Malaysia's National Cyber Security Policy

The Country's Cyber Defence Initiatives

Mohd Shamir b Hashim
Government & Multilateral Engagement
CyberSecurity Malaysia
Kuala Lumpur, Malaysia
shamir@cybersecurity.my

Abstract— **The launching of Malaysia's Vision 2020 mark the country's journey towards becoming a developed nation and embracing the knowledge-based economy as a mean of achieving it. By consciously choosing to utilize the information and communication technology as a tool for development, it has resulted in the increasing use of digital information systems throughout the industry, the private and public organizations and the society at large. However, the dependency on digital information systems bring with it escalating vulnerabilities and risks, especially to the Critical National Information Infrastructure (CNII) which among others include cybercrimes such as Hacking, Intrusion, Fraud, Harassment, Malicious Code and Denial of Service Attacks.**

Acknowledging the growth of cyber threats that are endangering the e-Sovereignty of the nation, a cyber security policy was put in place.

The National Cyber Security Policy (NCSP) is Malaysia's comprehensive cyber security implementation to be done in an integrated manner to ensure the CNII is protected to a level that commensurate the risks faced. Cutting across the government machineries, the implementation has drawn in various ministries and agencies to work together to meet the vision of having a CNII that is secured, resilient and self reliant that will eventually promote stability, social well being and wealth creation for the country.

After 4 years of the NCSP implementation, the Malaysia's cyber security is now being looked as something to be reckon with. Much has been done and more need to be done as the landscape of cyber threats changes with the development of new technologies and tools.

Successfully implemented, Malaysia's CNII will be better placed to meet the challenges and opportunities that technological advancement brings and that it will help to achieve the objectives of Vision 2020 and beyond.

I. INTRODUCTION

Malaysia's journey towards a knowledge-based economy or the K-economy began with the launching of Vision 2020 by the Prime Minister of Malaysia in February 1991. Accompanied with the launch of the Multimedia Super Corridor and the acknowledgment of the importance of moving towards a knowledge-base economy, Malaysia consciously chose to utilize the information and communication technology as a tool for the country's development. The increasing use of the digital information systems throughout the industry, the public and private organization and the society at large is a realization of this conscious choice.

This increasing dependency on digital information systems brings with it escalating vulnerabilities and risks, especially to the Critical National Information Infrastructure (CNII) of Malaysia. These risks include cyber crimes such as Hacking, Intrusion, Fraud, Harassment, Malicious Code and Denial of Service Attacks.

II. DEVELOPMENT OF A NATIONAL CYBER SECURITY POLICY

In recognition of the growing cyber threats surfacing and endangering the e-Sovereignty of the nation, the Ministry of Science, Technology and Innovation (MOSTI) conducted a study on the development of a policy or guidelines to address cyber security issues facing the country. The study was conducted in 2005 by a conglomerate of consultants and with the cooperation of the relevant ministries and government agencies.

The objectives of the study were to:

- Assess the current situation of cyber security risks within the CNII sectors;
- Ensure that the critical infrastructures are protected to a level that commensurate the risks faced; and
- Develop and establish a comprehensive roadmap and action plans for the implementation of a Cyber Security Framework.

The outcome of the study was presented and accepted at the National IT Council (NITC) meeting on 7 April 2006, which was chaired by the Prime Minister. This decision was noted by the Cabinet of Ministers on 31 May 2006 and endorsed for implementation as the National Cyber Security Policy (NCSP).

The NCSP is a comprehensive cyber security approach that provides the perspective of how cyber security should be implemented in an integrated manner. This policy has a vision that states: "Malaysia's CNII shall be secure, resilient and self-reliant. Infused with a culture of security it will promote stability, social well being and wealth creation."

III. THE CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Malaysia's CNII is defined as: "Assets (physical and virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on the;

- National economic strength;

978-0-615-51608-0/11 ©2011 EWI

- National image;
- National defence and security;
- Government capabilities to function; and
- Public health and safety"

The policy further identified ten sectors in Malaysia, which are considered as the CNII. These sectors are:

- National Defence & Security;
- Banking & Finance;
- Information & Communication;
- Energy;
- Transportation;
- Water;
- Health Services;
- Government;
- Emergency Services; and
- Food & Agriculture

IV. POLICY THRUSTS

The NCSP is divided into eight areas, which are being referred to as the policy thrusts. A Thrust Driver, from the ministries that have the authority in the respective thrust areas, leads the thrusts with the assistance of their respective working group.

The eight Policy Thrusts and corresponding Thrust Drivers are as in the following table.

TABLE I. POLICY THRUSTS & DRIVERS

No	Policy Thrust	Thrust Driver
1	Effective Governance	National Security Council
2	Legislative & Regulatory Framework	Attorney General's Chambers
3	Cyber Security Technology Framework	Ministry of Science, Technology & Innovation
4	Culture of Security & Capacity Building	Ministry of Science, Technology & Innovation
5	R & D Towards Self-reliance	Ministry of Science, Technology & Innovation
6	Compliance & Enforcement	Ministry of Informatio, Communication & Culture
7	Cyber Security Emergency Readiness	National Security Council
8	International Cooperation	Ministry of Informatio, Communication & Culture

V. IMPLEMENTATION APPROACH

On the subject of implementation, the NCSP is divided into three phases with their respective objectives. These three phases are as follows:

A. The First phase

This phase addresses the immediate concerns and measures that can be taken to immediately implement cyber security such as identifying stop-gap measures to address fundamental vulnerabilities to the information security of the CNII. This is accompanied with the creation of a centralized platform that provides security mechanism and raising awareness of information security and its implications within the CNII.

B. The Second phase

This phase concentrates on building the infrastructure required for cyber security, which also include the setting-up of the necessary systems, processes, standards and institutional arrangements (mechanisms). In this phase, efforts will be given to build capacity amongst researchers and info security professionals.

C. The Third phase

This phase focus on maintaining the efforts provided in the first two phases such as developing self-reliance in terms of technology as well as professionals and monitoring mechanisms to ensure compliance. As these efforts are established, there is a need to evaluate and improve such mechanism and to create the culture of cyber security.

VI. POLICY GOVERNANCE STRUCTURE

Implementing a national policy like the NCSP will require a governance structure that involves the public and private machineries. In line with this, a national level committee was established to oversee the implementation of this policy. The committee called the National Cyber Security Coordination Committee (NC3) consists of senior officials from the ministries and government agencies responsible for the operation of the country's CNII. The NC3 was originally chaired by MOSTI. However in 2010, with the amendments to the duties of the ministers, the responsibility of the nation's cyber security is placed with the National Security Council. This led to the handing over of the Chair of the committee from MOSTI to the National Security Council.

CyberSecurity Malaysia continues to provide services as the secretariat to the committee under the leadership of the National Security Council. As the secretariat, this agency coordinates all efforts in implementing the NCSP and proposing the way forward to reach the vision.

Going upwards, the NC3 reports to the e-Sovereignty committee chaired by the Deputy Prime Minister, which in turn will report to the National IT Council (NITC) chaired by the Prime Minister.

VII. POLICY THRUSTS

As mentioned earlier, the NCSP is divided into eight areas of focus, which are known as thrust. Following are the descriptions of the thrusts.

A. Thrust 1 – Effective Governence

The policy recognizes the interdependent nature of the CNII that an impact on one sector will affect the others. Although some progress has been made in securing the CNII, there are still challenges that remain to be overcome.

The main objectives of this Thrust are:

- To have a centralised coordination of the national cyber security initiatives;
- To promote effective cooperation between the public and the private sectors; and

- To establish and encourage informal information sharing exchanges.

During the study, it was found that information security programs are not well coordinated as it was done by each entity to satisfy their own requirements and focus on their own mission. This has resulted in confusion, misunderstanding and overlapping of resources not to mention losing sight of the overarching national needs.

Trends are not monitored and risk profiles of cyber security remain obscure for the country. Therefore, a single cyber security coordination body was proposed to consolidate cyber security initiatives of Malaysia, which also include awareness activities. The body is identified as CyberSecurity Malaysia.

CyberSecurity Malaysia, an agency of MOSTI, provides central coordination and assists the government in identifying challenges and the minimum standards for cyber security.

In addition to having a centralized body, this thrust for effective governance sees the formation of national committees that oversees cyber security initiatives and condition of the country such as the NC3 and its working groups and the e-Sovereignty committee, which involves very high-ranking officers of the government.

B. Thrust 2 – Legislative & Regulatory Framework

This thrust looks at the legal area of the policy. The laws and regulations are very important to create trust and confidence in the CNII. The objectives of this thrust are:

- To review and enhance Malaysia's cyber laws to address the dynamic nature of cyber security threats;
- To establish progressive capacity building programs for the national law enforcement agencies; and
- To ensure that all applicable local legislation is complementary to and in harmony with international laws, treaties and conventions.

The NCSP is about protecting the CNII by ensuring the confidentiality, integrity and availability of information and the non-repudiation of communication. Therefore, the laws and regulations are vital in ensuring the advancement of information technology benefit the people and country and at the same time ensuring the CNII are protected.

The aim of this thrust is to have adequate legal system, which can adapt to the ever-changing landscape of cyber security. Thus the initiatives within this thrust is to define, categorized and penalized cyber crimes so as to deter future malice and to provide a comprehensive framework for the country to have the appropriate level of compliance to protect the CNII.

For this purpose, the existing laws need to be enhanced in order to effectively address the legal challenges of the present cyber environment. CyberSecurity Malaysia has spearheaded the review of the laws of Malaysia that provide a view of the existing legislative and regulatory framework with respect to cyber security. Malaysia has a range of existing legislations dealing with the cyber environment, which among others are:

- The Computer Crimes Act;
- The Digital Signature Act; and
- The Communication and Multimedia Act.

There are also some conventional laws that have implication on the cyber environment such as:

- The Penal Code;
- The Internal Security Act;
- The Sedition Act;
- The Defamation Act; and
- The Evidence Act.

The cyber law review looks at all these laws and provided recommendations on improvement that need to be made. The outcome of this review was given to the Attorney General's Office (AGC) whom is the Thrust Driver.

The amendments to the law is now currently in progress where the AGC is now working with the respective ministries that 'own' the acts. This exercise is not only a national agenda but also as part of an international framework where the review looks at the European Convention and laws of other countries on curbing common threats to the global community.

C. Thrust 3 – Cyber Security Technology Framework

Information security guidelines are abundant within the public sectors in Malaysia. However, most of these guidelines are informative in nature and not so much as providing mandatory or minimum requirements. This policy thrust, which is led by MOSTI, has the objectives of:

- Developing a cyber security technology framework that specifies information security requirements, controls and baselines for the CNII elements; and
- Implementing an evaluation/certification programs for information security products and systems.

A few years ago, the need for equipment and systems are based on individual requirements and not based on a baseline or standards approved by the government. Thus for most cases, cyber security controls are determined at a later stage which prove to be expensive and damaging to the network.

Cyber security framework defined the security controls that are needed. Security such as management, technical and operational controls will provide some assurance that some security measures are in place. These measurements will be base on the respective entities where it will commensurate with the impact on the operations, assets or individuals if security breaches occur with respect to the confidentiality, integrity or availability of information.

Presently, the working group of this thrust has recommended that all CNII entities of Malaysia adopt the MS ISO/IEC 27001-2007 Information Security Management System (ISMS) as a security baseline and to obtain the certification. After much deliberation, the Government of Malaysia has agreed to this proposal and issued an instruction in February 2010 that all Malaysian CNIIs are to be ISMS certified within three years.

Another major initiative under this thrust is the establishment of the Malaysia Common Criteria Evaluation and Certification Scheme (MyCC). Malaysia through CyberSecurity Malaysia has become a member of the

Common Criteria Recognition Arrangement (CCRA) since 2007.

The CCRA (www.commoncriteriaportal.org) is an international agreement, which ensures that:

- Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
- Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation; and
- All the signatories of the CCRA recognized these certificates.

Malaysia has been a certificate consuming member and has been audited to become a Certificate Authorizing Member last year.

CyberSecurity Malaysia recognized that implementing security evaluation such as the Common Criteria would enable buyers to procure IT technology with greater confidence. The Common Criteria also validate vendors' claims about security and enable network architects and security professionals to choose the right technology for the right role.

This kind of evaluation will reduce the need for the individual CNII entities to perform their own testing. This will improve competitiveness, speedier deployment of technology and decrease the risk faced by implementers of the technology.

Due to the nature of cyber security technology, regular updates and review of the framework will be undertaken to ensure that the most appropriate technology is deployed.

D. Thrust 4 – Culture of Security and Capacity Building

This is the one thrust that gives focus on the human aspect of the policy. The objectives of Thrust 4 are:

- To develop, foster and maintain a national culture of security;
- To standardize and coordinate information security awareness and education programs across all elements of the CNII;
- To establish an effective mechanism for information security knowledge dissemination at the national level; and
- To identify minimum requirements and qualifications for information security professionals.

The continuing changes in information technology requires greater emphasis on security by the CNII entities whom develop, own, provide, manage, service and use information systems and networks. The wireless and broadband technologies have contributed significantly to the increase in Internet users that has increased the exposure of the public to a variety of threats and vulnerability. This raise the need for greater awareness and understanding of security issues and the need to develop a culture of cyber security that will focus on security in the development of the network and the adoption of new way of thinking and behaving when using information system such as the internet.

The efforts to promote a culture of cyber security require leadership and involvement of multiple parties. This is the concern of all government ministries and agencies which have to be represented by a strategic roadmap depicting well planned and well managed programs.

With this in mind, CyberSecurity Malaysia conducted a study in 2010 titled the National Strategy for Cyber Security Acculturation and Capacity Building. The study focuses on the key aspect, which are the cyber security acculturation and capacity building.

The cyber security acculturation programs target the public by having a plan to inculcate best practices, good habits and behaviours on good and safe use of the Internet. This includes the development of content, the approach and implementation plan of the acculturation. On the capacity building, the target group are the CNII entities where the study provides a plan to get the organizations and individuals towards building a pool of information security professionals. This include the propose content for skill areas, the approach and the implementation of the plan.

The result of the study will overcome the lack of initiatives that can drive and increase the level of cyber security awareness through the necessary training and education strategies provided by the outcome. In addition, CyberSecurity Malaysia will promote the consideration of security as an important objective among all elements in government agencies, businesses and private sector.

While the study was being conducted, CyberSecurity Malaysia has embarked on a national awareness campaign branded as CyberSAFE. CyberSAFE, which stands for Cyber Security Awareness For Everyone, is a cyber security program targeting the general public. This program includes seminars, awareness talk and exhibitions in order to reach out to the people. To extend the reach further, this program has a portal (www.cybersafe.my) that contains cyber security video clips and free downloads of posters, magazines and articles. Recently, CyberSecurity Malaysia launched an extension program called CyberSAFE in Schools to reach to young generation, which comprises the major portion of Internet user in the country and the most vulnerable group.

The development of human resources is critical to the success of efforts to improve security. In order to achieve the vision of the policy, the public and private sectors must have personnel that are sufficiently and professionally trained in the technical and non-technical issues of cyber security.

CyberSecurity Malaysia has alliances with international certification bodies to conduct information security courses and certification to information security professionals of Malaysia. Among the organizations are:

- The International Information Systems Security Certification Consortium, Inc. $(ISC)^2$ which is the global, non-profit leader in educating and certifying information security professionals throughout their careers;

- DRI International and DRI Malaysia which is an institute on continuity management;
- The International Council of Electronic Commerce Consultant (EC Council) which is a member supported organization the offers various e-business and security certifications; and
- ISACA and ISACA Malaysia which is an independent, non-profit, global association engage in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems.

The certified professionals and certification bodies will promote the culture of cyber security and setting the minimum standards for those involved in the information security knowledge processes.

E. Thrust 5 – Research and Development towards Self Reliance

In achieving the objective of this thrust, the CNII of Malaysia is protected by an integrated research and development framework that focuses on technology with the aim of being self-reliant.

The objectives of this thrust are:

- To formalize the coordination and prioritization of cyber security research and development activities;
- To enlarge and strengthen the information security research community;
- To promote the development and commercialization of intellectual properties, technologies and innovations through focused research and development; and
- To nurture the growth of information security industry.

The study on NCSP found that there was a lack of cyber security coordination and prioritization at the national level. This has cause research agendas and programs not to be systematically managed which cause important priorities to be overlooked. Determining the research areas is of paramount importance. A clear identification of priority areas is required to prevent uncoordinated research efforts where individual entities and research institutes focus on individual missions that may not meet the overarching national needs and priorities.

There is a need to have a central entity to coordinate and prioritize the current and future R&D agenda of the nation. In light of this, MIMOS an agency of MOSTI has been assigned the task. This agency will align and integrate R&D programs and initiatives to avoid duplication of efforts and to encourage collaboration where appropriate.

Since assigned this task, MIMOS has developed the National R&D Roadmap for Self Reliance in Cyber Security Technologies. This plan was formulated by MIMOS and a consortium of 22 organizations representing the academics, government, industry and researchers with the goal of aligning and integrating all R&D programs and projects related to cyber security. This will avoid duplication of efforts and to encourage collaboration, where appropriate, between academia, industry and government. Driven by an integrated R&D framework, the roadmap focuses on technologies that protect the country's CNII with the aim to achieve self-reliance in those technologies.

The R&D efforts are aimed at countering threats to the CNII by making improvements to the current capabilities and also by developing new ones. This is achieved by intensifying efforts to promote cyber security research at learning institutions to increase the size of cyber security research community.

With the national R&D Roadmap, it will churned revolutionary ideas rather than steady advancement in the field.

Another matter that is important is the intellectual property as an outcome from the research activities. It is vital that the country is able to protect home grown intellectual property because this will provide the environment for future creation and development of the original works and finally stimulate greater economic growth and entrepreneurial activities.

F. Thrust 6 – Compliance and Enforcement

The Ministry of Information, Communication and Culture (MICC) is driving this thrust. One of the reasons is because major information and communication regulator which is the Malaysian Communications and Multimedia Commission and CNII entities such as Telekom Malaysia, Maxis, Jaring to name a few are under the purview of this ministry.

The objectives of this thrust are:

- To standardize information security systems across all elements of the CNII;
- To strengthen the monitoring and enforcement of standards; and
- To develop a standard information security risk assessment framework.

Interdependencies across the CNII are complex such as no telecommunication organization can work without power and no financial institution can operate effectively without telecommunications. As the 10 CNII sectors of Malaysia are inter linked and reliant upon one another, a weakness in one sector can often translate into a weakness in all sectors. Therefore it is vital importance that all ten sectors achieve a minimum level of information security and that this achievement is independently verified.

MICC and the working group of NCSP Thrust 6 provides independent cyber security audits and other control mechanisms where the information will be use to monitor compliance, set baselines and identify trends. This will assist in identifying the sectors that need help in meeting the security baseline.

The Thrust 6 working group has develop a risk assessment framework for the CNII to use in identifying risk within their respective IT systems. This will help the entities to understand their own risk profile by using similar, acceptable and comparable techniques to identify risk. The uniformity in using the framework will allow the identification of trends, strength and weaknesses. Apart from allowing the working group to identify the critical systems that need to be secured, it will also provide assistance, focus resources and drive R & D initiatives. This is supported with

the annual risk assessment survey to monitor the progress of managing the threats and vulnerabilities.

The government of Malaysia has imposed the requirement of having the CNII entities to be ISMS certified by 2013. In ensuring compliance to the requirement, the working group Thrust 6 and 3 are working together to provide awareness on ISMS and the certification processes.

G. Thrust 7 – Cyber Security Emergency Readiness

The Computer Emergency Response Teams (CERT) or the Computer Security Incident Response Team (CSIRT) is an instrumental set up in mitigating cyber security incidences. CyberSecurity Malaysia hosts the Malaysian CERT (MyCERT), which monitor the cyber security threats in the country's cyber environment.

The objectives of the NCSP Thrust 7 are:

- To strengthen the national CERT;
- To develop effective information security incident reporting mechanisms;
- To encourage all elements of the CNII to monitor information security events;
- To develop a standard business continuity management framework;
- To disseminate vulnerability advisories and threat warnings in a timely manner; and
- To encourage all elements of the CNII to perform periodic vulnerability assessments programs.

Presently many organizations within the CNII do not report cyber security incidents. Although the increase in education and awareness will help, the existing incident response centre need to be strengthen to be able to provide the appropriate response.

Effective cyber security monitoring is not prevalent across the CNII. However, vigilant monitoring and correlation of data at the national level are crucial elements to ensure security incidents are identified and managed properly.

In view of this issues, the National Security Council whom is the driver of this Thrust has developed the National Cyber Crisis Management Plan (NCCMP) with the purpose of outlining the strategy that Malaysia will undertake in mitigating and responding to cyber incidents through the public and private collaboration and coordination.

Tied to this plan are the cyber drills co organized annually by the National Security Council and CyberSecurity Malaysia. The drill is to test the procedures and processes stated in the plan. All kinks are iron out to ensure continuous improvement to the NCCMP. The drills also observe the reaction of participating CNIIs and the flow of information. It is critical to ensure that all cyber security related information gathered be disseminated to all the relevant CNII sectors as and when needed. Therefore, vulnerability advisories and threat warnings can and should reach everyone in a timely and efficient manner.

H. Thrust 8 – International Cooperation

The cyber environment does not conform to the physical boundaries of the countries thus successful cyber security initiatives require international cooperation. Sharing intelligence, research, best practice, discussing challenges and learning from other mistakes as well as helping to formulate and drive international policy direction and initiative will help Malaysia to secure the CNIIs.

The objectives of this thrust are:

- To encourage active participation on all relevant international information security bodies, panels and multi-national agencies;
- To promote active participation in all relevant international information security events, conference and forums; and
- To enhance the strategic position of Malaysia in the field of information security by hosting an annual international information security conference.

The active participation in all relevant international cyber security bodies, panels and multi-national agencies will help to ensure that the country has a hand in driving the international cyber security agenda.

Under the spirit of this Thrust, Malaysia is the co founder of the Asia Pacific Computer Emergency Response Team (APCERT - www.apcert.org) and has played an active role since the formation. CyberSecurity Malaysia, acting on behalf of Malaysia has held the Chair and Secretariat position in providing leadership to the collaboration. Now CyberSecurity Malaysia is one of the steering committee members.

On a more active role, Malaysia through CyberSecurity Malaysia, spearheaded the formation of the Organization of Islamic Conference Computer Emergency Response team (OIC-CERT – www.oic-cert.net) in 2005. Now with 18 member countries and an affiliated institution of the OIC, Malaysia is at the helm holding the Chair position and providing the leadership required.

In addition to these major multilateral engagements, Malaysia participated in other information security events conducted by international organization among them are ITU, APECTEL, the Meridian Conference, FIRST, and APWG. On home ground, CyberSecurity Malaysia organized annual conferences such as the Cyber Security Malaysia Award Conference and Exhibitions (CSM-ACE).

VIII. LESSON LEARNED

With the dependent on IT infrastructure resulting to the increase in cyber incidents, it is a right move for MOSTI to conduct a study on the requirement of a national policy to mitigate such incidences. The NCSP aims at enhancing the security, resilience and self-reliance of Malaysia's CNII to promote stability, social well being and creating wealth.

In implementing the policy, the keys to success are;

- Effective governance and coordination with the establishment of a single coordination centre which in this case is CyberSecurity Malaysia. This has created organization clarity and accountability;
- Improving the public private cooperation;
- Improving the information security skills and capacity;

- Enhancing the existing research & development initiatives toward self-reliance;
- Map out the emergency readiness;
- Dictates the program for compliance and assurance across the whole of CNII; and
- Reaching out to international partners.

As a whole, the NCSP aims to improve trust and cooperation in the CNII for the benefit of the people of Malaysia.

REFERENCES

[1] Ministry of Science, Technology and Innovation, Malaysia, "National Cyber Security Policy: The Way Forward," Federal Government Administrative Centre. July 2006. (references)

[2] UK Office of Cyber Security, "Cyber Security Strategy of the United Kingdom : safety, security and resilience in cyber space" Office of Public Sector Information, Information Policy Team, June 2009. (references)

[3] United State, Executive Office of the President "Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure," United State, Executive Office of the President, May 2009. (references)

[4] Ministry of Science, Technology and Innovation. "National R&D Roadmap For Self Reliance in Cyber Security Technologies." Unpublished.

[5] ISACA and the IT Governance Institute. ISACA Overview. Retrieved April12, 2011. From http://www.isaca.org/About-ISACA /History/Pages /default.aspx

[6] **(ISC)² .** About (ISC)²**.** Retrieved April 12, 2011. From https://www.isc2.org/aboutus/default.aspx

[7] Ec-Council . About us. Retrieved April 12, 2011. From http://www.eccouncil.org/about_us.aspx