Proceedings of the 9th Colloquium for Information Systems Security Education
Georgia Institute of Technology
Atlanta, Georgia, 6-9, June 2005

# An Information Security/Assurance Vision: Development of a Multi-Disciplinary Institute at a Public University

William Caelli AO, Edward Dawson : Information Security Institute, Queensland University of Technology, Australia

***Abstract – The formation of a new research and postgraduate education institute, the Information Security Institute (ISI), was proposed for the Queensland University of Technology in 2004. The ISI concept involves a collaborative research undertaking of the Faculty of Built Environment and Engineering (BEE), the Faculty of Business (BUS), the Faculty of Information Technology (IT), and the Faculty of Law (LAW). The formation of the ISI was put forward as the next logical step in consolidating the already acknowledged expertise that the university had developed in all aspects of information security over the past 16 years. The ISI has been established to pursue multi-disciplinary research in technology, legal, policy and governance issues related to all aspects of information security and assurance. The ISI proposal was seen as placing an emphasis on research in the area of critical infrastructure protection (CIP) as well as national information infrastructure protection (NIIP). The ISI aims to be a dynamic research facility that integrates the research of the four founding faculties of the university to answer information security, information assurance and protection, and technology policy challenges that confront business, government and the community as a whole. The ability to encourage cooperative, multi-disciplinary approaches to research topics in the area has been a major aim of the ISI based upon prior experience in this activity.***

**Index terms – Information security research, information assurance, multi-disciplinary research, technology policy.**

## I. INTRODUCTION

During 2003 and 2004 the concept and vision for an integrated research and postgraduate education oriented institute in all aspects of information security and assurance at the Queensland University of Technology was developed. The major aim was to facilitate an environment where researchers can collaborate to advance major information and communications technology (ICT) security and assurance/ protection issues as well as to investigate and develop related technology policy strategies.

The institute's environment has been set out to promote inquiry into information security and related issues involved in, for example:

- the further development of trust in electronic commerce systems for both the private and public sectors;
- the protection of Australia's critical and national information infrastructures;
- the development of policy and legal frameworks for effective e-government and e-business;
- the advancement of secure computer systems (node) and data network solutions at the enterprise level;
- the development of frameworks for the advancement of justice, information protection and innovation, and
- contributions to safeguarding the nation through research and education in combating terrorism in all its forms.

The ISI formally commenced in January 2005 through a collaborative research undertaking of the Faculty of Built Environment and Engineering (BEE), the Faculty of Business (BUS), the Faculty of Information Technology (IT) and the Faculty of Law (LAW) in QUT. Indeed, this formal cooperating was made simpler by the fact that individual researchers in these faculties had already been involved in a number of collaborative research projects over the last few years.

In addition it was decided that the researchers and projects located in the 16 year old *"Information Security Research Centre (ISRC)"*, located in the Faculty of Information Technology (FIT), would be transferred to the ISI. Researchers from the Faculty of Built Environment and Engineering, the Faculty of Business and the Faculty of Law then also agreed to participate in the ISI.

As a major part of the overall vision for ISI, it was decided that researchers from other Faculties in QUT would be encouraged to join on individual projects. It is anticipated that as the ISI matures, more Faculties will join on a full membership basis rather than on a project by project basis.

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

Over the past 16 years, the ISRC had established itself as a premier research entity in the area of information security. However, most of the research undertaken by the ISRC had been conducted by members of the Information Technology Faculty. The ISI provided the university with an opportunity to expand this research in information security to include other disciplines such as law, sociology, economics, engineering, government and business. The expanded involvement of these other disciplines has evolved through the increasing need for secure use of information by the various sectors of society and the need to operate via the Internet. These sectors of society include the community at large, governments trying to provide their services more effectively, business wanting to more efficiently meet market needs, courts wanting to administer justice more cost effectively without any loss in the quality of justice and governmental organizations aiming to protect and safeguard the nation.

At the same time, the need for ICT professionals to be better educated, possibly at postgraduate level, in all aspects of information security and assurance became more pressing. In the commercial arena, for example, many sectors want to transact business via the Internet but a lack of trust in the digital environment is impeding adoption of technologies that potentially offer great societal benefits. To address this lack of trust, valid concerns over privacy and security must be addressed. This in turn raises a raft of pressing research challenges that demand a multi-disciplinary response.

The rationale for the ISI reflected the needs of a rapidly changing society that is increasingly reliant, or even totally dependent, upon information and communications technology. Developments in this area are bringing about an emerging scenario where converging information and communications technologies are becoming a ubiquitous part of the fabric of everyday life. Reliance on these technologies is rapidly becoming total and so society at large must be able to trust that the products, artifacts, systems and services of those technologies operate reliably and in the best interests of society.

Such a scenario introduces truly novel research problems that will not be solved by a purely single or even straight technical focus. Information security and assurance, in the ISI proposal, was seen as no longer simply involving mathematicians, engineers and computer scientists. In order to better understand information security at the enterprise and community levels it is necessary to involve many other disciplines. Hence, the ISI has been established as a multi-disciplinary institute undertaking research in new information security technologies and information protection policy as well as investigating the impact of these technologies from legal, business, sociological, management and economic perspectives.

The ISRC, now integrated into the ISI, had provided much practical research into the provision of solutions to current information security needs. The ISI will build on this approach with an expanded multi-disciplinary capability. The ISI will be a unique institute bringing together researchers with a common focus in developing practical solutions to satisfy the ever increasing desire by governments, business, consumers and even such entities as the court systems, to operate in a trusted and safe digital environment.

## II. THE ISI VISION

The vision of the ISI has been to make a “real difference” by establishing it as an internationally recognized centre of excellence in all aspects of information security and assurance as well as related legal and policy matters. Thus the ISI could become a strategic resource for government, business and the community alike.

It was essential, then, that the ISI would be seen by the university and researchers alike as a dynamic research facility that integrated, at least initially, the disciplines of the four original faculties to answer information security, information protection and technology policy challenges that confront business, government and the community as a whole. In addition, the ISI intends to play a major role in research and education matters related to critical infrastructure protection (CIP) in advancing solutions to the many problems involving the industries of telecommunications, banking and finance, energy and transport as well as matters related to the security of healthcare systems. The ISI’s involvement in CIP was seen as being of national importance in developing solutions to problems that could affect the economic well being of the nation. The owners and operators of the nation’s critical infrastructure are dependent upon a robust framework for the protection of information and therefore an essential element of the ISI’s purpose was seen and articulated as being to ensure that appropriate information protection policy frameworks are developed that take into account the advancement of information security and network security technology.

The ISI intends to play a significant role by assisting government in the task of safeguarding the nation and combating terrorism through the use of novel and advanced technologies in, for example, voice and video processing to identify and track suspects, detect human activity and gather intelligence information as needed. At the same time, the ISI also intends to play a significant role in developing relevant technology policy frameworks

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

for the new economy. In doing so, it will provide evaluation and strategic vision on innovation, competition, intellectual property and e-government as they relate to information security, information protection and technology policy.

## III. ISI OUTCOMES

In presenting a proposal of such magnitude to university management, it was essential to outline some key outcomes that could be expected through support for the proposal. The following key elements were seen as addressing those outcomes.

- the creation and support of an appropriate level of resources to be able to undertake leading edge research and consultancy in pursuit of the stated vision;
- the education of high quality graduates in the area;
- the provision of a specialized knowledge-based resource that will articulate solutions for community, industry and government activities;
- the development of the ability to propose and analyze relevant policy on information protection and associated technology innovation.

These outcomes were proposed as facilitating the commercial development of relevant products and processes. They were also seen as assisting in the transfer of new knowledge into the overall activity of formation of both public and technology policy, and practice, in information security and information assurance.

The ISI could in turn facilitate achievement of these outcomes or goals by:

- establishing a single multi-disciplinary research centre within a large public university that will, from its initiation, have critical mass in its selected research domains;
- providing a collaborative environment that is conducive to strong growth of high quality research by both experienced researchers and postgraduate students;
- strengthening the university's stated commitment to multi-disciplinary collaboration to achieve ground breaking research outcomes;
- consolidating the university's capacity to integrate research initially across the original member faculties and then, as the ISI matures**,** across even more Faculties of the university as they become members of the ISI;
- extending collaboration with national and international research groups;
- identifying and developing collaborative research relationships with industry, government and other Faculties to maximize commercialization opportunities; and
- providing a high quality research and training environment for post graduate students in challenging and relevant research projects.

## IV. RESEARCH DOMAINS

It was essential to clearly define to the university where cooperative research activity had already commenced among the members of the university who were proposing the new institute. It was found that key researchers from the four founding faculties had joined forces to undertake collaborative research in 8 domains of research activity in which the university had national or international expertise and perceived competitive advantage. Specific research programs build on existing areas of strength and focus on "real-world" ICT security, information protection and technology policy, issues that are best addressed through the collaboration of disciplines.

The 8 research domains do not represent fixed structures within the ISI but represent flexible areas of research within it. It is highly likely that as further opportunities arise, researchers from other faculties will join with the original four faculties to further enhance the reputation and activities of the ISI. As stated above, it must be re-iterated that the principal goal of the ISI is to create a flexible environment to undertake multi-disciplinary research in the designated area. In turn, it has been perceived that this multi-disciplinary approach will simplify and enhance opportunities for ISI researchers in collaborating with external contacts who are located outside the university environment.

As a start it was important to identify several key research areas or themes that would build upon already existing expertise. Thus it was decided that the following 8 "research domains" would be identified for original emphasis. These domains are:

(a) Cryptology
(b) E-Business and E-Government
(c) Technology, Law and Policy
(d) Governance and Information Protection
(e) Network Security and Trusted Systems

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

(f) Computer Intrusion, Forensics and Evidence

(g) Biometric Person Authentication

(h) Social and Behavioral Issues

Individual research leaders were identified from current researchers for each of the above domains of interest. As well it was important to identify for each domain research projects that were currently underway as well as those that had potential. At the same time, these domains had to be related to the research priorities set out by government particularly through Australia's appropriate research sponsoring organization, the "Australian Research Council (ARC)". Research activities nominated for the ISI were then seen as fitting within the national priority research areas of *"Safeguarding Australia"* and *"Transformational Technologies"*, two of the four priority areas of research for ARC. This alignment was important for university research administration purposes.

## V. EDUCATION AND RESEARCH TRAINING

There currently exists a substantial demand for highly qualified information security experts in both the public and private sectors. This demand is both domestically and internationally driven. Further, the market demand spans many industry sectors such as government, banking and finance, healthcare, transport, telecommunications infrastructure as well as others. There is an even more pressing demand for cross disciplinary expertise, e.g. in the intersection between information and network security and the law. The aim was clearly articulated that ISI would contribute to meeting this demand by producing graduates who possess expertise in multiple disciplines, e.g. law, business, behavioural science and others as well as information assurance and protection, information security, e-government and technology policy.

At the same time it was essential to emphasize the more generic purposes of research training in a university environment. The ISI was seen as providing a unique and high quality research training environment, emphasising research excellence and encouraging the development of entrepreneurial skills. This research training effort was presented as growing from an existing research base. Initially, the majority of researchers were seen as coming from the original ISRC, i.e. from staff members of the Faculty of Information Technology. It was suggested in the proposal that this would most likely change as more researchers from the Built Environment and Engineering, Business and Law Faculties became involved.

Over time, it is anticipated that each of the participating and founding faculties will equally participate in the ISI. Notwithstanding this initial anomaly in researcher numbers, each of the faculties was presented as participating in the ISI on an equal, co-operative basis. It was also essential to present to university management a marketing program for the ISI that could be evaluated in the future in terms of numbers of postgraduate students encouraged to it, new research positions, and so on.

In providing the correct educational environment, the ISI was cited as a necessary structure in the university to produce post-graduate level ICT and allied security professionals who will assist in meeting the current and future demand that the market requires. This demand will continue as the use of open, commodity level systems continues to proliferate across the world. The establishment of the ISI was thus seen as creating a research culture that will encourage students to undertake higher degree research.

A key theme that the ISI proposal put forward was to integrate student research with its own team-based, project-oriented approach, thus providing students with first hand experience of "real world" research activity. At the same time, the development of and support for academic supervisors of research oriented postgraduate students was seen as a vital factor in creating the ISI. In addition, the use of the quality assurance systems already implemented and used by the ISRC was seen as being a high priority for the Institute. At the same time, since each of the Faculties involved in the Institute already had a research training strategy in place, the ISI was seen as being in an ideal position to profit from best practice processes across those Faculties.

Cross Disciplinary supervision of research students within the ISI will be encouraged. The aim will be for each student to have a supervisor from more than one faculty.

Individual ISI researchers were seen as continuing to compete actively in competitive and other research granting schemes and contract research tendering processes to increase overall revenue. In addition potential commercialisation opportunities could now be pursued with increased vigour, co-ordination and support.

The focus of the ISI will be primarily on research projects and training postgraduate students at the research Master and Doctoral level. However, the availability of multi-disciplinary research staff within a single organisation provides QUT with an opportunity to develop multi-disciplinary information security coursework at both the undergraduate and postgraduate level. Currently, investigations are under way to develop a cross faculty coursework Masters degree. It is envisaged that, to obtain their degree, a student will be required to undertake major studies from at least two faculties. For example, a student would complete a postgraduate certificate in Business in the area of information assurance and a postgraduate certificate in Information Technology in the area of

information security. Each of these postgraduate certificates would be the equivalent of one semester of fulltime study. In order to obtain a coursework Master the student would be required to complete one further semester of postgraduate coursework in information security at an advanced level.

The establishment of the ISI was presented as adding significantly to the activities above through the integration of human and other resources. In addition, there will be substantial synergies achieved through a multi-disciplinary approach which will consolidate the sustainability of the ISI as a new collaborative research centre.

## VI. CONCLUSIONS

Training the next generation of recognised professionals and researchers in this emerging multi-disciplinary field will be a major and vital activity of the ISI. Through industrial partnerships, outreach programs and professional education activities in the areas of information assurance and security, risk assessment and management and other matters related to CIP/NIIP, the ISI will contribute to the development of the managers and technical practitioners who are responsible for safeguarding the nation's critical infrastructure. In particular, the ISI will enable interaction between key stakeholders in tertiary education, government and the private sector, both in Australia and overseas.

The important factors in the success in the formation of the ISI can be readily determined from the experience gained. These factors include:

- the ability to convince university management that a multi-disciplinary research institute as proposed would provide the level of attraction needed to create a "critical mass" of researchers and research in the area,
- demonstration that the ISI could provide a research facility in the interest of the nation and in line with research priorities clearly articulated by government,
- provision for accelerated processes in attraction, retention and successful completion of postgraduate, research student programs and projects, and
- clear articulation of a research theme in which many university research professionals could participate.

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE 