday 25th November, 2014, from 9.30am to 1.30pm. (Please note there will be refreshments at 9.30am and an early lunch will be available from 11.30am onwards).

Those attending: Dr Peter Trim (Birkbeck, University of London)(Chairman); Mr. Robert Hall, Director, Security & Resilience Network, London First; Mr. Oliver Hoare, CEO, Dysart Solutions Ltd., Mike Humphrey, Head of Information Assurance and Accreditation, National Crime Agency; Dr. Yang-Im Lee, University of Westminster, and EurIng Dr. Richard Overill, King's College London.

Those unable to attend but to be informed of the outcome of the meeting: Mr. Kevin Brear, Information Risk Manager, JP Morgan Chase; Dr. Tom Chen, City University; Mr. Patrick Curry, CEO, MACCSA (Multinational Alliance for Collaborative Cyber Situational Awareness Ltd); Tony Holmes, BT; Ms. Rhian Jones, Cabinet Office, UK; Nigel Jones, UK Defence Academy, Cranfield University; Mr. Austen Okonweze, Department for Business Innovation & Skills (BIS),UK; and Professor Tim Watson, Director, Cyber Security Centre, WMG, University of Warwick.

CC Hye Young Kim (British Embassy, Seoul) and Professor Heung Youl Youm (Soonchunhyang University).

Points for discussion

1. Welcome and introductions. (Each person has between 5 to 10 minutes to introduce themselves and their work). (Those arriving later in the morning will be given time to introduce themselves).

2. A brief summary of the current situation vis-à-vis the Korea-UK Cyber Security Research Network.

3. Matters arising from the report by Trim, P.R.J., and H.Y. Youm (March, 2014)(Editors). *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership.* British Embassy Seoul: Republic of Korea. The report was submitted to the Korean Government and the UK Government on 18th March, 2014.

4. The 2014 to 2015 Korea-UK Cyber Security Research Network.
   - Budget.
   - Workshops and meetings.
   - Final report.

5. Outline programme for the two workshops (Seoul and London, 2015).
   - First workshop Seoul: possibly 4 people from the UK to attend.
     - The draft itinerary for the UK delegation/speakers:
     - 17/1/2015: (Saturday) depart from the UK to Seoul (Incheon airport).
     - 18/1/2015 (Sunday): arrive at Incheon airport at 8:00 am (?)/free time.
     - 19/1/2015 (Monday): Korea-UK workshop on Cyber Security at COEX meeting room.
     - 20/1/2015 (Tuesday): site visits plus wrap-up meeting and dinner.
     - 21/1/2015: (Wednesday): UK delegation/speakers depart (10:30am).
   - Immediate action: to discuss and agree the themes/speakers with Professor Youm.

   - Second workshop London: possibly 3 to 5 people from Korea to attend.
     - Final wrap-up meeting at BIS Conference Centre. (Closed audience: 3 to 5 Korean people and 10 invited UK participants). Proposed date(s): 2nd and/or 3rd March, 2015.

6. Any other business

Minutes of the UK Cyber Security Research Network Group Meeting

The meeting of the UK Cyber Security Research Network Group was held in room 224 at 43 Gordon Square (Birkbeck, University of London) on Tuesday 25th November, 2014, from 9.30am to 1.30pm.

In attendance was Dr Peter Trim (Birkbeck, University of London)(Chairman); Mr. Robert Hall, Director, Security & Resilience Network, London First; Mr. Oliver Hoare, CEO, Dysart Solutions Ltd., Mr. Mike Humphrey, Head of Information Assurance and Accreditation, National Crime Agency; Dr. Yang-Im Lee, University of Westminster, and EurIng Dr. Richard Overill, King's College London.

Those unable to attend included: Mr. Kevin Brear, Information Risk Manager, JP Morgan Chase; Dr. Tom Chen, City University; Mr. Patrick Curry, CEO, MACCSA (Multinational Alliance for Collaborative Cyber Situational Awareness Ltd); Tony Holmes, BT; Ms. Rhian Jones, Cabinet Office, UK; Mr. Nigel Jones, UK Defence Academy, Cranfield University; Mr. Austen Okonweze, Department for Business Innovation & Skills (BIS),UK; and Professor Tim Watson, Director, Cyber Security Centre, WMG, University of Warwick.

1. Welcome and introductions.

Each person provided a short talk about their background, experience and work.

Mr. Robert Hall, Director, Security & Resilience Network, London First, outlined his background and experience and explained that he liaises with law enforcement personnel and works closely with the various police forces protecting London. He has been involved in the production of the Organisational Resilience standard and is aware of the fact that companies need more support and assistance in the area of cyber security and resilience. His involvement in a communication hub in relation to the 2012 London Olympic Games brought home the fact that security is multidimensional and for the 200 members of London First it is known that resilience is a key consideration because businesses in London face a range of evolving threats. Corporate reputation is an immediate area of concern among managers based in small and medium sized enterprises (SME's), as well as large corporates, because the risks are increasing. In particular, managers are aware of the fact that more interaction is needed between cyber security specialists and those able to provide practical help and assistance to staff based in SME's. It is acknowledged that the guidance offered is very good. However, more needs to be done in order to move from increased security awareness to the implementation of security policy within SME's and policy makers need to be aware of this. Increasing the impact or bringing about change needs to move beyond a nudge strategy. More needs to be done to make managers aware of the current and developing threats, and assistance is needed to ensure that companies have an adequate security and resilience policy in place.

Mr. Oliver Hoare, CEO of Dysart Solutions Ltd., now employed by an SME is involved in providing training and support of a holistic cyber security nature and is able to draw on his 20-years experience of government. Being previously based in the Cabinet Office and dealing with information assurance and cyber security, and more generally, security policy framework, has provided insights into how government and industry can work together. More recently he has been involved in cyber security initiatives including major sporting events (the 2012 London Olympic Games) and the Protective Marking Scheme. He is at present extensively involved in work overseas and is undertaking a lot of work with a US company

that specializes in detecting and dealing with advanced persistent threats. Key areas of interest include cyber insurance; cyber security and the retail sector; cyber security and the Olympic games; digital broadcasts and risk; leveraging national capability; the Cyber Essentials Scheme (comparison of the UK and Korea); the political landscape and how it is changing in relation to risk threats; and countries of immediate interest include Korea and Japan.

Mr. Mike Humphrey, Head of Information Assurance and Accreditation at the National Crime Agency, outlined the risk associated with information sharing and talked about the various challenges associated with information security. He reinforced the need expressed by others a mechanism for assistance to be provided for cyber users and explained how the National Crime Agency was structured to deal with requirements and the regulatory conditions under which it functions. Insights were provided as to why certain types of crime were undertaken and why it is important not just to prosecute but also disrupt a criminal organizational business model highlighting that many cyber criminals operate from overseas to exploit differing levels of legislation. Focussing on small business, if criminals or hackers are able to take down their website, this could have severe ramifications for the SME. It may delay the company receiving orders or promoting its products and services, and could, witness a business exiting the market due to lost business so it is important to recognise it is not just large corporates who are at risk but the smaller enterprises as well.

It is important to realize that the different categories of crime are linked, for example, digital crime is linked with economic crime that is linked with border crime and so on. Those involved in cyber security need to be aware that more attention needs to be given to adequate risk assessment and factor into the risk equation human as well as technological considerations. Organizations also need to take more responsibility for ensuring that adequate organizational structures are in place to allow individual managers to assume responsibility for risk rather than think it is for someone else. The digital age means managers must be aware of the risks associated with on line business and think about it in the same way as other business risks such as finance, health and safety etc. The National Crime Agency have industry liaison officers in place and officers based abroad to facilitate communication, information sharing and cooperation with counterparts in law enforcement. What is clear is that new ways of working and cooperating will be required if that is cyber crime is to be managed adequately. This means that trust based relationships will need to be formed that are sustainable and which are underpinned by advice and assistance, and which counteracts the sometimes present silo mentality.

EurIng Dr. Richard Overill, King's College London, provided a brief overview of cyber security in the context of international security, and talked about his interests in digital forensics, encryption, digital evidence, and the use of mathematical modelling and statistical analysis, and how it can provide insights into cyber crime and also, allow policy makers to impose legal measures to assist the police in their investigations. Research has been undertaken vis-a-vis cyber crime in the UK and Hong Kong, and it is possible to broaden the scope of the research to include Korea. Work currently being undertaken includes: the source of various computer code used in malware; DDoS detection and mitigation; statistical analysis of cyber crime to determine the different modes of operation; and studies that highlight how specific technologies are susceptible to cyber attack. King's College London is unique in the

sense that it has a War Studies Department and academics are engaged in various types of collaborative research relating to cyber-war policy and strategy

Dr. Yang-Im Lee, University of Westminster, and Dr Peter Trim (Birkbeck, University of London) work closely together in the area of cyber security management. They have undertaken research involving risk, compliance and governance, and are involved in social science research that focuses on culture and cross-cultural issues; and organizational learning, group work and cooperation. They are interested in how different forms of leadership model are deployed and how staff are motivated to manage change in the context of the cyber environment.

2. A brief summary of the current situation vis-à-vis the Korea-UK Cyber Security Research Network.

The Korea-UK Cyber Security Research Network is active and it is envisaged that several members of the group will travel to Korea in the new year in order to participate in the Korea-UK Cyber Security Research Workshop and other related activities. They will also be involved in the Korea-UK Cyber Security Research Workshop that will be held in London in Spring 2015. Aspects of their work will also appear in the report to be submitted to both governments, which will be produced in March, 2015. In order to simplify matters, an inner group of members and an outer group of members was established for 2014 to 2015, and at present the inner group is participating in the meetings and being included in the email exchanges.

3. Matters arising from the report by Trim, P.R.J., and H.Y. Youm (March, 2014)(Editors). *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership.* British Embassy Seoul: Republic of Korea. The report was submitted to the Korean Government and the UK Government on 18th March, 2014.

No matters arising were evident. Notwithstanding, the UK Cyber Security Research Network Group in their discussions covered many of the points and recommendations cited in the report. The outcome of the discussions has been written up in point form by Dr. Trim and will be placed in context and will appear in the forthcoming report for the two governments.

Each member of the UK Cyber Security Research Network Group has been asked to consider producing a short paper for inclusion in the forthcoming report for the two governments. The objective is to include in the report a range of material relating to cyber security and security and resilience more generally, that highlights work being currently undertaken and which is of interest to Korean cyber security experts. It is envisaged that each paper or article will have at least one recommendation.

4. The 2014 to 2015 Korea-UK Cyber Security Research Network.

Budget.
The grant won for the UK group was £9,500.

Workshops and meetings.
It is envisaged that two meetings of the UK Cyber Security Research Network Group will be held and up to four members of the group will attend the Korea-UK Cyber

Security Research Network Workshop in Seoul and a larger number is likely to attend the Korea-UK Cyber Security Research Network Workshop in London. It is proposed that the UK Cyber Security Research Network Group will meet again in February, 2015.

Final report.
A final report will be produced in March, 2015 and circulated to various people and placed on the world wide web.

5. Outline programme for the two workshops (Seoul and London, 2015).

First workshop Seoul: possibly 4 people from the UK to attend.
The draft itinerary for the UK delegation/speakers:
17/1/2015: (Saturday) depart from the UK to Seoul (Incheon airport).
18/1/2015 (Sunday): arrive at Incheon airport at 8:00 am (?)/free time.
19/1/2015 (Monday): Korea-UK workshop on Cyber Security at COEX meeting room.
20/1/2015 (Tuesday): site visits plus wrap-up meeting and dinner.
21/1/2015: (Wednesday): UK delegation/speakers depart (10:30am).
Immediate action: to discuss and agree the themes/speakers with Professor Youm.

Second workshop London: possibly 3 to 5 people from Korea to attend.
Final wrap-up meeting at BIS Conference Centre. (Closed audience: 3 to 5 Korean people and 10 invited UK participants). Proposed date(s): 2nd and/or 3rd March, 2015.

With reference to point 5, discussions are underway between Dr. Trim and Professor Youm regarding the content and the structure of the workshops in Seoul and London, and related activity. Dr. Trim and Professor Youm are in close contact with Hyeyoung Kim at the British Embassy Seoul, and are being greatly assisted by her.

6. Any other business

Once the minutes of the meeting were approved, they would be circulated to Professor Youm and Hyeyoung Kim.

The date and times of future meetings will be confirmed in due course.

Appendix 5: A list of the four main cyber security research workshops funded during the period 2013 to 2015.

The First Korea-UK Cyber Security Research Workshop Programme at the British Embassy in Seoul on 16th October, 2013.

9:00 - 09:30	Registration (British Embassy Seoul)
Opening session (E.J. Kim)	
09:30 - 09:40	· Greeting, Gareth Davies, Head of Science and Innovation, British Embassy Seoul. · Welcome and the objective of the workshop and future activities, Peter Trim, Birkbeck, University of London, UK and Heung Youl Youm, Soonchunhyang University, Korea.
09:40 – 10:00	· Welcome, Jamie Saunders, FCO, UK. · Congratulatory remarks, J.M. Park, MSIP Director General, Ministry of Science, ICT and Future Planning, Korea.
10:00 – 10:10	· Photo Session
Session A < National strategy & policy in cyber security and privacy > Moderator : Peter Trim	
10:10 - 11:00	· Policy and strategy on cyber and privacy in the UK: A programme for change?, Nigel Jones, Cranfield University, UK. · The policies for promoting the cyber security industry, Soon Tae Park, KISA , Korea. · Discussion.
11:00-11:20	Coffee break
Session B < Cyber security & privacy landscapes (e.g., cyber threats and vulnerabilities) > Moderator : K.H. Chung	
11:20 - 12:10	· Consumerisation and information sharing: What happens when it goes wrong?, Mike Humphrey, National Crime Agency, UK. · Recent cyber security and privacy landscapes in Korea: Challenges and responses?, Heung Youl Youm, Soonchunhyang University, Korea. · Discussion
12:10 - 14:00	**Networking lunch**

Session C < Best practices for SMEs > **Moderator : Godfrey Gaston**	
14:00-14:50	· Cyber security culture and ways to improve security management, Peter Trim, Birkbeck, University of London, UK. · Personal information protection and supportive policy for SME in Korea, Kim Du-Hyun, NIA, Korea. · Discussion
14:50-15:10	Coffee break
Session D < Academic and Business relationships > **Moderator : B.S. Kim**	
15:10 - 16:00	· A model for ensuring a win-win situation in academic-business partnerships, Godfrey Gaston, Centre for Secure Information Technologies (CSIT), Queen's University Belfast, UK. · Korea-UK ICT security tech R&D collaboration case study: ETRI and CSIT, Dooho Choi, Electronics and Telecommunications Research Institute (ETRI), Korea. · Discussion.
Session E < Education/training > **Moderator : Nigel Jones**	
16:00 – 16:50	· Education and training for improving cyber security within organizations, Peter Trim, Birkbeck, University of London, UK; Nigel Jones, Cranfield University, UK; Mike Humphrey, National Crime Agency, UK; Godfrey Gaston, Queen's University Belfast, UK; and David Upton; Oxford University, UK. · Education and training for cyber security in Korea, Yoonsoo Lee, KISA, Korea. · Discussion
Wrap-up <Establishing future collaboration> **Moderators: Peter Trim and Heung Youl Youm**	
16:50 - 17:20	Workshop conclusion and ending remarks

The Second Korea-UK Cyber Security Research Workshop Programme at Birkbeck, University of London on 21st March, 2014.

9:00 - 09:30	**Registration** (Room B30, Birkbeck,University of London, Malet Street, London. WC1E 7HX)**.**
Opening	
09:30 - 09:35	▪ Welcome, the objective of the workshop and future activities, Peter Trim (Co-chairman) ▪ Congratulatory remark (I), Mike Humphrey, National Crime Agency, UK ▪ Congratulatory remark (II), Heung Youl Youm (Co-chairman) , Soonchunhyang University, Korea
09:35 – 10:00	▪ **Key note address**: Visualization and cyber security, Robert Ghanea-Hercock, BT Technology, Service and Operations (TSO), UK
10:00 – 10:10	**Photo Session**
Session A < Cybersecurity information exchange/Computer Emergency Response Team > Moderator: Heung Youl Youm	
10:10 - 11:00	▪ Sharing Information about cyber attacks: The role of WARPS (Warning, Advice and Reporting Points), Tony Proctor, University of Wolverhampton, UK ▪ Framework for cyber security information exchange in Korea, Jong-hyun Baek, KISA, Korea ▪ Disaster recovery management, Kevin Brear, J.P. Morgan, UK.
11:00- 11:20	**Coffee break**
Session B < Critical National Infrastructure Protection> Moderator : D.H. Park	
11:20 - 12:10	▪ Critical Network Infrastructure Protection (CNIP) in the UK, Hugh Boyes, IET and Warwick University, UK ▪ Critical Network Infrastructure Protection (CNIP) in Korea, Heung Youl Youm, Soonchunhyang University, Korea ▪ Discussion
12:10 - 13:15 13:15- 14:00	**Networking lunch** Followed by two talks: Organizational learning and simulation exercises, David Weston, Peter Trim, Birkbeck, University of London, and Yang-Im Lee, University of Westminster, UK and **Key note address**: How recent cyber attacks were dealt with in Korea, Jong-hyun Baek, Korea Internet Security Agency, Korea

Session C: Issues regarding cyber security standard collaboration **Moderator:** Mike Humphrey	
14:00-14:50	▪ A holistic approach to the development and use of cyber security standards, in response to emerging legislation and changing threats, Patrick Curry, MACCSA, UK ▪ Current issues for standardization activities (e.g. age verification, identity proofing, ISMS maturity level, ITS security), D.H. Park, Korea Cyber University/S.W. Lee, ETRI, Korea. ▪ Discussion
14:50-15:10	**Coffee break**
Session D < Table top exercise(s): > Moderators : Peter Trim and Heung Youl Youm	
15:10 - 16:30	One or more of the topics cited): (1) To establish how scenario-based training and the organizational learning concept can promote the collectivist decision-making approach to security. (2) Produce a conceptual cyber security risk communication model to facilitate incident management and business continuity planning. (3) Provide insights into how sophisticated cyber attacks are emerging and how managers can categorize these attacks and link them with organizational vulnerabilities, and implement solutions. For example, attention might be given to the cyber resilience issues affecting an organization that comes under cyber attack, focusing on both conventional attacks, e.g. of websites and data processing systems, and innovative attacks on the organization's cyber infrastructure, e.g. buildings, operational (control) systems, etc). (4) To establish measurements to let policy makers or CSOs learn about the status and competence (readiness or posture) of imminent cyber attacks.
Session E < Workshop conclusion & Ending remarks > Moderator : Peter Trim and Heung Youl Youm	
16:30 - 16:45	General discussion.

The Third Korea-UK Cyber Security Research Workshop Programme at the COEX, Seoul, 19th January, 2015.

9:00 - 09:30	· Registration (Room 403, COEX, Seoul)
Opening session **Chairman: Professor Daeha Park, The Cyber University of Korea, Korea**	
09:30 - 09:55	· Welcome remarks, Mr. Jin Bae Hong, Director, Ministry of Science, ICT and Future Planning, Korea. · Opening remarks, Mr. Gareth Davies, Head of Science and Innovation, British Embassy Seoul. · Congratulatory remarks, Dr. Kyungho Chung, Executive vice-president, Korea Internet&Security Agency (KISA), Korea.
	· Opening remarks and introduction to Korea-UK cybersecurity research network, Dr. Peter Trim, Birkbeck, University of London, UK and Professor Heung Youl Youm, Soonchunhyang University, Korea.
09:55 – 10:00	· Group photo session
Keynote **Chairman: Professor Heung Youl Youm, Soonchunhyang University, Korea**	
10:00 – 10:20	· The Korean government's IoT security roadmap, Mr. Jin Bae Hong, MISP, Korea.
Session A < Cybersecurity Information Exchange and Computer Emergency Response Team > **Moderator: Dr. Peter Trim, Birkbeck, University of London, UK.**	
10:20 - 11:40	· Cybersecurity information exchange and the role of the Computer Emergency Response Team, Mr. Patrick Curry, Director, British Business Federation Authority (BBFA) Ltd., UK. · National Computer Emergency Response Team and international cooperation, Mr. Hongsoon Jung, KISA, Korea. · Cyber risks to the critical infrastructure, Mr. Kwangtaek Youn, Symantec, Korea. · Discussion.
11:40-11:50	Coffee break
Session B < Critical National Infrastructure Protection > **Moderator: Dr. Youngwha Kim, TTA, Korea.**	

11:50 - 12:40	・The London 2012 Olympic Games: Cyber security and the critical national infrastructure, Mr. Oliver Hoare, Dysart Solutions Ltd., UK. ・Security reimagined – Time to detect, time to remediate for the advanced persistent threat, Mr. Hyunjun Kim, FireEye, Korea. ・Discussion.
12:40 - 14:00	**Lunch Break**
Session C < Issues Regarding Cyber Security Standard Collaboration > Moderator: Mr. Patrick Curry, BBFA, UK.	
14:00-14:50	・Increasing cooperation through Information sharing, Mr. Mark King, Broadsail, UK. ・How to protect telecom infrastructure effectively, Mr. TaeSun Hwang, KT (Korea Telecom), Korea. ・Discussion.
14:50-15:10	Coffee break
Session D < Academic and Business Relationships > Moderator: Dr. Jae Hoon Nah, ETRI, Korea.	
15:10 - 16:00	・Establishing sustainable working relationships in cyber security involving government, industry and academia, Dr. Peter Trim, Birkbeck, University of London, UK. ・Best practices for information security training and educational system for business, Mrs. Yoonjeong Kim, KISA Academy, Korea. ・Discussion.
Session E <Best Practices & Certification for Improving Cybersecurity Capability> Moderator: Mr. Oliver Hoare, Dysart Solutions Ltd., UK.	
16:00 – 16:50	・Cyber security and critical infrastructure capability: Priorities and the way forward, Mr. Patrick Curry, Mr. Oliver Hoare, Mr. Mark King and Dr. Peter Trim, UK. ・The Information Security Readiness Certification System in Korea, Professor Heung Youl Youm, Soonchunhyang University, Korea. ・Discussion.
Session F < Future Collaboration and Ending Remarks > Moderator: Dr. Peter Trim, Professor Heung Youl Youm	
16:50 - 17:30	・Issues for future collaboration (e.g. PKI federation and internet governance), all Korean and UK speakers. ・Workshop conclusion and ending remarks, Mrs. Hyeyoung Kim, Science and Innovation Manager/ Kevin Jenkins, First Secretary Defence & Security, British Embassy Seoul.

The Fourth Korea-UK Cyber Security Research Workshop Programme at the BIS Conference Centre, London, 23rd February, 2015.

9:00 - 09:30	· Registration (BIS Conference Centre, 1 Victoria Street, Westminster, London. SW1H 0ET).
Opening session **Chairman: Professor Dae Ha Park, The Cyber University of Korea.**	
09:30 - 09:55	· Welcome remarks, Neil Fisher, Foreign and Commonwealth Office, UK. · Congratulatory remarks, Mr. YeonHo Pang, Science & ICT Attache, Korean Embassy London.
	· Opening remarks and introduction to Korea-UK cybersecurity research network, Dr. Peter Trim, Birkbeck, University of London, UK and Professor Heung Youl Youm, Soonchunhyang University, Korea.
09:55 – 10:00	· Group photo session.
Keynote Addresses **Chairman: Dr. Peter Trim, Birkbeck, University of London, UK.**	
10:00 – 10:15 10:15 – 10:30	· Austen Okonweze, Supporting the Growth of the Cyber Security Sector, BIS, UK. · Recent Korean security policy for the financial sector, Professor Heung Youl Youm, Soonchunhyang University, Korea.
10:30 - 10:40	Coffee break
Session A < Collaboration and Cooperation in Cyber Security and Personal Information Protection> **Moderator: Mr. Robert Hall, LondonFirst, UK.**	
10:40 - 11:40	· Working within and across cultures: Insights into managing international research projects, Dr. Yang-Im Lee, University of Westminster and Dr. Peter Trim, Birkbeck, University of London, UK. · Cloud Services Security Countermeasure Criteria for Korean Personal Information Protection Act based on International and Domestic Standards, Professor Dae Ha Park, The Cyber University of Korea. · Discussion.
Session B < Critical National Infrastructure Protection and Cybersecurity Capability> **Moderator: Dr. Jae Hoon Nah, ETRI, Korea**	
11:40 - 13:00	· Reducing People-risk in Organisations, Tony Butler, Delphinitum, UK. · Protection of personally identifiable information (PII) in public clouds, Alan Shipman, Group 5 Training Limited, UK. · Korean cybersecurity capabilities for UK collaboration, Mr. Ki-Woon Lee, KISA, Korea.

	· Discussion.
13:00 - 14:00	**Lunch Break**
Session C < Cyber Security Standard Collaboration > Moderator Mr. Mark King, Broadsail, UK.	
14:00-15:00	· ISO 29115 - Entity Authentication Assurance Framework - What happens next? Mr. Patrick Curry, Director, British Business Federation Authority (BBFA) Ltd., UK. · Standardization collaboration on age verification, Dr. Jae Hoon Nah, ETRI, Korea. · Discussion.
15:00-15:10	Coffee break
Session D <PKI Federations and Olympic Cyber Security > Moderator: Mr. Pilyong Kang, KISA, Korea.	
15:10 - 16:00	· Cyber security in relation to the 2018 Winter Olympic Games in Pyoeng Chang, Oliver Hoare, Dysart Solutions Ltd, UK. · Key elements for PKI federation, Mr. Jaejung Kim, KICA, Korea. · Discussion.
Session E <Specific collaboration issues between UK and Korea> Moderator: Mr. Mike Humphrey, National Crime Agency, UK.	
16:00 – 16:50	· Trust through Certification in SME Cloud Adoption, Dmitry Organ, The Risk Advisory Group plc., UK. · The Korean information security certification, Professor Heung Youl Youm, Prof. Dae Ha Park and Mr. Jae Hoon Nah, Korea. · Discussion.
Session F < Future Collaboration and Ending Remarks > Moderators: Dr. Peter Trim and Professor Heung Youl Youm	
16:50 - 17:30	· Issues for future collaboration (e.g. internet governance and PKI federation), all Korean and UK speakers. · Workshop conclusion and ending remarks, Dr. Peter Trim, Birkbeck, University of London, UK.