# Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership

## Report Submitted to the Korean Government and the UK Government
## March, 2014

Peter Trim and Heung Youl Youm
(Editors)

# Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership

## Report Submitted to the Korean Government and the UK Government March, 2014

Peter Trim and Heung Youl Youm
(Editors)

© The individual authors

British Embassy Seoul: Republic of Korea.
March 2014.

## Dedication

This report is dedicated to those that are actively engaged in cyber security and those that are actively supporting the campaign for a cyber security profession.

## Acknowledgements

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 also like to record a special thank you to various representatives of the UK's Foreign and Commonwealth Office, and in particular Kyungah Lee and Steve Wood for their support at the outset of the project, and to Gareth Davies, Jamie Saunders and Hyeyoung Kim for their continued support once the project got under way.

In addition, we would like to record a very special thank you Eunjeoung Kim (E.J.) for the outstanding contribution she made throughout the life of the project: arranging meetings and visits; providing feedback and advice; and working at speed, continuously to ensure that the deadlines set were adhered to. We remain deeply appreciative for a job well done.

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.

Peter Trim (London) and Heung Youl Youm (Seoul).
March, 2014

**Foreword**

There is much we could say, however, we would like to quote the President of the Republic of Korea, Park Geun-hye; Korea's Foreign Minister, Yun Byung-se; and the UK's Foreign Secretary, William Hague.

> "More than four billion people still cannot enjoy the benefits of the Internet. The digital divide is a significant task that should be tackled immediately…….
>
> Cyberspace is increasingly vulnerable to security risks such as the leakage of personal data, spam and the spread of malicious code. We need to come up with global principles to prevent such things from occurring, without compromising its openness".
>
> Park Geun-hye, President of the Republic of Korea

> "Cyberspace is a place for immense possibilities and an unchartered continent of the future. To make it one of prosperity and opportunities, international cooperation is essential".
>
> Yun Byung-se, Foreign Minister of the Republic of Korea

Source: Kim Tae-gyu (2013). Park calls for digital equality, *The Korea Times*, 18th October, p.1.

> "The Internet is the heartbeat of the global economy, linking businesses that are based thousands of miles apart and constantly creating new markets, industries and technologies".
>
> William Hague, UK Foreign Secretary

Source: Kim Tae-gyu (2013). Britain against state control, *The Korea Times*, 18th October, p.4.

## Table of Contents

**Appendices**

## SECTION 1: Introduction and Background to the Research Network

### Paper 1: Challenges, issues and considerations regarding an integrated cyber security programme of co-operation between Korea and the UK

Peter R.J. Trim and Heung Youl Youm.

### Introduction

It is clear that cyber security involves many issues and that the challenges facing governments around the world are the same. The only point of divergence is that the intensity and sophistication of cyber attacks differ in terms of degree and frequency, hence policy makers and their advisors need to understand that dealing with cyber attacks is something that government representatives, seniors managers employed by both private sector and public sector organizations, academics and researchers, need to view as an international or regional problem as opposed to a national problem. Hence policy decision-makers and their advisers need to adopt a more pro-active approach with respect to counteracting cyber attacks if that is the current and future forms of cyber attack are to be dealt with in a way that protects society, the digital economy and underpins government's commitment to borderless trading. By putting adequate cyber security policies, systems and frameworks in place to deal effectively with the various forms of cyber attack, it should be possible to limit the disruption and information leakage caused. However, a great deal still needs to be done in order to ensure that when an attack does get through, as indeed some will, the defensive umbrella in place allows for a rapid recovery and that the organization attacked is able to continue functioning. By ensuring that an organization is sustainable, it should be possible to maintain the quality of life that people are used to. If we become complacent to cyber attacks and all that they represent, it will not be possible to maintain the way in which organizations function as we require, through regulation and compliance. It must also be remembered that cyber security needs to be placed within the context of governance and a relevant international regulatory framework.

It is hoped that this report will focus attention on identifying measures that need to be undertaken in order to ensure that the investment in cyber security to date, and the anticipated future investment, are sufficient to reinforce and make known, what additional investment in cyber security is needed in order to ensure that current and future unknowns, are contained when actions manifest in an impact of some kind. In order that the most efficient use is made of past, current and future investment in cyber security, it is necessary to form workable partnership arrangements between individual nation states. If this is achieved, then it will be (i) possible to share information about the nature and type of cyber attack being unleased more effectively than is the case at present, and thus put in place defences to deal with such attacks; (ii) it will be possible to establish joint research programmes to study various aspects of technology oriented and behavioural patterns associated with organized criminal groups and terrorist organizations; and (iii) it will be possible to develop joint security products and services for all industries.

The report makes reference to the cyber security project itself, its purpose and background. The indicators of success/impact are cited and various recommendations are provided that if addressed, should decrease the risk of cyber attacks manifesting and/or penetrating the defensive umbrella. The term defensive umbrella, should be viewed from the objective of

making both Korea and the UK safe places in which to conduct business and attract inward investment from a range of sources. By providing a means whereby the Korea-UK cyber security research network can be sustained, it will be possible for the individual members of the network to continue their open dialogue with their group and also with their counterparts abroad. Furthermore, they will be able to draw on the cyber security knowledge of their personal contacts and consult and recommend various relevant, published reports, academic journal articles and books to a wider audience.

**Background**

The rationale, aims and objectives of the research network can be explained as follows:

> A co-funded, Anglo-Korean government approved university-business project entitled *Increasing Cyber Security Provision in the UK and Korea: Identifying Market Opportunities for SME's*; has been established 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 countries. A conceptual cyber security risk communication model will be produced to facilitate incident management and business continuity planning in SME's in the UK and Korea. In addition, knowledge transfer will occur between UK and Korean companies and this will result in enhanced cyber security technology being marketed.
>
> The two project leaders, Dr. Peter Trim, Birkbeck, University of London and Professor Heung Youl Youm, Soon Chun Hyang University, are each responsible for organizing a research network in their respective countries that will provide insights into how sophisticated cyber attacks are emerging and how managers in SME's can categorize these attacks and link them with organizational vulnerabilities, and implement solutions. To assist them in this process, two UK-Korea Cyber Security Workshops are planned. The first will be in Seoul, in October 2013 and the second will be in London, in March 2014. The workshops represent the mechanism through which the outputs will be delivered and will facilitate continued co-operation between the research network members by enhancing communication.
>
> The academics and practitioners in the research network will disseminate their research findings (case studies, reports, workshop/conference papers and journal articles) among people in education and training in the UK and Korea so that security provision is enhanced, and staff in small and medium sized enterprises are better able to deal with the cyber attacks launched against their organization. By working closely with organizations in both the public and private sectors, managers will acquire a better appreciation of risk management and will increase cyber security training provision. A report outlining how government, academia and industry can increase cyber security provision will be presented to both the UK government and the Korean government.

During the duration of the project, attention was given to the scale and support that needed to be provided to small and medium sized enterprises (SME’s) vis-à-vis cyber security and more generally, the way in which government could work more effectively with staff in various

types of organizations throughout the public and privates sectors. The members of the Cyber Security Research Network, which was divided into a Korean group and a UK group, held various networks meeting in Seoul and London, respectively.

Following a number of meetings of each of the research groups in their respective countries, the UK Cyber Security Research Group visited Korea in October 2013. The UK group was composed of Godfrey Gaston (Queen's University Belfast); Mike Humphrey (National Crime Agency); Nigel Jones (Cranfield University); Peter Trim (Birkbeck, University of London); and David Upton (Oxford University). All the group members provided a talk at the First Korea-UK Cyber Security Research Workshop at the British Embassy in Seoul on 16th October, 2013. Members of the Korea group that provided a talk at the workshop were: Soon Tae Park and Yoonsoo Lee (Korea Internet & Security Agency (KISA)); Kim Du-Hyun (National Information Society Agency (NIA)); Dooho Choi (Electronics and Telecommunications Research Institute (ETRI); and Heung Youl Youm (Soonchunhyang University). The workshop programme is outlined in Appendix 1. On 15th October, 2013, the UK delegation was invited to meet and talk with Korean cyber security representatives of the Police Cyber Terror Response Centre (CTRC); the National Information Society Agency (NIA); and the Korea Internet Security Agency (KISA). After the cyber security workshop, the UK delegation attended the reception at the 3rd Cyber Space Conference at the COEX in Seoul and then attended the main conference on the Thursday and Friday.

**The purpose of the project**

The purpose of the project was 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. In order to achieve this, the organizational visits, workshop presentations, networking discussions, and meetings at the 3rd Cyber Space Conference, allowed attention to be given to establishing how cyber security solutions and services could be arrived at and/or indicate where possible solutions would originate from. Also of importance was the ability to identify problems; strengthen existing UK-Korea academic relationships; and ensure that the timetable for delivery was adhered to.

As well as attention being given to how the security provision of SME's could be enhanced, it was decided to think in terms of supporting business infrastructure (e.g., the role of chambers of commerce and industry, and professional associations for example), and to place the relationship building process in a wider context, namely how government was to achieve its national cyber security objectives in the context of its own cyber security strategy and the initiatives undertaken by friendly governments. In the context of the project, this can be defined at the Korean government and the UK government working together and forming a sustainable partnership through university and organizational links.

The group members were aware of the sensitivity of the nature of the project and did not ask for or seek sensitive or confidential data and information, as this would militate against the formation of developing a sustainable working relationship or set of relationships. It was suggested that once the network was established and functional, that in the long-term, attention could be given to having additional workshops in the area of the "creative economy" and in particular, establishing and implementing procedures relating to best

practice relating to personal information transfer across borders; security and privacy issues for SMEs in Korea and the UK; intelligence and information sharing where appropriate; insights into current and evolving types of cybercrime and cyber security opportunities; and knowledge and guidance as to how cultural practices in Korea and the UK differed.

In addition to the points above, it was considered essential to map the various links, relationships and procedures in both countries in order to establish the differences and similarities relating to organizing and dealing with cyber crime prevention in both countries. An area of focus was national cyber security strategy and how this could be placed in an international context in order to promote working relations between Korean and UK cyber security experts. By identifying how collaboration between Korea and the UK could progress, it would be possible to consider the immediate national security issues and the immediate economic development issues, and to identify gaps that could be turned into opportunities (technological breakthroughs manifesting in new products and services). What was given some attention, was the role that university researchers could play in the development of cyber security training (short courses) and educational provision (courses for business executives and postgraduate students).

The main deliverable of the project was a final report, which was to be distributed to representatives of the Korean government and the UK government; and senior managers in SME's and a range of organizations operating in the public and private sectors, as well as staff at various universities. Most importantly, it was considered that the recommendations outlined in the report and which were grounded in or based on evidence unearthed during the life of the project, would make explicit how the various stakeholders (government, industry and academia) would integrate their efforts in order to support current and future cyber security initiatives that were deemed of importance by the Korean and UK governments and their advisors.

**Actions identified and made explicit**

The members of the network consider that it is appropriate and relevant to establish a formal arrangement, funded appropriately, to act as a focal point to manage and promote cyber security relations between Korea and the UK. By doing so, it was envisaged that the activities of the research network would take forward a number of the initiatives discussed and set out at the highly informative and successful 3rd Cyber Space Conference, which was held in Seoul on 17$^{th}$ and 18$^{th}$ October, 2013. By establishing an active Korea-UK cyber security research network, relevant cyber security stakeholders and interested parties in Korea and the UK, would, through Dr. Peter Trim and Professor Youm, be able to keep in contact with appropriate staff and develop a number of research initiatives that were considered appropriate by both governments. Indeed, by integrating further the efforts of government, industry and academia, through sharing information and best practice, it would be possible to engage in research of a strategic, tactical and operational nature that reinforced work undertaken by other interested parties in the area of cyber security.

It was generally agreed that more attention needs to be given to establishing how large, medium and small sized organizations, throughout the public and private sectors, can share knowledge, experience and solutions in the area of counteracting cyber attacks. This may have the added advantage of identifying market opportunities that could be exploited by companies that were encouraged to collaborate. For example, during the project, it was

discovered that companies from Korea and the UK, had distinct competencies in the area of information security and that a range of additional security products could be developed through collaboration on an industry by industry basis.

Bearing the above in mind, it was considered important that opportunities were identified for researchers at Korean and UK universities to work together and again it was suggested that Dr Peter Trim and Professor Youm could initiate a process whereby joint research grant applications were developed; joint teaching initiatives in the area of cyber security and security management courses/programmes of study were devised; and collaborative projects with industry representative could be identified that bridged the industry-academia divide. In addition, it was suggested that staff and student (research) exchange programmes be devised so that working relationships between universities in both countries could be established.

As well as the many advantages of such collaboration, it was considered important that the research network, could through funding, facilitate and generate a number of sustainable international networks of cyber security researchers that would keep in touch and where necessary share information about a range of cyber related issues.

With regards to future cyber security cooperation between Korea and the UK, it was decided that it was possible to identify a number of priority areas, but it was agreed that other areas/topics could be added. The topics of immediate interest were:

computer forensics;
faulty software;
current and evolving cyber threats;
organizational vulnerabilities (eg., BYOD – Bring Your Own Device to work);
social networking and online behaviour;
second life and its ramifications;
governance and compliance;
virtual money;
trusted services;
human factors;
business and competitive intelligence;
risk management and risk analysis;
types and forms of cyber crime;
current and future industry standards;
privacy and the law;
employment law;
types and forms of certification for industry practitioners;
the role of trade associations and government bodies;
FDI (Foreign Direct Investment) and knowledge transfer;
business and organizational practices;
university-industry collaboration;
business and management theory and practice; and
cross-cultural decision-making.

In order that the research network develops in the way expected, it was suggested that work in the area of cyber security projects evolve to take into account the needs and priorities of researchers in Korea and the UK, and that the outcome of such a working relationship has to be viewed as mutually beneficial.

It was considered essential to include in the cyber security research network representatives from Korean companies that had an operational base in the UK and representatives from UK companies that had an operational base in Korea as this would help to facilitate the activities of the network and result in and underpin Korea-UK research initiatives. Dr. Trim made known that CAMIS (Centre for Advanced Management and Interdisciplinary Studies), which he is the director of, had signed a memorandum of understanding with a research group at Yonsei University in 2013 in a non-cyber security area and that this was a good example of the potential for further cooperation. It would be possible to take this a step further by securing funding that would be able to provide support for helping staff in organizations, both in Korea and the UK, to develop and maintain workable relationships outside their immediate area of activity. A mechanism for maintaining working relationships was considered a sound investment in the sense that damage caused by cyber attacks could be severe enough to result in an organization exiting the market and the more robust an organization was, the better for the industry as a whole.

CAMIS, with appropriate funding, is well placed to assist organizations in Korea and the UK to network and interact with individuals in government, industry and academia. The CAMIS newsletter has a circulation of over 700 and is read by an international audience. The CAMIS workshops had over the years been focused on a range of issues related to security and it was considered that as CAMIS was an independent entity, it would be well placed to serve the interests of those intent on building Korean-UK relations in the area of cyber security and other important and related areas.

**The deliverables**

The deliverables associated with the project are outlined below.

A report outlining how government, academia and industry can increase cyber security provision and which contained case studies/best practice (Korea and the UK) in cyber security training and educational provision. The objective being to make managers in SME's aware of the increasing number of cyber attacks; outline a conceptual cyber security risk communication model that would facilitate incident management and business continuity planning in SME's in the UK and Korea; incorporate an existing mapping process outlining the cyber security landscape (e.g., government agencies, trade associations, professional institutions; and provide cyber security counterintelligence guidelines and cyber security supply chain guidelines for managers in SME's; UK-Korea comparison of cyber security threats and perceived vulnerabilities. In addition, the report would list the relevant cyber security sources of published data and information in the UK and Korea; provide a brief explanation of the role that institutional and professional bodies involved in cyber security in the UK and Korea undertook; and provide a brief explanation of the role that universities involved in cyber security in the UK and Korea were known for. It was envisaged that the report would also indicate market opportunities, the key point being to outline how horizon scanning and a change in industry standards would facilitate new products/opportunities, and provide insights into market development for example. An area of increased attention was likely to be on-line shopping and information relating to trends both in the UK and Korea.

The individual sections of the report would be attributed to the contributing research members and their affiliation(s) and information would also be provided regarding the names, expertise and research areas of the individual research network group members.

Reflecting on the above, it can be noted that the indicators of success/impact were:

(1) Appreciation of risk management.
(2) An increase in 5% of cyber security experts.
(3) A 5% increase in cyber security training.
(4) Comparison of vulnerabilities in UK and Korea.
(5) Market opportunities in UK and Korea identified.

**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).

**Immediate future activity: The Korean delegation's visit to the UK in March, 2014**

A delegation of Korean cyber security experts will visit the UK in March, 2014, and will be involved in an extensive programme of activities including:

18th March, dinner/reception in London.
19th March, visit to the National Crime Agency and talk between the Korea CERT and the UK CERT.
20th March, attendance at the iMM Cyber Security Conference in London, and a representative from the delegation will provide a talk at the conference.
21st March, attendance at the Second Korea-UK Cyber Security Research Workshop at Birkbeck, University of London.

While in the UK, the Korean delegation will discuss a number of topics with their UK counterparts including:

(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 companies 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. Possibly in the areas of: (i) incident management; (ii) human behaviour, trust and culture related factors; (iii) the link between privacy and technology; (iv) EU privacy and legislation; (v) cooperation involving companies, universities and government; (vi) KISA and CPNI and their scope and objectives; (vii) the role of CERTS and WARPS and organizations such as Get Safe On Line; (viii) the EU-ASEAN cyber security context; (ix) governance inside government; (x) the development of trust based relationships across industry and information sharing; (xi) the notion of the cyber community; (xii) identifying the impact of cyber security research projects; (xiii) how a capability audit would benefit funders of research projects; (xiv) the development of risk management models; (xv) the development of an all-embracing trust model and supply chain management; (xvi) access control and authentication; and (xv) interoperability.
(7) Ways in which to receive support from industry.

**Paper 2: Summary of the First Korea-UK Cyber Security research Workshop.**
Heung Youl Youm and Peter R.J. Trim.

## The objectives of the workshop

The workshop objectives included the following but were not confined to them only:

(1) Sharing information about landscapes, activities and policies in cyber security and privacy.
(2) Strengthening academic and business relationships and establishing synergy among companies involved in cyber security work in the cyber security area.
(3) Providing solutions to protect against cyber attacks and/or providing information where solutions are likely to come from for SMEs.
(4) Identifying problems and ensuring that the timetable for delivery of the project adheres to the plan.

## Presentations of the workshop

The title of each presentation, the speaker(s) and the content of each talk are outlined below.

- "The objective of the workshop and future activities and collaboration" by Heung Youl Youm and Peter Trim (SCH University, Korea; and Birkbeck, University of London, UK). This presentation outlined the aims and objectives of the workshop and suggested potential areas of future collaboration for members of the Korea-UK cyber security research network.

- "A model for ensuring a win-win situation in academic-business partnership" by Godfrey Gaston (Centre for Secure Information Technologies (CSIT), Queen's University Belfast, UK).This talk outlined a model for best practice in academic and business partnerships, focusing on the approach taken by staff at the Centre for Secure Information Technologies (CSIT), Queen's University Belfast. A wide range of aspects including industry membership models, staff roles and responsibilities, team dynamics, the wider ecosystem and international links were explored. Three case studies were cited: one involved a large UK corporation, another involved a local small startup and the third featured a Korean collaborative project.

- "Cyber security culture and ways to improve security management" by Peter Trim (Birkbeck, University of London, UK). The presentation focused on a number of issues that managers are currently concerned with and highlighted the threats that are evident and which are forcing managers to adopt a new approach to risk management. Attention was given to how an organization can be made more resilient and how stakeholders can be kept informed about events through a well crafted communication strategy. Reference was made to how a collectivist approach to security can be adopted. Insights into social engineering and behavioural factors that place an organization at risk were mentioned and so too was the concept of corporate intelligence. In addition, coverage was given to how managers can work with partner organizations in order to develop a joint security approach. Current and future security issues received attention and limited attention was given to how management can devise an organizational cyber security policy that is underpinned by the organizational learning concept. Areas of best practice were also given attention.

- “Education and training for improving cyber security within organizations” by Peter Trim, Nigel Jones, Mike Humphrey, Godfrey Gaston and David Upton (respectively Birkbeck, University of London; Cranfield University; National Crime Agency; Queen's University Belfast; and Oxford University). Various insights were provided into initiatives underway that are aimed at improving cyber security training within and between organizations. Reference was made to how universities are creating and responding to market demand and how government and some business initiatives are encouraging universities to offer relevant security programmes. Several government initiatives to increase cyber security awareness and raise the cyber security skill base of the workforce were highlighted. In particular, the Cyber Security Challenge UK and a recently introduced internship programme were outlined. Attention was also given to how companies can engage with universities and colleges in a partnership context to form workable partnership arrangements. Examples were provided of how managers can utilize table top exercises and develop a research culture within an organization. In addition, examples of the potential consequences of data breaches where the boundary between home and work devices is becoming increasingly blurred was examined. It was noted that many small businesses do not have the capability, or finances, of large corporates to adequately consider or address these issues. Attention was also given to how senior managers and the board of directors should provide leadership in order to ensure that the organization developed a security ethos, and how relevant stakeholders can work with government to improve cyber security educational provision and how employers can work with educational institutions and professional organizations to ensure that the training provided, whether in-house or contracted-in, achieved the appropriate standard. Recent moves in the UK to professionalize information security practitioners was outlined and a brief mention was made of the Institute of Information Security Professionals. The move by CESG to provide a method to certify security professionals as competent in certain roles to three levels (practitioner, senior and lead) were covered and the certification bodies of which the IISP is one were referred to.

- “Policy and strategy on cyber and privacy in the UK: A programme for change?” By Nigel Jones (Cranfield University, UK). A brief overview of policy and strategy in the UK regarding cyber security and privacy was provided and the UK approach was examined through the lens of planned change. An assessment was made of a broad range of political, economic, social and technological barriers and enablers that provided successful implementation of the policy and strategy

- “Consumerisation and information sharing: What happens when it goes wrong?” By Mike Humphrey (National Crime Agency, UK). This presentation provided a snapshot into how organized criminals share information and collaborate. The insider threat was made reference to and information was provided as to how a variety of people, including the elderly and the highly educated, fall for scams (fraud/deception). Reference was also made to how the Internet is providing criminals intent on conducting scams with facilities to do so anonymously and on a large scale. Attention was given to individuals and companies and their vulnerability. With regards to consumerisation it was acknowledged that any incident that occurs can be considered complex and the more reporting-less reporting dilemma was made reference to. Additional topics that were covered were the rules governing how a work device is used and the privacy situation; who is accountable when a device is lost that contains work and personal information; and best practice guides to help organizations and their staff. The speaker also made known that if a compromise on a device used for work and home use occurs, what

happens regarding a need to forensically examine it when there is work and private data on that device?

- "Korea-UK ICT security tech R&D collaboration case study: ETRI and CSIT", by Dooho Choi (Electronics and Telecommunications Research Institute (ETRI), Korea). This talk provided an example of Korea-UK joint collaboration in a research and development (R&D) project in the area of ICT Security technologies. It was explained how ETRI (Korea) had been successfully collaborating with CSIT, Queen's University Belfast (UK) for five years (since 2009). The talk highlighted many aspects of the ETRI-CSIT/QUB joint-collaboration process and strategy.

- "Personal information protection and supportive policy for SME in Korea", by Kim Du-Hyun (National Information Society Agency (NIA), Korea). The speaker talked about personal information protection policy in relation to the Personal Information Protection Act (PIPA) that was recently been enacted in Korea. Attention was given to first, the background relating to legislate PIPA as a comprehensive law; secondly, the core principles and standards of personal information protection through processing stages; and thirdly, technical, administrative and physical measures for securing personal information. In addition, the speaker outlined several policies to ensure the establishment of a sound personal information protection culture; and gave attention to supportive policies for small and medium-sized enterprises vis-à-vis introducing main policies.

- "Recent cyber security and privacy landscapes in Korea: Challenges and responses?" By Heung Youl Youm (Soonchunhyang University, Korea). The talk focused on the major cybersecurity and privacy breach incidents in Korea that had occurred recently: 7.7 DDoS attack in 2009; the 3.4 cyber terror incident in 2011; and the 3.20 cyber terror incident in 2013. The speaker also explained how Korea had responded to these incidents.

- "The policies for promoting cyber security industry", by Soon Tae Park (Korea Internet & Security Agency (KISA), Korea). The presentation covered a number of key points including: current status; and vision and strategies of the cyber security industry.

- "Education and training for cyber security in Korea", by Yoonsoo Lee (Korea Internet & Security Agency (KISA), Korea). The presentation provided a comprehensive outline of educational and training provision in cyber security and how the provision had been mapped against known needs. Various insights were provided into the use of scenario-based educational materials that could be used to educate and train cyber security professionals. The overall approach adopted by KISA to counteract advanced persistent attacks was made known.

**Recommendation**: 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)**.**

**Paper 3: A brief introduction to the presentations of the Second Korea-UK Cyber Security Research Workshop** Peter R.J. Trim and Heung Youl Youm

Following on from first workshop, the second workshop aims to highlight how both governments can engage more strongly with organizations in the private and public sectors and provide direction and guidance as regards future cyber security policy. The topics selected for the second workshop include: visualization and cyber security; sharing information about cyber attacks; a framework for cyber security information exchange; critical national infrastructure protection in the UK and Korea; organizational learning and simulation exercises; and issues regarding cyber security standard collaboration. A number of table top exercises have been identified that will allow cyber security experts from Korea and the UK to work together in order to solve real problems. In addition, the table top exercises will allow Korean and UK cyber security specialists to think through complex subject matter and develop an understanding of how to work together in the future. The programme for the workshop is outlined in Appendix 2. A brief note will now be provided regarding the content of the second workshop.

Robert Ghanea-Hercock: "Visualization and cyber security", the focus is on how skilled cyber security experts are becoming the last line of defence in roles such as analysts in a Security Operations Centre (SOC). The skills and knowledge of analysts is clearly critical, and in short supply, so the right resources to support their efforts for network monitoring and alerting, is to be viewed from the perspective of how a more effective use can be made of analysts' time. Visual Analytics (VA) can support such individuals in detecting, investigating and assessing cyber threats. Robert will consider and review some of the primary methods for visualisation of cyber threats and discusses a specific BT developed research tool for such support.

Heung Youl Youm: "Critical Network Infrastructure Protection (CNIP) in Korea", pays attention to organizational structure, the legal background and the procedure for designating the protection of critical national infrastructure in Korea.

Jong-hyun Baek: "Framework for cyber security information exchange in Korea", outlines the framework for cyber security information exchange among relevant organizations to prevent, detect, respond to, and recover from a cyber security incident. In addition, public-to-public partnerships and private-to-private partnerships to respond to the cyber incidents are addressed.

D.H. Park/S.W.Lee: "Current issues for standardization activities", address a number of current issues such as age verification, ISMS maturity model, ITS security, etc., which might need close cooperation and collaboration between Korea and the UK vis-à-vis ISO/IEC JTC 1/SC 27 and ITU-T SG 17.

Jong-hyun Baek: "How recent cyber attacks were dealt with in Korea", addresses various types of threat that exists as well as those that are evolving. Attention is also given to how cyber security policy or activities are coordinated and implemented among relevant sectors, and some unique approaches for counteracting recent cyber threats in Korea will be made known.

Patrick Curry: "A holistic approach to the development and use of cybersecurity standards, in response to emerging legislation and changing threats". Regions, governments and industry

are increasingly collaborating to establish legislation and policies for cybersecurity. Standards organizations have to do likewise to keep pace with demand and increasingly complex threats. This talk explores collaborative initiatives to provide a more holistic and productive approach.

David Weston, Peter Trim and Yang-Im Lee: “Organizational learning and simulation exercises”, several related areas will be covered. Attention will be given to the role that organizational learning plays vis-à-vis knowledge and skill development, and how it facilitates the process of communication. As regards simulation exercises, of key interest is how threats can be modelled and risks identified, and counteracting policy devised and implemented.

Tony Proctor: “Sharing Information about cyber attacks: The role of WARPS (Warning, Advice and Reporting Points)”, will explain how managers in various organizations are liaising with each other and sharing information about cyber attacks. In addition, a number of constraints and pitfalls will be highlighted that impede the sharing of information.

Kevin Brear: “Disaster recovery management”, will outline why it is important for managers to engage in business continuity planning and why it is important to adopt an approach that assumes that the organization will at a certain point in time be subject to an attack. Having suffered an attack, it is important to implement the recovery process and guidance will be provided as to how this can be organized and managed.

Hugh Boyes: “Critical Network Infrastructure Protection CNIP) in the UK”, will look at a range of issues that take into account what advice government agencies need to provide organizations with in order that they can develop resilience based policies. In addition, reference will be made to best practice and a number of challenges will be cited including organizational, legal and skills based. Specific examples will be cited that link theory and practice.

The table top exercises have been included to allow Korean and UK cyber security experts to work on a number of current and future problems, and should provide an opportunity for the participants to understand how decisions are made, why they are made in the way they are, and how decisions are implemented. Various policy issues will be discussed and reference will be made to how problems are researched and how compromises are made. The table top exercises will foster interaction and through discussion cultural and legal challenges will be highlighted.

## SECTION 2: Cyber Security Perspectives

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

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

### Introduction

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

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

### Cyber security issues and challenges

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

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

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

about incidents/cyber attacks; and it promotes a community approach to identifying and solving problems (http://www.warp.gov.uk/background.html).

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

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

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

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

**Addressing the knowledge and skill gap**

Policy makers and their advisors are addressing the knowledge and skill gap that exists and they are to be applauded for doing so. Notwithstanding, more needs to be done and it needs to be done urgently, if that is, the more sophisticated forms of cyber attack are to be dealt with. For example, researchers based at various organizations including universities and government research centres and institutions, as well as those in the corporate and not-for-profit sectors, need to share knowledge and experience. By joining forces in order to pool specialist knowledge and expertise they will be able to produce additional cyber security knowledge that provides a more integrated and joined up approach to counteracting cyber attacks. The advantage of sharing information and/or case examples with staff in partner organizations and indeed government agencies, is that trends relating to cyber attacks can be

identified and organizational vulnerability reduced. The reason why this is important is because as the UK and Korea engage more fully in trade related activities, it is crucial to secure the business environment in which these relationships operate. If trading is disrupted, both the corporate needs and the government objectives will not be met, and turmoil may result. This raises current concerns regarding how managers undertake risk assessment and deploy risk management tools. BCS, The Chartered Institute for IT, has extended its BCS CESG Certified Professional Scheme, for Information Assurance (IA) professionals, and has launched the scheme to the UK private sector, building on what had been previously available to "government employees or those working on government contracts"(http://www.bcs.org/content/conWebDoc/51368). (For information about the UK information assurance community please consult: www.cesg.gov.uk/publications/Documents/uk_ia_community.pdf).

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

**Information sharing and organizational learning**

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

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

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

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

**Identifying the central issue**

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

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

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

How can managers ensure that an organization is resilient?

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

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

(1) Current and future security issues.

(2) Organizational issues in relation to cyber security policy.

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

**List of recommendations**

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

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

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

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

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

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

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

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

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

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

## References


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

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

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

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

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

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

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

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


## Websites


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

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

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

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

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

**Paper 5: Korean and UK perspectives: Reflecting on the past and looking forward to future cyber security collaboration in the area of training, education and research.**

Dooho Choi, Kim Du-Hyun, Godfrey Gaston, Mike Humphrey, Nigel Jones, Soon Tae Park, Peter R.J. Trim, David Upton and Heung Youl Youm.

## Introduction

This paper builds on and develops some of the points covered during the UK delegation's visit on 15th October, 2013 to the Korea Police Cyber Terror Response Centre (CTRC); the National Information Society Agency (NIA); and the Korea Internet & Security Agency (KISA). During these visits, attention was focused on a number of topics including collaboration with law enforcement agencies; the evolving nature of advanced persistent threats (APT): the analysis of cyber crime and the benefits associated with digital forensics; engagement with the public; changing behaviour in society and known and emerging cyber security problems; the emerging concept of cyber terror; the possibility that members of the general public could report crimes on-line; the scale and impact of cyber attacks and their ability to disrupt services and do greater damage; the need for intelligence and a wider appreciation of how organizations in the public and privates sectors could cooperate more effectively; the need for society to embrace more fully the role of e-government; the concept of smart government and how the public understand and accept the concept; literacy levels in society; the need for policy makers and their advisors to fully understand the trade offs that have to be made as regards investment in cyber security; involving the local population so that a resilient community was established; the role of data centres; the perception associated with social networks; emergency, recovery and support; the national cyber security framework; homeland/internal security and the need to monitor domestic websites; and information sharing and the need to foster close working relationships with companies in the private sector.

## Identifying the challenges and working in partnership

As well as understanding why governments need to adopt an integrated approach to solving cyber security problems, it has to be borne in mind that different governments may act differently when confronted with cyber related situations. Indeed, a government may adopt a collectivist approach to cyber security or a more individualistic approach, or through a common understanding, may move towards an integrated and pro-active approach that sees more shared responsibility and more accountability.

A more integrated and pro-active approach to cyber security is advocated if that is we are to see shared responsibility and more accountability vis-à-vis the implementation of cyber security initiatives. We accept that from time to time there may be conflicts of interest or indeed commercial rivalries that militate against cooperation and collaboration. Notwithstanding, the examples provided herewith provide evidence that cooperation and collaboration can do much to increase our understanding of sharing information and best practice relating to cyber security. It is pleasing to report that research undertaken in the area of cyber security management will emerge in the months ahead (Trim and Lee, Forthcoming 2014) and combined with existing literature in the field, will provide a firm basis from which new insights can be drawn and new research initiatives stimulated. In order to develop a

robust cyber security literature, it is important that collaborative international projects are undertaken that promote an integrated and collectivistic approach to the subject.

The Centre for Secure Information Technologies (CSIT), Queen's University Belfast and the Electronics and Telecommunications Research Institute (ETRI), based in Daejeon can be classified as a highly successful ICT security technology R&D collaboration. ETRI and CSIT have successfully collaborated for five years (since 2009). This win-win academic-business partnership has involved process and strategy, and can be flagged as a successful model.

Making an international collaborative successful requires resources and commitment. In addition, a distinction needs to be made between education and training, and management need to understand what skills are needed and where those skills can be acquired. In some cases, new teaching material has to be developed and new ways of imparting knowledge deployed. A range of teaching methods can be used to impart knowledge. These include scenarios, table top exercises, and public competitions such as the Cyber Security Challenge UK. Ways need to be found to secure relevant teaching material but also, ensure that it is available when needed and can be updated through time.

There is no doubt that more needs to be done in the area of personal information protection and supportive policy for SME's and this is something that can be done in an interdisciplinary or multidisciplinary way. This may mean that policy makers need to engage more widely and ensure that a comprehensive law is in place; that core principles and standards of personal information protection are guaranteed during the various processing stages; and the technical, administrative and physical measures for securing personal information are as robust as possible What needs to be advocated is a sound personal information protection culture and the supportive policies for small and medium-sized enterprises need to be made known more widely than is the case at present. Although cyber security and privacy landscapes have been defined, challenges still exist. The reason as to why this is the case is because major cyber security and privacy breach incidents may be viewed as a cyber terrorist attack, and this has connotations for how the incident should be responded to. It is clear therefore, that policy makers and their advisors, need to be committed to promoting workable policies throughout the cyber security industry. No doubt this will be made easier when a true cyber security profession emerges, however, the following question can be posed: Why do we need a cyber security profession?

In response to the question posed, it can be noted that organized criminals share information and collaborate. What police forces around the world are concerned with is that the insider threat is growing in intensity and all sections of society (individuals and organizations) are at risk from scams (fraud/deception) due to the fact that the Internet is providing criminals intent on conducting scams with facilities to do so anonymously and on a large scale. With respect to companies, vulnerability may be increasing due the effects of consumerisation which has witnessed individual employees taking into work their own device (normally a laptop computer) and when the device is compromised or lost, the personal information and/or company data on it could be retrieved by an unscrupulous individual who is intent on selling the data or using it in a harmful manner. Changes in behaviour need to be studied if that is we are to be able to project forward and anticipate how such devices are used in an everyday situation.

What is clear, is that senior management need to define better the organization's training needs vis-à-vis cyber security and the need to make a distinction between investing in

educational provision (sponsoring an employee to undertake a masters degree) and devising bespoke training sessions relating to skill enhancement. Various initiatives can be used to improve cyber security knowledge and government representatives do need to work with university staff in order to identify and develop and implement relevant cyber security programmes.

Government initiatives to increase cyber security awareness and raise the cyber security skill base of the workforce are to be applauded and the Cyber Security Challenge UK can be cited as a highly worthwhile activity that can be replicated in different ways.

Owing to the sophisticated types of cyber attack now being conducted, it is clear that managers throughout the private and public sectors need to adopt a new approach to risk management. Organizations need to be more resilient and it is advised that a well crafted risk communication strategy is in place so that all the stakeholders can be kept informed about the situation.

There is no doubt that policy change is required and that a nation's cyber security strategy needs to be well thought through and amended through time. Owing to the uncertainty that exists in this ever increasingly connected world, we can assume that cyber security and privacy will remain on the agenda for a considerable number of years. What policy makers and their advisors need to note is that when placing risk management in the context of behavioural change, a broad range of political, economic, social and technological factors, barriers and enablers need to be taken into consideration if that is, a nation's cyber security strategy is to be implemented effectively.

Bearing the above in mind, a number of recommendations can be put forward.

**List of recommendations**

**Recommendation 1**: Research needs to be undertaken into how social engineering and human behavioural factors are placing an organization at risk.

**Recommendation 2:** 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 3:** 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 4:** 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 5:** 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 6:** 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 7:** 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 8:** 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 9:** 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 10:** 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 11:** 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 12:** 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 13:** 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 14:** 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 15:** 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 16:** 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 17:** 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.

## Reference

Trim, P.R.J., and Lee, Y-I. (Forthcoming 2014). *Cyber Security Management: A Governance, Risk and Compliance Framework*. Farnham: Gower Publishing. ISBN: 978-1-4724-3209-4 (hardback) and e-book 978-1-4724-3210-0 and Kindle 978-1-4724-3211-7.

## Website

The 1st KR-UK Cyber Security Website: http://elec.sch.ac.kr/~csw/information.php

## SECTION 3: Current and Future Research

### Paper 6: Cyber security indicators of risks for SMEs

Heung Youl Youm (Editor of Recommendation ITU-T X.1208)

### Introduction

The objective of this paper is to introduce cybersecurity indicators that can be used by managers in SMEs to evaluate the posture and readiness to counteract advanced emerging threats. The text below builds on and modifies part of text of the Recommendation ITU-T X.1208, which represents a cyber security indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies [b-ITU-T X.1208].

Numerous efforts have been made to measure cyber security performance, track progress, and evaluate the impact of the use of ICTs. Examples of these sector specific indicators include the Global Cloud Computing Scorecard [b-BSA] and the security metrics published by the Center for Internet Security [b-CIS]. The cyber security indicator consists of multiple cyber security indicators combined into a risk measure describing the current risk posture of cyber security capabilities and their effectiveness as well as the efficiency of the implementation of security controls for an organization or a community. There may be two separate conditions under which a cyber security indicator of risk measure could be calculated: a self-evaluation of its cyber security capabilities or the collection of indicators calculated by some external third party organization. The indicators may be grouped according to business function(s): incident management, vulnerability management, patch management, application security, configuration management, and financial category.

### Cyber security indicators' development process

The cyber security indicator development process consists of five steps: stakeholder interest identification; goals and objectives definition; information security policies, guidelines, and procedures review; information security implementation review; and indicator selection.

- Step 1, stakeholder interest identification, involves identifying the relevant stakeholders and their interest. The primary stakeholders include the organization head, the chief information officer, the chief security officer, the information system security officer, the programme manager, the network administrator, the security engineers, and the information system support personnel. The outcome of this step includes all interests in the information security measurement. Each stakeholder may request a different set of indicators representing their view within their area of responsibility.

- Step 2, goals and objectives definition, involves identifying the goals and objectives of information security performance. They may be expressed as policies, requirements, guidelines, and guidance. The goals and objectives of the information security programme can be derived from high-level goals and objectives to support the organization's mission.

- Step 3, information security policies, guidelines, and procedures review, involve describing the details of how security controls should be implemented in organization-specific policies and procedures.

- Step 4, information security implementation review, involves reviewing existing indicators and relevant data repositories that can be used to derive new indicators.

- Step 5, indicator selection, involves selecting and developing as appropriate three types of indicators. This step involves selecting a suite of indicators that track process implementation, efficiency/effectiveness, and mission impact, and if required developing as appropriate new indicators.

**Recommendation:** 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.

## References


[b-ITU-T X.1208] Recommendation ITU-T X.1208 (2013). A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies.

[b-CIS] Center for Internet Security (2011). The CIS Security Metrics.

[b-BSA] BSA (2013). BSA Global Cloud Computing Scorecard. http://cloudscorecard.bsa.org/2013/


## Websites

ITU Website: http://www.itu.int/rec/T-REC-X.1208/en

**Paper 7: An interdisciplinary approach and framework for dealing with security breaches and organizational recovery.**

Peter R.J. Trim, Yang-Im Lee and David Weston.

## Introduction

This paper takes into account the work undertaken by Winsberg (2003), Yao et al., (2005), van der Aalst and Stahl (2011), and Thomas et al., (2013). It represents an attempt at studying the effect of an information breach, how an organization recovers from an attack and also, how management can estimate the cost of an attack in terms of resources, lost income and future investments in recovery related expenditures. We concur with the view of Thomas et al., (2013, p.2) and accept that more needs to be done with respect to developing methods and frameworks that assist the closure of the gap between academic research and professional practice. The objective of this paper is therefore, to explain how managers in an organization can estimate the cost of a potential security breach and make a case to senior management for additional resources that assist the repair and recovery stage. We assume, therefore, that a breach will occur and that by investing resources in the recovery stage, the organization will be able to continue functioning. We assume that managers within the organization will, by referencing the incident in the organization's risk register, be transparent about a potential impact and its consequences, and will share information with other organizations in the industry and elsewhere. It is our ultimate intention to produce a virtual cyber security emergency planning simulation that can train cyber security professionals and those undertaking a training and/or educational programme in the area of cyber security.

## Scenario exercises

It is our intention to add to the academic literature highlighting the importance of scenario planning, for example, Yao et al., (2005, p.1645) are right to suggest that: "Through scenarios we can prioritize the opportunities or threats and put our scarce and valuable resources to producing the greatest return". This statement has implications for management and we intend to make clear the fact that by adopting a pro-active approach to cyber security problems, management can think less about the "what if" factors and more about the contingencies that need to be in place to stop an impact having a detrimental effect on a company. Another point to take into account when engaging in modelling of any kind, is that a business intelligence system (van der Aalst and Stahl, 2011, p.11): "provides tools to analyze the performance-that is, the efficiency and effectiveness-of running business processes". It is envisaged that the research referred to in this paper will add to the body of knowledge relating to how modelling is used to facilitate decision-making in complex situations. As regards the benefits associated with simulations, Winsberg (2003, p.116) has suggested that "Simulation is a technique that begins with well-established theoretical principles, and through a carefully crafted process, creates new descriptions of the systems governed by those principles. It is a technique that, when properly used, will provide information about systems for which previous experimental Data is scare.……..Furthermore, simulations often yield sanctioned and reliable new knowledge of systems……"

Yao et al., (2005, p.1644) acknowledge that: "Simulation is probably the most widely used and the most effective method to train emergency management workers. Its fidelity can create

tensions and stimulate emotions similar to real emergency/disasters". There are two types of simulation. The real world version such as "Operation Waking Shark 2" (where UK banks were subject to a simulated attack) and the type of simulation we shall do using, the petri-nets where we attempt to model certain aspects of the information security process. A virtual simulation has a number of advantages associated with it, for example, according to Yao et al., (2005, pp.1644-1645) it can be considered (i) flexible (various emergency/disaster situations can be incorporated); (ii) easy to deliver (those involved can be based anywhere and only need a personal computer, to be connected to the Internet, and a groupware server package); (iii) promote collaborative learning, as the on-line learning environment can facilitate, through interaction, deep thinking, as well as critical and creative thinking.

## Theoretical framework and conceptual approach

The focus of attention is how managers in an organization establish that a potential cyber attack launched on an organization will cause harm and how resources for the recovery period can be committed so that the organization is able to carry out a full repair and continue in business. We assume that the impact on the organization is insufficient to put it out of business for a long period of time and assume that the organization will be fully operational within 24 hours. Should the breach be more harmful than expected, it is envisaged that the company will be unable to operate for 48 hours; and if it is considered a really devastating attack, the company will be unable to trade for 36 hours or longer. From a financial point of view, we estimate that the cost of not operating for 24 hours (wages, insurance, lost business for example) is referred to as LB (loss in business) and denoted as LB-1, and for subsequent days is LB-2, LB-3 etc. If the cost of a data breach is £100 per record, then if 1,000 records are effected, the cost would be 1,000 x £100 = £100,000 times 2 days represents £200,000 and three days would represent £300,000. This cost is not we consider unreasonable although we accept that it is higher than other estimates reported (House of Commons, 2012, p.6).

We accept that research related to recovery and restoration underpins resilience planning (Thomas et al., 2013, p.9) and it is our intention to provide an interactive framework so that managers within an organization communicate with each other in order to rectify a problem as soon as possible. For example, we have used the following weighting factor: c (communication) is excellent and rated C1. When communication is poor, we assume that there is a 24 hour delay in a message being transmitted so therefore, C+24, is represented by C+0.24 (weighting factor) and for a 48 hours delay we use C+0.48 and for three days we use C+0.60 for example. If we accept that cyber attacks are increasing in intensity and sophistication, it is possible to include in the equation an extra element, namely the cost of buying in expertise and assistance. For example, a 'light' impact which causes limited disruption means that the organization's cyber security defences are reasonably robust, however, a devastating impact allows us to assume that the organization's cyber security defence system is ineffective in which case the in-house cyber security knowledge and capability is deemed to be poor and the company has to buy in knowledge and expertise from specialist providers. We denote this in the following way: CSP (cyber security provision) can be rated as poor, adequate or satisfactory. This can be interpreted at levels, for example, CSP 3(poor) and a high need represents a weighting factor of 0.3; CSP 2 (adequate) represents a weighting of 0.2; and CSP 1 (satisfactory) represents a weighting of 0.1. It is possible to quantify these weightings in terms of cost: poor represents an immediate investment in cyber

security services of £75,000; adequate represents an immediate investment in cyber security services of £50,000; and satisfactory represents an immediate investment in cyber security services of £25,000.

With reference to the case example outlined below, we can assume the reputational damage to the company was 15% of its share value. Therefore, we need to include in the above equation a weighting factor of 0.15 loss in company value which can be interpreted as a multiplier of 0.15. Should this be the case, it is possible that shareholders will divest their shares in the company because they consider that the company's shares will deteriorate further. Hence we assume that one shareholder will sell their shares in the company and as a result, the share price will fall by another 5 per cent. We include this in the calculation as an additional multiplier of 0.05. So reputational damage is estimated at 20% of the share value of the company or 0.20.

As regards quantifying the share value, it can be noted that the day before the incident the share price of the company stood at £20; therefore, on day 1 of the incident, the share value represented £17 and day 2 witnessed a decrease of an additional 5%, so the actual value of the shares would be £16.15 each representing a decrease of £3.85 or 19.25% from the day before the incident.

Owing to the fact that companies do not operate in isolation and have a number of interdependent relationships with other companies, and are part of a network of organizations, it can be assumed that there is a risk that the company that has sustained a cyber attack will lose future business as customer organizations consider that the staff in the company are untrustworthy if they do not communicate the depth of the problem at the earliest opportunity. For example, if on day one management within the company attacked keep quiet (do not inform customer organizations, financiers (banks) and suppliers for example), the risk associated with these stakeholder organizations terminating business links with the company is considered to be low (e.g., a weighing of 0.10 is assigned). However, once rumours spread or matters become public the risk that the stakeholder organizations will terminate business with the affected company increases from low to medium risk (e.g., 2 to 3 days and a weighting of 0.2 to 0.3). By day 4 a high risk is recorded. From day four onwards a weighting of 0.4 is recorded because it is assumed that after day 4 the risk will become constant because it is not in the interest of anybody to terminate the business relationship by then.

**Case example. The branching or cascading effect.**

The IT Manager, had discovered that the company's marketing data base had been penetrated by a competitor and that staff in the competitor organization had been stealing data from the company. This was not unusual because a report in a national newspaper had indicated several cases of hacking in association with customer client lists. In some cases, it was the result of insider action. For example, in one case, two employees working for the same company had taken a manager's password and entered and downloaded sensitive company data from one of the subsidiary organizations working in the area of government contracts and the same company had been subject to several hacking attacks from a private company that was known to be stealing sensitive data for resale.

A competitor had also been attacked at some stage or been associated with one or several

attacks, and had started a rumour about the market leader resulting in the company's market share value falling by 15% in a single day. Following an internal inquiry, it was clear that the data that was hacked related to:

1. data regarding suppliers (e.g., types of contract awarded, penalty clauses and prices paid for example);
2. information about the company's new product development process (e.g., a specific 3D printing technology and intellectual property); and
3. information about the online customer-finance department payment system.

It seemed that large blocks of data relating to existing customers had been obtained (so the competitor could offer better price deals) and establish what type of risk was involved (e.g., this would result in improved risk assessment and risk analysis). In addition, the data obtained relating to the company's new product development process would allow the competitor to circumvent the company's main patent and/or identify the next generation of the technology/application. An internal investigation had also unearthed the fact that some staff had been actively involved in exchanging information with unknown individuals on social websites and as a result two junior members of staff in the organization's design department had been enticed into giving away sensitive data.

The inquiry undertaken by senior managers and the corporate security team within the organization, revealed that the company's website had been infected with malware and those downloading a company brochure had had their details sent secretly to the competitor so potential customers could be easily targeted. This was most disturbing and it was necessary for the legal team to be consulted vis-à-vis possible legal action against the company. Three months prior to this set of events, the IT manager had been asked to undertake a security review of the company's computer systems and networks and an internal report, sent to the company's board had indicated that:

> "The IT manager had been asked to undertake an audit of the company's computer system and network but was reluctant to talk with staff in other departments (especially marketing and finance) because they could not understand the technical aspects of the proposed work. Several influential and knowledgeable people had been excluded from the work because they were either disliked by the IT manager or were thought to have limited intellectual capability and were thought not to be able to understand what was going on. This being the case, it was thought that some staff would not be able to contribute to the study.
>
> On one occasion, the marketing research manager was required to purchase data from an outside market research agency but refused to inform the IT manager about where the data was stored as they were not on speaking terms. It is believed the data was stored with a cloud provider but no record existed of what data or indeed other company data was stored in the cloud".

Additional evidence of mismanagement was also outlined in the report:

> "The Marketing Manager informed his boss, the Marketing Director, that one of the company's suppliers, had informed him, via their Managing Director, that they had heard that they were offering their top suppliers (those with 20% of their business (category A supplier)) a financial incentive to lower costs and gain more

business. This was a surprise to the Marketing Manager because this had only been discussed internally by several senior managers, the Marketing Director and the Finance Director. It seems that either one of the category A suppliers had leaked the information or the teleconferencing facility had been hacked into and rumours circulated for a deliberate reason".

The report continued:

> "This sensitive information or the ability of other suppliers to influence negotiations, was crucial as there was a shakeout in the industry and price cutting had taken hold. The effect would possibly be that lower prices would have to be set; profit margins would be lower, and more emphasis would be placed on promotion and advertising to gain more customers to offset the reduced profitability".

The minutes of a meeting held to discuss the findings of the report suggested that:

> "The consequences for the marketing department were:
> confidential and sensitive data had already been leaked;
> once prices fell it would be difficult to increase them again;
> the public relations department would have to work harder and faster, and would have to embrace digital marketing campaigns to get the appropriate message out to customers and end users faster.
>
> The implications for security were:
> either somebody within the company or somebody within a supplier organization was leaking information;
> the company's marketing data base had been penetrated;
> company passwords had been intercepted;
> a contractor may have stolen and sold sensitive data;
> company representatives or supplier representatives had attended a venue that was electronically bugged;
> a third party (bank) may have released information or a wholesaler or retailer may have done so; and
> a competitor may have deliberately started a rumour to gain insights and information about the company and its relationships with it suppliers".

In addition, those attending the meeting that had discussed the issues and challenges resulting were convinced that:

> "A new information security policy and strategy was needed.
> A risk manager needed to be appointed.
> A risk mitigation strategy was needed.
> The company needed to establish a risk register.
> A new model of risk management was needed.
> The marketing supplier data base needed to be patched".

The report made known the following:

> "It became clear from a board meeting held earlier in the month that the initial report had raised concerns among senior management with respect to how the

> scenario would unfold, and also, how mechanisms could be put in place to produce a receptive and sympathetic organizational culture that resulted in cyber security management processes being implemented that would change the organizational culture for the better. The following question had been posed: How would the scenario play out?"

The head of corporate security had stated at the time:

> "Some of the actions outlined will in actual fact have a very negative impact on the company. What worries me more than anything, is how can we square the marketing situation and ensure that the security consequences do not snowball out of control".

A background company report had been produced one year earlier and had made interesting reading:

> "A small company with 50 employees and 5 directors. Managing Director, Marketing Director, Finance Director, Human Resource Management Director and Technology Director. There was a marketing manager, a marketing research manager, a marketing data base manager, a finance manager, an IT manager, a personnel manager, a technology manager and a research and development manager. The main workforce was employed in marketing and sales work. Immediate problems facing the company were:
>
> *Known threats*
>
> Two non-information security threats were: competitor companies were increasing their market share by (1) introducing new products (4 in the last 12 months) and (2) price cutting (which was attracting price sensitive customers).
>
> *Unknown threats*
>
> A criminal group had attempted to hack directly into the company's bank account to steal money from the company. A son of one of the mangers was downloading games from the Internet on his father's laptop computer which the manager used to take to work and download files and then take them home to work on at the weekend.
>
> A new cleaning company had been hired and one of the cleaners had been paid by a competitor to try and steal a data stick from the company and other information (eg., financial data reports and design work) that was left openly available and unguarded by staff after they finished work for the day.
>
> As well as this, the company was facing a law suit over non-payment of an account, because they said they had not received delivery of a component. When looked into, it was discovered that the component had been signed for by somebody within the company, but the signature did not match a current employee. It was possibly a casual worker employed by the company during a temporary period of high demand and the person(s) no longer worked at the

company. News of this had got out and some existing customers had not renewed their business contracts (e.g., reputational damage).

The marketing director and the finance director had been in discussions with a potential collaborator and had mistakenly provided them (via an email) with the blue print of a new technology the company was developing. The company concerned said that they had deleted the material as a matter of policy but this could not be verified.

It was known that one of the company's suppliers was regularly being subject to power shortages and the electricity supply to the company was disrupted two to three times per month. On one occasion the product produced and shipped to the company was faulty and this had raised concerns that the supplier was not carrying out quality checks. But the company in question had not invested in sufficient quality control (both internally (products made or assembled in-house) and externally (those bought in from external suppliers).

Owing to the fact that the company's sales were declining and the profit margins were being squeezed, rumours had started to surface that the company would go bust and because of this two experienced staff members had left the company and taken up work with other companies. They had taken knowledge about the company and its management procedures with them.

The company's information security system was dated and the manuals relating to the system had been misplaced.

The finance director and his staff undertook risk management but did not talk with staff in other departments. The risk analysis model was statistical in nature and was not that well understand by some managers.

Company staff had not adhered to any industry standard and managed as they considered relevant. There was an ad hoc approach to problem solving and the common message was: "If it is okay leave it. If it is broken fix it. Do not fix it until it is broken".

The IT manager had read about the cloud and said that the company should outsource to a cloud provider the human resource management capability of the company. It was reported that the personal records of staff may be at risk and then staff and the organization would be vulnerable. The IT manager said it should be okay because the cloud provider could take responsibility for managing the situation and they must be responsible for everybody's data".

**Recommendation:** 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.

**A framework for information security modelling**

A Petri net is a mathematical modelling tool that has a simple graphical representation. Within the context of security Petri nets have been used in diverse number of ways, ranging

from modelling of cyber-physical attacks on smart grids (Chen et al., 2011), to formal verification of security policies (Huang and Kirchner (2011). We propose to build an information security framework using Petri nets and we provide herewith a brief description of Petri nets before we introduce our framework.

*A brief introduction to Petri nets*

A Petri net can be conveniently described using its graphical representation (van der Aalst and Stahl (2011). Consider the simple Petri net is shown in Figure 1. The circles denote *places*, inside some of the places there are dots, these are denoted *tokens*. Taken together, the places and the tokens represent the *state* of the Petri net. The rectangles denote *transitions*; it is through the actions of these transitions that the Petri net state can evolve.

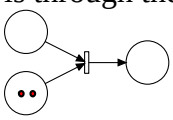


Figure 1 A simple Petri net

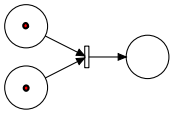
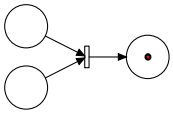


Figure 2 (a) An active transition



(b) Petri net state after the transition has fired

The arcs in the net are directed (they have arrows showing their direction) and these arcs only join a place to a transition (and vice versa). For each transition, we distinguish between places that are connected to it with arcs that are entering the transition (input places) and places connected with arcs exiting the transition (output places). A transition that has at least one token in each of its input places may then *fire*. Firing a transition simply means subtracting one token from each of its input places and adding one token to each of its output places (Figure 2).

From this simple local update rule sophisticated models may be built, which can model processes that involve concurrency and synchronization. However, there are limitations and a variety of extensions to the basic Petri net have been proposed. For our purpose, we propose to build the framework using a *timed* and *coloured* Petri net. This type of net extends the concept of tokens such that they can contain information themselves. Timing allows us to model temporal processes. Indeed it is this type of Petri net that has been demonstrated to be useful for modelling business processes (van der Aalst and Stahl, 2011).

*The Petri net framework*

Figure 3 shows a representation of the proposed Petri net. Before describing the network in detail, there are two issues we wish to clarify. First the boxes “A” through “E” are not transitions but entire petri nets, henceforth *subnets*. These subnets are plugged into the framework and must conform to certain constraints described below. Second, for technical reasons we would wish to have bi-directional arcs, this allows a subnet the flexibility to remove or replace tokens from input places. However, for ease of exposition we have used dashed arrows to represent these bi-directional arcs. The direction of each arrow allows the

reader to clearly see which places are considered inputs and which are considered outputs from each subnet.

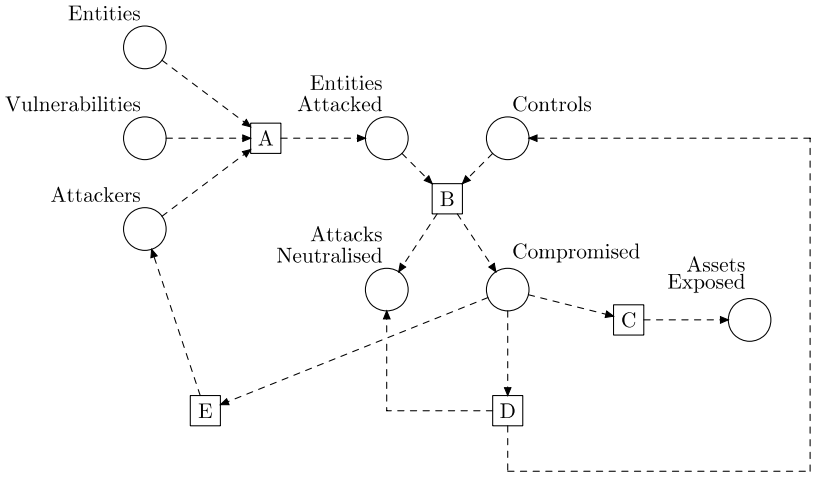



Figure 3 The Petri net Information Security Framework

The subnet denoted "A" (near the top left of the network shown in Figure 3) has three input places:

"Entities" contains (coloured) tokens representing all the possible targets (particular organisations, individuals, etc). Each token has at least a unique identifier, but will typically also contain a record of relevant information regarding the particular entity.

Similarly the place denoted "Vulnerabilities" contains tokens relating to all forms of vulnerability, each token will have at least a unique identifier.

Finally the place denoted "Attackers" contains tokens representing different possible attackers, each with a unique identifier. Maintaining the identity of an attacker throughout the framework is useful for modelling composite (attack tree) style attacks and for being able to introduce into the model the idea that different attackers will have different goals once they have compromised an asset.

Subnet "A" produces new tokens, denoted **attack** tokens, which are a join of the **Entity, Vulnerability** and **Attacker** tokens, (for clarity we use a bold font to identify token types). It is important to note that due to the Petri net's ability to model concurrency; the output of subnet "A" can result in multiple tokens. Hence we can model multiple attacks on multiple entities that are all occurring simultaneously. The output tokens from subnet "A" enter the "Entities Attacked" place. This place represents all the currently active attacks.

Moving on to subnet "B", the input places are "Entities Attacked" and "Controls". The "Controls" place contains tokens representing each control that each entity currently has in place. Each **control** token will have a list of vulnerabilities it covers and a list of vulnerabilities it exposes, along with an identifier for the particular entity. It is the job of subnet "B" to determine if a **control** token exists that has an entity/covered vulnerability component that matches the entity/vulnerability component of the **Attack** token. If an **attack** token is covered by a **control** token, then the **attack** token is moved into the "Attacks Neutralised" place. This particular place allows us to record all successfully defended attacks. If an **attack** token is not successfully covered by a **control** token, this means that the entity has been successfully compromised. The **attack** token is moved to the "Compromised" place.

The “Compromised” place is an input to the last three remaining subnets. We shall describe each of these subnets in turn.

Subnet “E” returns information back to the attacker. At a minimum this can be the fact that the attack was successful, which is useful for modelling the ordering within attack trees. That is to say the attacker can initiate a further attack based on the success of the original attack(s). Subnet “C” is used to determine which assets are exposed given the set of successful **attack** tokens. The output is an **Asset Exposed** token which contains an asset identifier and the relevant attack tokens. (The details regarding assets and the attacks required to expose them is part of the information recorded about an entity.)

Finally subnet “D” models the ability to find and exploit and potentially deal with it, first by neutralising the attack and then by building new controls. It is worth noting that this process of security hardening need not be modelled independently for each entity. Information is typically shared between entities in order to speed up this process.

By probing the state of the framework we can reason about variety of attack scenarios and responses. Cost models can be built on top of this framework by introducing additional information relating to costs such as the cost of exposure of each asset and the cost of maintaining a particular control.

**References**

Chen, T. M., Sanchez-Aarnoutse, J. C., and Buford, J. (2011). Petri net modeling of cyber-physical attacks on smart grid. *Smart Grid, IEEE Transactions on*, *2*(4), pp.741-749.

House of Commons. (2012). *Malware and Cyber Crime: Twelfth Report of Session 2010-12.HC 1537*. London: The Stationery Office Limited.

Huang, H., and Kirchner, H. (2011). Formal specification and verification of modular security policy based on colored petri nets. *Dependable and Secure Computing, IEEE Transactions on*, *8*(6), pp.852-865.

Thomas, R.C., Antkiewicz, M., Widup, S., and M. Woodyard. (2013). “How bad is it? A branching activity model to estimate the impact of information security breaches”. 12th Annual Workshop on the Economics of Information Security. Washington DC.,: Georgetown University 11th to 12th June), pp.1 to 34.

van der Aalst, W., and Stahl, C. (2011). *Modelling Business Processes: A Petri Net-Oriented Approach.* Cambridge, Massachusetts: The MIT Press.

Winsberg, E. (2003). Simulated experiments: Methodology for a virtual world. *Philosophy of Science*, 70 (January), pp.105-125.

Yao, X., Konopka, J.A., Hendela, A.H., Chumer, M., and Murray, T. (2005). Unleash physical limitations: Virtual emergency preparedness planning simulation training, methodology and a case study. Proceedings of the Eleventh Americas Conference on Information Systems, Omaha, NE (11th to 14th August), pp.1643 to 1652.

**Appendix 1: The First Korea-UK Cyber Security Research Workshop Programme at the British Embassy in Seoul on 16th October, 2013.**

| | |
|---|---|
| 9:00 - 09:30 | Registration |
| **Opening session (E.J. Kim)** | |
| 09:30 - 09:40 | · Greeting, Gareth Davies, Head of Science and Innovation, British Embassy Seoul.<br>· 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.<br>· 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 ><br><br>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.<br>· The policies for promoting the cyber security industry, Soon Tae Park, KISA , Korea.<br>· Discussion. |
| 11:00-11:20 | Coffee break |
| **Session B < Cyber security & privacy landscapes (e.g., cyber threats and vulnerabilities) ><br><br>Moderator : K.H. Chung** | |
| 11:20 - 12:10 | · Consumerisation and information sharing: What happens when it goes wrong?, Mike Humphrey, National Crime Agency, UK.<br>· Recent cyber security and privacy landscapes in Korea: Challenges and responses?, Heung Youl Youm, Soonchunhyang University, Korea.<br>· Discussion |
| 12:10 - 14:00 | **Networking lunch** |

| | |
|---|---|
| **Session C < Best practices for SMEs >**<br><br>**Moderator : Godfrey Gaston** | |
| 14:00-14:50 | · Cyber security culture and ways to improve security management, Peter Trim, Birkbeck, University of London, UK.<br>· Personal information protection and supportive policy for SME in Korea, Kim Du-Hyun, NIA, Korea.<br>· Discussion |
| 14:50-15:10 | Coffee break |
| **Session D < Academic and Business relationships >**<br><br>**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.<br>· Korea-UK ICT security tech R&D collaboration case study: ETRI and CSIT, Dooho Choi, Electronics and Telecommunications Research Institute (ETRI), Korea.<br>· Discussion. |
| **Session E < Education/training >**<br><br>**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.<br>· Education and training for cyber security in Korea, Yoonsoo Lee, KISA, Korea.<br>· Discussion |
| **Wrap-up <Establishing future collaboration>**<br><br>**Moderators: Peter Trim and Heung Youl Youm** | |
| 16:50 - 17:20 | Workshop conclusion and ending remarks |

**Appendix 2: 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)<br>▪ Congratulatory remark (I), Mike Humphrey, National Crime Agency, UK<br>▪ 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 >**<br>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<br>▪ Framework for cyber security information exchange in Korea, Jong-hyun Baek, KISA, Korea<br>▪ Disaster recovery management, Kevin Brear, J.P. Morgan, UK. |
| 11:00- 11:20 | **Coffee break** |
| **Session B < Critical National Infrastructure Protection>**<br>Moderator : D.H. Park | |
| 11:20 - 12:10 | ▪ Critical Network Infrastructure Protection (CNIP) in the UK, Hugh Boyes, IET and Warwick University, UK<br>▪ Critical Network Infrastructure Protection (CNIP) in Korea, Heung Youl Youm, Soonchunhyang University, Korea<br>▪ Discussion |
| 12:10 - 13:15<br>13:15- 14:00 | **Networking lunch**<br>Followed by two talks:<br>Organizational learning and simulation exercises, David Weston, Peter Trim, Birkbeck, University of London, and Yang-Im Lee, University of Westminster, UK<br>and<br>**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**<br>**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<br>▪ 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.<br>▪ Discussion |
| 14:50-15:10 | **Coffee break** |
| **Session D < Table top exercise(s): >**<br>Moderators : Peter Trim and Heung Youl Youm | |
| 15:10 - 16:30 | One or more of the topics cited):<br>(1) To establish how scenario-based training and the organizational learning concept can promote the collectivist decision-making approach to security.<br>(2) Produce a conceptual cyber security risk communication model to facilitate incident management and business continuity planning.<br>(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).<br>(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 >**<br>Moderator : Peter Trim and Heung Youl Youm | |
| 16:30 - 16:45 | General discussion. |

## Appendix 3: Korean and UK Cyber Security Research Network Member Profiles

**Mr. John Austin,** CSC Global Cybersecurity
Mr. John Austin is Head of Cybersecurity Consulting (UK) Strategy & Architecture, Europe ICS Practice Coordinator at CSC Global Cybersecurity, He holds a masters degree in Information Security from Royal Holloway, University of London and during his studies produced a dissertation entitled: A Review of Security Awareness in Large UK Public Sector Organisations.

*Publications*

Trim, P., Hadfield, R., Garlati, C., Smith, M., Austin, J., and Lee, Y-I. (2012). "Understanding, explaining and counteracting inappropriate user behaviour: Insights and recommendations", *IAAC Consumerisation of IT Workshop Research Report.* London: Information Assurance Advisory Council.

Trim, P.R.J., Blyth, A., Tryfonas, T., Ralph, S., and Austin, J. (2012). "Risk and advanced persistent threat agent: Context and counteracting strategy", *IAAC Consumerisation Workshop Research Report.* London: Information Assurance Advisory Council.

Trim, P., Hadfield, R., Garlati, C., Smith, M., Austin, J., and Lee, Y-I. (2012). "Understanding, explaining and counteracting inappropriate user behaviour", *IAAC Consumerisation Pre-Workshop Briefing Papert.* BCS, The Chartered Institute for IT, London: Information Assurance Advisory Council.

Trim, P., Austin, J., Aston, S., and Lee, Y-I. (2012). "Common and shared services in the context of cloud computing: Analysis and interpretation", *IAAC Consumerisation Workshop Research Report.* London: Information Assurance Advisory Council.

Trim, P., Lee, Y-I., Austin, J., and Aston, S. (2011). " Common and shared services in the context of cloud computing", *IAAC Consumerisation Pre-Workshop Briefing Papert.* BCS, The Chartered Institute for IT, London: Information Assurance Advisory Council.

**Dr. Jong-hyun Baek,** Korea Internet Security Agency
Areas of Interest/research expertise: security for ubiquitous telecommunication services, e.g. IoT, ITS, Mobile, Smart grid security, and PKI-related applications and services.

Dr. Jong-hyun BAEK, who has been a senior researcher at the Korea Internet & Security Agency since 2001, had been a Director of Korea Certification Authority Central (KCAC) in Korea Internet & Security Agency from 2008 to 2009, and had been a Director of the Smart Internet Division in Korea Internet & Security Agency from 2010 to 2012. In addition, he is a Rapporteur of ITU-T Study Group 17 Question 6 (Security Aspects of Ubiquitous Telecommunication Services) since 2009. He has been a Vice-chairman of the Korea local Group for ITU-T Study Group 17 to the Ministry of Science, ICT and Future Planning since 2009. He had been a chairman of the Telecommunication Technology Association (TTA) PG501 (Information Security Algorithms and Protocols) from 2008 to 2009 and a chairman of NFC application service committee of Korea NFC Forum Standardization in 2011.

**Hugh Boyes,** Warwick University

Area of interest: cyber security issues related to industrial control systems and the built environment.

**Kevin Brear,** J.P. Morgan
Kevin served for 20 years in City of London Police and spent the last 5 years of his service in the Anti-Terrorism and Public Order Dept, as the Force Major Incident Officer. He and his team were responsible for writing and contributing to many of the plans and processes that were used in the response to the 7 / 7 attacks on London. He implemented the UK's first recognised BC programme in a blue light agency, when he introduced the CoLP Business Continuity programme in 2002 and worked with the Corporation of the City of London contingency planning team to deliver industry briefings and develop blue light / public sector and private sector collaboration for BC and community resilience. Since leaving the police service in 2005, he has worked for a number of private sector firms, including as a Crisis Management Team Leader for a large professional services firm, where he led the firm's responses to a number of major Information Security incidents and breaches. Since October 2010, he has worked for JP Morgan Chase as an Information Risk Manager, initially as a line of Business IRM responsible for the Global Commodities Group, Rates and Fixed Income in EMEA and for Tax Orientated Investments in North America. Since September 2013, he has been working as the Third Party Risk Lead for JPMC, Global Technology Infrastructure, Corporate Sector in EMEA.

He has been involved in writing BSI standards since 2005 and contributed to the development of BS 25599 Parts 1 & 2, BS PD 25666, BSI / ANSI BCM.01, BS 25777, BS PAS 200, BS ISO 22301 and BS ISO 22313. In 2011 he was appointed as the Chairman of the BSI's Societal Security Management 1 (SSM / 1) committee and in 2012 he was appointed as the UK's principal expert to the ISO Technical Management Board Strategic Advisory Group on Security.

SSM / 1 is the UK national mirror committee of ISO TC 223, ISO TC 247 and CEN 391 committees and is charged with the oversight for developing standards in organizational resilience, security and aligned matters, including crisis management.

Kevin holds an MSc from the University of Leicester in Risk, Crisis and Disaster Management. He is currently a PhD candidate at the University of Portsmouth, Business School, researching organizational learning and knowledge management from business disruptions, crises and enterprise risk management failures and how the information gained from those events may contribute to building organizational resilience.

**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)
Dooho Choi is currently a principal researcher at the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea, which he has been with since January 2002. He received his M.S. and Ph.D. degrees in mathematics from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea in 1996, 2002, respectively. His current research interests are side channel analysis and its resistant crypto design, security technologies of RFID and wireless sensor network, lightweight cryptographic protocol/module design, and cryptography based on non-commutativity. He was the editor of the ITU-T Rec. X.1171.

**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. Kim Du-Hyun is director of Privacy Protection Policy Department at the National Information Society Agency (NIA), which is a specialized institution governed by the Personal Information Protection Act (PIPA). He is in charge of the main policy programmes based on PIPA, such as Privacy Impact Assessment (PIA), Certification for Personal Information Protection Level (PIPL), and personal information protection training and public relations.

**Dr. Godfrey Gaston,** Queen's University Belfast
Godfrey is currently Director of the Centre for Secure Information Technologies (CSIT), based at Queen's University Belfast, where his role involves both the day to day and strategic management of the centre, including business, academic programme and project management. He has expertise in commercialisation and knowledge transfer within an open innovation research environment. CSIT is acknowledged as an "Academic Centre of Excellence in Cyber Security Research" by the UK Government, in partnership with the Research Councils' Global Uncertainties Programme (RCUK) and the Department for Business Innovation and Skills (BIS). CSIT, which currently employs about 80 staff, has world leading capability and research excellence in security for Cyber, Cloud Computing, Smart Grid and Cyber Physical Systems. Godfrey is also CEO of startup company, Titan IC Systems.

**Dr Robert Ghanea-Hercock,** BT Technology, Service and operations (TSO)
Dr Robert Ghanea-Hercock is a Chief Research Scientist in the British Telecommunications Security Research Practice. He has many years experience in managing security research projects in the UK, and was theme leader for networks and security in the UK MOD Information Fusion Defence Technology Centre.

He chairs an international workshop on adaptive cyber defence, and has over thirty international publications in AI and security concepts, in addition to filed twelve patents. His latest book is on the theme of resilience and cohesion in social systems: ("Cohesion – The Making of Society", available from Amazon.)

Professionally he is a Chartered Engineer and Fellow of the British Computer Society. He is also a Visiting Fellow at the School of Electronics and Computer Science at Southampton University, and at the Said Business School in Oxford University, and an Honorary Fellow at Imperial College. He has also served for several years as an independent technical expert for the UK Defence Science Advisory Council (DSAC), and was a Business Research Fellow at the Santa Fe Institute in New Mexico.

In his current role, Robert provides strategic advice to BT and major corporate and government customers on Cyber Security and Defence technologies. Lead role, as Chair and programme manager for a major three year collaborative research venture with the Technology Strategy Board. I am responsible for all programme design, operation and exploitation. (Partners have included: Northrop Grumman, Oxford Said Business School, Imperial College, and Warwick University.) The research domains covered by the teams include: A.I, Cyber Security, Dependable systems and Defence technologies.

*Invited Lectures*
Keynote: “Project Saturn”, an overview of novel Cyber Defence Technologies, Georgetown University, Washington April 2012.

- Keynote: “Autonomous Information Security in Cyber Warfare”, SMI Conference on Cyber Defence and National Security, Copenhagen, May 2008.
- Keynote: “Information Fusion and NEC”, Stepping C4ISTAR into the Future, RUSI Conference, Malvern, Sept. 19th 2006.
- Keynote: “The probable shape, form and capability of Networks in 2015”, Whither Warfare Conference series, General Dynamics Research Foundation, Shrivenham, June 2006.
- Keynote: “The view from BT's research centre on the future of communications”, Cambridge Networks, Robinson College Cambridge, 3rd May 2006.
- Keynote: “Role of Data and Information Fusion in NEC”, Data & Information Fusion Defence Technology Centre Annual Conference, Shrivenham, September 2005.
- Keynote: “Adaptive Defence of Computing Infrastructures”, Santa Fe Institute annual Business Network meeting, Santa Fe, Nov. 2003. (Cited in Wall Street Journal Magazine).

*Patents*
Fourteen international patents filed in the domains of Machine Learning, Resilient Networks and Security Architectures.

*External Roles*
Invited to serve on the expert industrial panel, for the new GCHQ Academic Centres of Excellence in Cyber Security, from Jan 2013. Chair of Audit committee for MoD DSTL Knowledge Systems group, at Portsdown West, in 2009 and 2011. Chair of Steering Committee for the Cyber-Security Knowledge Transfer Network, (appointed 2006-2009). This role involved leadership and direction setting for the Steering Committee of the UK Technology Strategy Board for the Cyber Security Knowledge Transfer Network (KTN). This KTN had a national UK role in advising government and industry on best practice in all issues surrounding cyber security. The role included providing strategic advice to Home Office, MoD, and other government departments.
Selection of Publications

*Foresight Report*

"Large-scale, small-scale systems." Report by the Foresight Cognitive Systems Project, Professor Jim Austin, Professor Dave Cliff, Dr Robert Ghanea-Hercock, Dr Andy Wright, online at: http://www.foresight.gov.uk/Previous_Projects/Cognitive_Systems/Reports_and_Publications/Research_Reviews/Research_Reviews__Physical_Sciences/4_Largescale_Smallscale_Systems.html , 2004.

*Books*

- Ghanea-Hercock R., "Cohesion – The Making of Society", pub. Lulu Press, Oct. 2009.
- Ghanea-Hercock R. (Editor), & Thompson S. (Editor), "Defence Applications of Multi-Agent Systems": International Workshop, DAMAS 2005, Utrecht, the Netherlands, July 25, 2005: Revised and Invited Papers (Lecture Notes in Computer Science S.)
- Ghanea-Hercock R., "Applied Evolutionary Algorithms in Java", pub. Springer, New York, April 2003.

*Journals*

Ghanea-Hercock R., "Why Cyber Security is Hard", Georgetown Journal of International Affairs, p.81-89, International Engagement on Cyber Oct. 2012.

A. Healing, H. Duman, R. Ghanea-Hercock, "Autonomic Middleware and Resilient Information Systems", UK MoD Codex Journal, December 2009: http://www.science.mod.uk/codex/issue5/journals/journals3.aspx

*Conferences*

- Visual Analytics in the Cyber Security Operations Centre; Rowlingson R., Healing A., Shittu R., Matthews S., Ghanea-Hercock R., NATO Symposium on Visual Analytics, Defence Academy, Shrivenham, UK, October 2013. (Best Paper Award.).
- H. Duman, A. Healing, R. Ghanea-Hercock, Adaptive Visual Clustering for Mixed-Initiative Information Structuring, presented at the HCI International 2009 Conference, San Diego, July 2009.
- H. Duman, A. Healing, R. Ghanea-Hercock, An Intelligent Agent Approach for Visual Information Structure Generation, presented at the 2009 IEEE Symposium on Intelligent Agents (IEEE IA 2009), Tennessee. April 2009.

**Professor Hugh Griffiths,** University College London

Area of interest/expertise. Formerly Head of the Department of Electronic and Electrical Engineering, and Principal of DCMT at the Defence Academy of the United Kingdom. Serves on the Supervisory Board of MoD's EMRS Defence Technology Centre (DTC). A broad interest in sensors and the associated signal processing and image processing issues.

**Mr. Oliver Hoare,** Dysart Solutions Ltd.

**Ms. (Elly) IL young Hong,** Supreme Prosecutors' Office of Korea.

**Mr. Mike Humphrey,** National Crime Agency

Areas of interest: Critical infrastructure protection; security incident reporting and information sharing; information security risk advice and professionalism in information security. Mike was a police officer in Kent Police for 30 years He served at numerous locations in a number of operational and headquarters roles. These included match commander for football and other major sporting events. Silver commander roles in the

policing of hunts, demonstrations, public events and critical incidents. As an Inspector he worked in the research and planning department and later supporting the Chief Constable and Chief Officers in the introduction and monitoring of Key Performance Indicators, which at the time was groundbreaking for the police service.

In the Information and IT Department he was the implementation manager for a combined crime, custody, case and intelligence relational database system before joining the Police IT Organisation as a Chief Inspector where he was the National Liaison Officer for Networks and Infrastructure, in particular the UK wide police critical infrastructure – the Police National Network (PNN2). This was the first time the police service had access to a UK wide IP infrastructure that provided secure communications and access to national police systems. He was heavily involved in the requirements capture and procurement evaluation of its subsequent replacement PNN3. He was an active member of a Cabinet Office group which aimed to provide a certification scheme for security products and services that met the needs of national and local government and this encouraged more niche companies to submit their products for evaluation.

He became increasingly involved in Information Assurance and Critical Infrastructure for the police service. He took a part time masters degree in ICT Security at the University of Westminster, achieving a distinction with a dissertation on protecting critical infrastructures entitled *'Monitoring, Response and alerting Capability of a Secure community: A Strategic Approach'*.

He then joined SOCA in 2007 as a Senior Manager heading up the Information Assurance and Accreditation team; this includes being the lead Accreditor for SOCA (Serious Organised Crime Agency). His areas of responsibility include provision of information risk management advice to the business.

Mike sits on the HMG National Accreditor Committee. He is an elected member of the management committee of the Information Assurance Advisory Council (IAAC), a member of the IAAC Government Liaison Panel and sits on the IAAC board. He is a full member of the Institute of Information Security Professionals (IISP) and an elected member of their membership accreditation committee. This also includes accreditation of security professionals who wish to be certified under the Government Certified Practitioners Scheme. These are all linked to improving the competencies and professionalism within the discipline of information security He also represents UK Law Enforcement as the Designated Security Authority on the Europol Security Committee.

He has led IAAC workshops on issues surrounding 'consumerisation' and information sharing particularly surrounding Bring Your Own Devices, jointly producing a final report with Dr. Trim and two other co-authors. He has peer reviewed academics papers and led workshops in the EU on cyber security provision for non EU developing counties. Mike has also commenced lecturing on information/cyber security at universities. He regularly presents at national and international information security conferences and seminars on information security and on this PhD subject of interest.

He is currently taking a part-time PhD in an information security related research subject at the Defence Academy Shrivenham - Cranfield University. His Thesis is based on the issues surrounding the reporting of security incidents (cyber and other types) and the perceived barriers to reporting including them and the effect this may have on information sharing at local, national and international level.

**Dr. Inkyung Jeun,** a director of KISA.

**Mr. Nigel Jones,** UK Defence Academy, Cranfield University,
Areas of interest/research expertise: strategy, planning and communications; Military Information Operations; security management and the human factor; and cross-cultural decision-making. Nigel Jones is Senior Research Fellow at Cranfield University at the Defence Academy of the United Kingdom. He is Director of Postgraduate Studies in Cyber Defence and Information Assurance and Cyber Operations. Prior to joining Cranfield he ran a Security and Information Operations research and consultancy team at QinetiQ, during which time he was also Director of the UK Government's Cyber Security Knowledge Transfer Network. He teaches modules on social technologies and planning. Working across the socio-technical domain, he has particular interest in the human dimension of network and information operations and planning. This he developed in a military career that saw Info Ops deployments in the Balkans, Middle East and elsewhere. He currently supervises a number of PhDs that research risk communication. One is focussed on cocaine use and another on the protection of critical infrastructure. His research and writing has concentrated on social science in supporting strategy, planning and communications.

*Publications*

- Jones, N., and Baines, P. (2013). "Losing control? Social media and military influence". *RUSI Journal*, 158 (1) (February).
- Jones, N.A., and Dodd, L. et al. (2011). *Operationalising Social Science for the Military Planner*. Defence Academy of the United Kingdom, Directed Research Project (August).
- Trim, P.R.J., Jones, N., and Brear, K. (2009). "Building organisational resilience through a designed-in security management approach". *Journal of Business Continuity & Emergency Planning*, 3 (4), pp.345-355.
- Jones, N. (2009). *Building in…Information Security, Privacy and Assurance – a High-level Roadmap.* Cyber Security KTN and FCO Science and Innovation.

**Professor Jina Kang,** Seoul National University
Areas of interest/expertise: Technology management, economics and policy.

**Professor Beomsoo Kim,** Yonsei University.

**Dr. Du-Hyun Kim,** National Information Society Agency (NIA)
Areas of Interest/research expertise: privacy policy, privacy governance, PIA (privacy impact assessment), and performance management.

Dr. Du-Hyun Kim is a director of Privacy Protection Project Department at the National Information Society Agency (NIA), which is a specialized institution determined by the Personal Information Protection Act (PIPA). He is in charge of the main policy programmes based on PIPA, such as Privacy Impact Assessment (PIA), Certification for Personal Information Protection Level (PIPL), and personal information protection training and public

relations. He studied Public Administration (BA, MA, PhD) at Hankuk University of Foreign Studies (HUFS) in Korea. He served as a Policy Adviser to the Education and Science Minister for 2 years (2008-2010).

**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
Areas of Interest/research expertise: security for networks, e.g. Cloud computing, SDN, sensor network, Security standards: COP. Dr. Tae Kyung Kim, who has been an associate professor in the Department of Liberal Art and a director of the computer and information center at Seoul Theological University since 2008.

**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

Areas of Interest/research expertise: cybersecurity measurements, privacy management system related to processing of PII and privacy impact assessment, and malware analysis. Mr Jae Nam Ko graduated from Soonchunhyang University. He is a master course student at SCH University in Korea.

**Professor Kyungho Lee,** Korea University
Area of interest/expertise: Information security.

**Dr. Sang Woo Lee,** ETRI.

**Dr. Yang-Im Lee,** University of Westminster
Areas of interest/research expertise: strategic marketing; marketing strategy; international marketing; integrated risk, compliance and governance (iGRC); organizational learning; cyber security university-industry collaboration; business and management theory and practice; and cross-cultural decision-making. Dr. Yang-Im Lee is a Senior Lecturer in Marketing at Westminster Business School, University of Westminster and is a specialist in strategic marketing and culture. Dr. Lee is fluent in Korean and Japanese and has in her writings explained how national cultural value systems influence organizational value systems and in particular, how a collectivist culture embeds the organizational learning concept. Her approach has led to new insights into the strategic marketing-decision making process. Dr. Lee has studied and worked in Korea, Japan and the UK. She as studied at the School of Oriental and African Studies in London (where she has also provided a number of guest lectures); and was awarded a scholarship by Stirling University to undertake a PhD at that institution. During her PhD studies, she was invited to present a paper at a conference of the Korea Institute at Harvard University. Dr. Lee has to date worked for both Brunel University and Royal Holloway, University of London and has published widely in a range of academic journals with Dr. Trim including the *European Journal of Marketing* and *Industrial Marketing Management*. She has also co-authored a book and co-edited a book with Dr.

Trim, and when Dr. Trim was chairman of the Society for the Advancement of Games and Simulations in Education and Training, she provided continued support and took on the task of editing the society's newsletter (Interact). Indeed, she has over 30 publications in total and has reviewed papers submitted to the *International Business Review*, the *Journal of Global Fashion Management, Industrial Marketing Management, International Journal of Service Technology and Management*, a special issue of *Management Decision*, the Academy of International Business (AIB) Annual conference, the American Marketing Academy Annual Conference, Academy of Management Annual conference, and a marketing text book for example. She is a Fellow of the Higher Education Academy and the Royal Society of Arts. Dr. Lee has been involved in the iGRC Consortium three-year research project with Dr. Trim, which was funded by the Technology Strategy Board and SEEDA, provided research input into the Technology Strategy Board Fast Track project undertaken by Dr. Trim and David Upton. Dr. Lee is an internationally recognized scholar in the area of strategic marketing and culture, and has been involved in various conferences (co-organizer, presenter and chairing sessions). She has been selected to chair a session at the Global Marketing Conference in Singapore in July 2014. As well as having a deep interest in education, Dr. Lee has provided support for the Information Assurance Advisory Council and has been their Academic Liaison Panel Co-ordinator for a number of years. In this capacity she has worked with various academic, industry and government representatives in the UK.

**Dr. Dae-Ha Park,** The Cyber University of Korea
Areas of interest/research expertise: information system auditing; information security management system; security and privacy in social networking, cloud computing and ubiquitous computing, etc. Dr. Dae-Ha Park is an associate professor in the Department of Information Management and Science, The Cyber University of Korea, South Korea. He received BSc, MSc, and PhD degrees in computer science from Korea University. He is a senior auditor for both K-ISMS (Korea Information Security Management System) and K-ISA (Korea Information System Auditing). He worked for a PKI solution vendor named Security Technologies Inc., for 5 years as a chief researcher. Currently he is a committee member of ISO/IEC JTC1/SC27 Korea.

**Dr. DeaWoo Park,** Hoseo Graduate School of Venture
Dr. DeaWoo Park is currently a professor at Hoseo Graduate School of Venture, in South Korea. Professor Park undertakes research into Hacking Forensic, Information Technology Communication in Lab at Hoseo Gaduate School. Dr. Park has published over 90 theses in a range of journals including Computer and Networks, Information Security, Mobile Security, Network Security, Hacking & Forensic of Theory, Practice and Research. Recently, he received 'Best Paper Awards' from the Korea Information and Communications Society (2013). His paper title is 'A Study of Intrusion Security Research and Smishing Hacking Attack on a Smartphone'. Nowadays, he has undertaken teaching assignments in National Research Foundation of Korea (2014) and undertaken a study on Attacks and Defense Techniques of Smishing Hacking and Compensation for Damages Forensic Technology. He has Studied at Soongsil University in Korea (MSc and PhD). Dr. Park has recently been appointed Vice-Chairman of the Korea Institute of Information Security & Cryptology, Korea Information and Communications Society, Korea Digital Forensic Society. He has also been appointed, Secretary General of the Forum of National Cyber Security Policy, and Chair of Forum of Hacking Security Technology.

**Soon Tae Park,** Korea Internet & Security Agency
Soon Tae Park is a senior researcher in the electronic signature and authentication team, and has been in the Security Industry division since 2007. He is a PKI policy research and auditing area expert, and also an ISMS expert.

**Tony Proctor,** University of Wolverhampton
Managing, implementing and developing an information security Warning, Advice and Reporting Point (WARP). This is a UK Government initiative. The main activity of a WARP is to issue information security alerts, provide information security advice and to facilitate the secure sharing of information. WARPs are formal networks for sharing information on security vulnerabilities and incidents. Tony is currently involved in a number of WARPs in the public sector.

**Dr. Peter Trim,** Birkbeck, University of London
Areas of interest/research expertise: strategic marketing; marketing strategy; international marketing; integrated risk, compliance and governance (iGRC); corporate/competitive intelligence; security and business and organizational practices; cyber security university-industry collaboration; business and management theory and practice; and cross-cultural decision-making.

Dr Peter Trim is currently a senior lecturer in management at Birkbeck, University of London and Director of the Centre for Advanced Management and Interdisciplinary Studies. He has studied at a number of institutions including Cranfield University (MSc and PhD), City University (MBA) and the University of Cambridge (MEd). Dr. Trim has recently been appointed Managing Director of GAMMA (Global Alliance of Marketing and Management Associations) Europe and is a Fellow of the Higher Education Academy and the Royal Society of Arts, and a Member of the Information Assurance Advisory Council (IAAC) Academic Liaison Panel. He is also on the editorial board of several academic journals including *Simulation & Gaming: An International Journal of Theory, Practice and Research*; and *Qualitative Market Research: An International Journal*. At Birkbeck, Dr. Trim teaches Marketing Strategy to undergraduate students and International Marketing to postgraduate students, and is Programme Director and Admissions Tutor of the MSc International Marketing. He is also a Teaching Fellow at the School of Oriental and African Studies, University of London and has supervised a number of PhD students. Peter has published over 50 academic articles in a range of journals including *Industrial Marketing Management*, the *European Journal of Marketing*, the *Security Journal*, *International Journal of Intelligence and Counter Intelligence*, *Disaster Prevention and Management*, *Cross-Cultural Management: An International Journal*, *Journal of Business Continuity & Emergency Planning*, and *Simulation & Gaming: An International Journal of Theory, Practice and Research*. Dr. Trim has produced a number of single authored, co-authored and edited books including: Trim, P.R.J., and Upton, D. (2013) *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training*, Farnham: Gower Publishing; and Trim, P.R.J., and Caravelli, J. (Eds) (2009) *Strategizing Resilience and Reducing Vulnerability*. New York: Nova Science Publishers Inc. His work has been well received in a number of countries. Dr. Trim draws on his past work experience which includes employment in a small family business, an electronics company, an oil surveillance company,

an international bank. He has also undertaken teaching assignments abroad in France, Hong Kong and the Netherlands; and has also undertaken a limited amount of consultancy work. Dr. Trim has provided a number of guest lectures at various institutions including Canfield University and University College London, and has been involved in a number of initiatives such as the Canada-UK Partnership for Knowledge Forum and the Law Enforcement and National Security Global Forum. In addition, to this he has been a panellist for an American economics newsletter and provided a major international consultancy company with information for a workshop in Lagos, Nigeria. He contributed the Cyber Attacks section (pages 8 and 9) of the University College London report entitled Scientific Advice and Evidence in Emergencies which was edited by Professor McGuire and submitted to the House of Commons Science and Technology Committee as written evidence in 2010. Dr Trim has been Principal Investigator on two grants awarded by the Technology Strategy Board (TSB) and the TSB and SEEDA in the area of network security and information infrastructure protection. He has reviewed a great deal of work submitted work to various academic journals including the *Security Journal;* the *Journal of Security Sector Management; Disasters: The Journal of Disaster Studies, Policy and Management; International Journal of Emergency Management; Industrial Marketing Management; Journal of Strategy and Management; Journal of Global Scholars of Marketing Science;* and *Simulation & Gaming: An International Journal of Theory, Practice and Research.* Dr. Trim has also reviewed various books and a number of research grant applications (both UK and US).

Contact details:
Dr. Peter R.J. Trim,
Senior Lecturer in Management and Director of CAMIS,
Department of Management,
Birkbeck, University of London,
Malet Street,
London. WC1E 7HX. United Kingdom.
E-mail: p.trim@bbk.ac.uk Telephone +44 (0)207 631 6764

**Professor David Upton,** University of Oxford
David Upton is American Standard Companies Professor of Operations Management at the Saïd Business School, University of Oxford. He came to Oxford from the Harvard Business School, where he was the course head for the first-year MBA courses in Technology and Operations Management, and developed additional courses in Operations Improvement and Information Technology. He serves on the board of Tech Data Inc., a Fortune 100 company based in Clearwater, Florida.

Area of interest/expertise: He consults internationally on competitive strategy, information technology and the improvement of service and manufacturing operations.

**Professor Tim Watson,** University of Warwick
Professor Tim Watson is the Director of the Cyber Security Centre at the University of Warwick. With more than twenty years' experience in the computing industry and in academia, he has been involved with a wide range of computer systems on several high-

profile projects and has acted as a consultant for some of the largest telecoms, power and oil companies. He has designed, produced and delivered innovative courses on cyber security for a variety of public and private-sector organisations. Tim's current research includes EU funded projects on combatting cyber crime and research into the protection of infrastructure against cyber attack.

Tim is a member of the following academic/professional bodies:
Fellow of the British Computer Society (BCS).
BCS Working Group on Cyber Security.
Institution of Engineering and Technology (IET) Cyber Security Steering Committee.
Information Assurance Advisory Group (IAAC) Academic Liaison Panel.
CESG Academia Advisory Group.
National Information Assurance Forum.
ISO/IEC Joint Technical Committee Subcommittee 27 "IT Security Techniques"
(this is the UK national body for the 27000 series ISO standards, represented
by the British Standards Institute (BSI) Expert Panel IST/033).
Council of Professors and Heads of Computing (CPHC).
Vice President (Academic) of the Trustworthy Software Initiative.

Tim is also a regular media commentator on digital forensics and cyber security.

**Dr. David J. Weston,** Birkbeck, University of London
*Main publications*

- Weston D.J., Adams N.M., Russell R.A., Stephens D.A. and Freemont P.S. (2012). Analysis of Spatial Point Patterns in Nuclear Biology. *PloS* one 7, no. 5.
- Heard N.A., Weston D.J., Platanioti K, Hand D.J. (2010). Bayesian anomaly detection methods for social networks, *Annals of Applied Statistics*, 4 (2), 645-662.
- Weston D.J., Hand D.J., Adams N.M., Whitrow C. and Juszczak P. Plastic card fraud detection using peer group analysis, *Advances in Data Analysis and Classification*, 2(1), (2008), 45-62.
- Hand D.J., Whitrow C, Adams, N.M., Juszczak P. and Weston, D.J. (2008). Performance criteria for plastic card fraud detection tools, *Journal of the Operational Research Society*, 58, pp. 956-962.

**Professor Heung Youl Youm,** Soonchunhyang University
Areas of Interest/research expertise: security for applications, e.g. ITS, smart grid, IPTV, security standards: cybersecurity measurements, privacy management system related to processing of PII and privacy impact assessment, and malware analysis.

Dr. Heung Youl Youm is currently a professor in the Department of Information Security Engineering at Soonchunhyang University, Korea (since 1990) as well as a director of the cybersecurity research center which was recently established at SCH University (December 2013). He received his Bachelor, Master, PhD degree, respectively in 1981, 1983, and 1990 from Hanyang University, Korea.

He has been involved in many policy advisory committees in the area of Information Security to the Korea Communications Commission, the Ministry of Security and Public Administration, Ministry of Science, ICT and Future Planning and the National Information Service of Korea (Republic of), etc. He was a chairman of the KIISC (Korean Institute of Information Security and Cryptography) in 2011. In addition, he is a Vice Chairman of ITU-

T Study Group 17 (Security) and a Chairman of Working Party 3 (Identity management and cloud computing security) of ITU-T Study Group 17. He has been a chairman of the Korea local group for ITU-T Study Group 17 to the Ministry of Science, ICT and Future Planning since 2009; and a chairman of Korea Information Security Standardization Forum since 2012.

Contact details:
Dr. Heung Youl Youm
Professor, Department of Information Security Engineering
Director, Cybersecurity research center at SCH University
Soonchunhyang University, Korea
22 Soonchunhyang-ro, Shinchang-myeon, Asan-si, Chungnam-do, Seoul, Korea
E-mail : hyyoum@sch.ac.kr Telephone : 82-41-530-1328

**Professor Hyeon Yu,** Korea Police Investigation Academy
Areas of interest/expertise: Cybercrime Investigation.

**Dickie Whitaker,** Financial Services Knowledge Transfer Network

**International Group Member**

**Professor Hironobu Nakabayashi,** Meiji University
Area of interest/expertise: International relations, crisis management, human security, comprehensive security, including non-traditional security

After finishing his doctoral studies at Keio university Graduate School of Media and Governance in 2008, Dr. Nakabayashi served as a senior researcher at Japan's Independent Institute Inc. Since the end of 2009, Dr. Nakabayashi has served as Research Fellow at the Meiji University Research Center for Crisis and Contingency Management and in the summer of 2010, Dr. Nakabayashi established the Limited Liability Partnership Security Knowledge Networks. Dr. Nakabayashi participated in the Independent Investigation Commission on the Fukushima Daiichi Nuclear Accident as a member of working group (2011.09-2012.02), and National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission as a researcher of the secretariat. Since 2006, Dr. Nakabayashi has engaged in research about Nuclear security, trends in terrorism and related issues. Dr. Nakabayashi received Ph.D. in media and governance from Keio SFC (2010).

**Observers**

**Ms. Rhian Jones**, Cabinet Office, UK

**Mr. Austen Okonweze**, Department of Business Innovation and Skills, UK