An approach to establish a Center of Excellence in Information Security

Khaled Alghathbar
ghathbar@ccis.ksu.edu.sa
Information System Department, Center of Excellence in Information Security
Collage of Computer and Information Science,
King Saud University, Saudi Arabia

Summary
With the adoption of advanced information technology around the world where it relates directly to our productivity, success and heath, it is crucially important to tightly secure these fast-growing technologies to ensure sustainable development. The most important strategy to secure information technology is to conduct relevant research on developing more effective methods and novel products to ensure information security and reliability. It is also crucially important to create awareness and educate common people to understand the importance of securing information and to make them able to properly utilize the available technologies. This is the role of the center of excellence in information security at King Saud University as well as other centers worldwide that group multidisciplinary researchers to coordinate in tackling multitude problems of information security. We have taken an initiative to establish a center of excellence in information security at King Saud University with the aim to promote quality research and education in the field of information security. This paper summarizes the overall approach including center vision, mission, goals, philosophy, structure and other aspects. A brief account of infrastructure and expertise of well known information security centers around the world is also presented.

Key words:
Center of Excellence; Information Security; Strategic Plan; Education; Case Study; Viewpoint.

1. Introduction

It became known the importance of information technology (IT) on the scale of individual, society, government and companies, and how it impacts economy, policy and culture. Information technology can increase the gross domestic product, raise the productivity in many sectors up to 74%, diversify sources of income and provide new jobs with highly paid salaries [9]. These factors encourage governments around the world to increase the investment and prioritize spending in information technology. The government of Saudi Arabia has timely realized the roles of IT in National interest and has come forward to join the common tracks with the pioneers in IT field. The recent allocation of SR3 billion to set up infrastructure facilities for 150 e-government and 1,000 subsidiary services by 40 government agencies within the next five years shows the keenness of Saudi government to develop our IT sector in parallel to leading IT countries [9]. However, failing to secure such IT services or data may result in negative impact on people, organization and the adoption of technology. The fast growing digital world is now highly vulnerable to constantly changing security threats resulting in serious consequences. If these threats are not tackled meticulously, the implication of IT services would be severely hampered. Information security is not limited to antivirus software and passwords; it goes beyond this to different angles and spectrum from social engineering to cryptanalysis. Also, information security is an integral part of the national security and therefore investment in this field from educating society and training qualified people to building products for critical mission is highly demanded.

Being located in the largest and the capital city of Saudi Arabia, King Saud University (KSU) hosts the first college for computer and information sciences in the Middle East and the founder of the Saudi Computer Society. KSU hosts the largest number of faculty members specialized in information security in Saudi Arabia and in the region either in the college of computer and information sciences or in other colleges such as college of engineering, college of sciences and college of business. For many years, these faculty members have been providing consultation, research and studies to government and private sectors in the field of information security, in addition to their role in educating students and society. Having the advantage of the wealth and diversity of specialized faculties, KSU has realized the urgent need of a national source of high-quality research and education in information security and has come forward with a pledge to establish the Center of Excellence in Information Security (CoEIS). The proposed center is raised as an internationally recognized

Manuscript received March 5, 2008
Manuscript revised March 20, 2008

center of excellence in information security and the first source of expertise in the region in the field of Information security. This mission is achieved by grouping top quality information security researchers and professionals to transfer knowledge and assess and solve information security problems for flawless functioning of IT machinery. CoEIS goals aligns with the National Information and Communication Plan (NICTP), where CoEIS meets all the major goals of the plan in general and two in specific, fulfils 8 execution policies, and can effectively undertake partial or full role of 12 out of 24 projects specified by NICTP.

This paper highlights the establishment approach and strategic plans of the CoEIS with the aim to share our experiences with other parties to promote research and education in information security around the world.

2. Background

The term Centers of excellence (CoE) can be defined as follows:

"Physical or virtual centers of research which concentrate existing capability and resources in order to enhance the pursuit of excellence, typically on Research and Development (R&D)"[10]. "These enable personnel to collaborate across disciplines and institutions on programmes or projects that are locally relevant and/or internationally significant."[7]

In corporate side: "An organizational unit that embodies a set of capabilities that has been explicitly recognized by the firm as an important source of value creation, with the intention that these capabilities be leveraged by and/or disseminated to other parts of the firm" [11]

CoE brings group of researchers from multi-disciplinary areas in many universities under one virtual roof for a specific research focus [3]. Moreover, it brings a new form of investment that targets a layer between basic research fund and venture capital for commercializing services and products [12]. CoE opens a channel between researchers and the industry for potential products or services.

3. Related work

There are several information security centers running around the world; each of them is specialized in particular research topics depending on the researchers' expertise and the research grants they receive. This section will highlight several well known information security centers and their specialties.

3.1 The Center for Education and Research in Information Assurance and Security

The center for Education and Research in Information Assurance and Security (CERIAS) [12] in Perdue University is specialized in education and research in information security. It offers educational program at master and doctoral degrees as well as other services like workshops, courses, seminars for computer-based training. It focuses one wide spectrum research topics from technical to ethical, legal, educational, communicational, linguistic, and economic issues. This spectrum is the result of the collaboration of more than 20 departments across the Purdue University. The following are the research topics CERIAS covers:

- Risk management, policies, and laws
- Trusted social and human interactions
- Security awareness, education, and training
- Assured software and architectures
- Enclave and network security
- Incident detection, response, and investigation
- Identification, authentication, and privacy
- Cryptology and rights management

The mission of CERIAS is to advance the knowledge and practice of information assurance and security through the performance of world-class research, the delivery of the highest quality education, and by serving as an unbiased source of information locally, nationally and internationally. The goals of CERIAS are summarize below:

- Empower faculty and research staff from diverse disciplines to address information security problems, formulate research and education solutions, and secure funding and support.
- Strengthen meaningful partnerships with Discovery Park and its affiliated centers.
- Establish and advance the scientific rigor of the field.
- Discover, develop, and transfer technologies, methods, and information that enhance practice in the field.
- Establish CERIAS's prominence as a leader in the development and delivery of educational curriculum from K-12 to graduate programs and continuing education and training.
- Engage industry, government, and other academic institutions as awareness, education, and research partners.

3.2 Information Security Institute

Information Security Institute (ISI) [5] is one of the specialized research centers in Queensland University of Technology, Australia. Similar to CERIAS, ISI relies on

the collaboration of Faculties of Built Environment and Engineering, Business, Information Technology and Law. The vision of ISI is to make a real difference by establishing the institute as an internationally recognized centre of excellence in information assurance and technology policy as a strategic resource for government, business and community alike. The research focus of ISI covers the following areas:

- Cryptology
- E-business and e-government
- Technology, law and policy
- Speech, audio, image and video technologies
- Trusted systems and network security
- Governance and information protection
- Computer intrusion, forensics and evidence
- Risk and crisis management

3.3 Georgia Tech Information Security Center

Georgia Tech Information Security Center [4] concentrates on research and education with the vision that effective information security in context of real-world problems could only be achieved through user-centered approaches that integrate technology research with policy research. The missions of the center are summarized below:

- Invent and evaluate the key innovative user-centric security technologies and policies that will yield significant impact.
- Educate future researchers, policy makers, and information security leaders, and train current professionals in the most up-to-date methods for securing information systems.
- Provide a trusted set of resources and a safe haven where individuals and industrial, academic, and government organizations can access, understand, and evaluate issues related to new technologies and policies.

3.4 National Information Assurance Training and Education Center

The National Information Assurance Training and Education Center (NIATEC) [8] is associated with Idaho State University and focuses on education. It is a consortium of academic, industry, and government organizations to improve the literacy, awareness, training, and education standards in information assurance technology.

3.5 Information Trust Institute

Information Trust Institute (ITI) [6] of University of Illinois at Urbana-Champaign with over 80 researchers provides research and education in information security with industrial collaboration. The thrust areas of its research are summarized below:

- Critical infrastructures and homeland defense
- Embedded and enterprise computing
- Multimedia and distributed systems

ITI accommodates seven major centers:

- The Boeing Trusted Software Center
- CAESAR: the Center for Autonomous Engineering Systems and Robotics
- the Center for Information Forensics
- NCASSR: the National Center for Advanced Secure Systems Research
- the NSA Center for Information Assurance Education
- TCIP: the Trustworthy Cyber Infrastructure for Power Center
- Trusted ILLIAC

3.6 Center for Applied Cyber Security Research

Center for Applied Cybersecurity Research (CACR) [1] is one of Indiana University's research centers and works to enhance the security and integrity of information systems, technologies, and content by facilitating research and education informed by, and integrated with, the practice of information assurance. The center's goals are summarized as follows:

- Serve as a meeting ground for cyber security scholars, teachers, and practitioners from all campuses.
- Provide a clearing house for information on cyber security research, teaching, and practice at Indiana University.
- Link Indiana University faculty and staff with external resources in cyber security and related fields.
- Seek funding for cyber security research, instruction, and practice at Indiana University.
- Facilitate advanced cyber security research and the sharing ideas and information both inside and outside of the university.
- Help coordinate the development of an innovative undergraduate, graduate, and continuing education cyber security curriculum, including degree and joint-degree programs.
- Improve the practice of information assurance at Indiana University and elsewhere by drawing on the results of research in cyber security and related fields.

- Partner with federal and state governments, business, and other education institutions to improve the quality of information assurance practice, research, and teaching.

3.7 Center for Secure Information Systems

Center for Secure Information Systems (CSIS) [2] of George Mason University aims to be one of the leading academic institutions for research in Information Systems Security. It works collectively with academic institutions, industrial and government organizations to advance the state of the art in information systems security, and to provide an environment for education and training in Information Systems Security.

4. Strategic Plan

4.1 Vision

To be an internationally recognized center of excellence in information security and the first source of expertise in the field of Information security in this region.

4.2 Mission

To set a group of top quality information security researchers and professionals to share/transfer knowledge, assess potential threats and find out effective solutions to ensure unrestricted information security.

4.3 Goals/Objectives

4.3.1 Targeting researches to assess and solve information security problems in Saudi Arabia
Definitely, there are many thrust areas of research to timely address and mend Information Security risks in Saudi Arabia. The center will draw the researchers' attention to target national information security problems starting from assessing and evaluating critical systems in Saudi Arabia to developing policies, procedures and guidelines to solve existing problems in Information Security.

4.3.2 Innovative solutions in Information Security.
The center focuses on teamwork efforts by establishing worthy groups of talented researchers and professionals to innovate new solutions and techniques that address client problems and demands.

4.3.3 Transfer the knowledge of Information Security by holding international workshops and training.
It is one of the major concerns of the center to mutually transfer the knowledge of Information Security to Saudi Arabia by providing high quality and specialized training course, workshop and conferences.

4.3.4 Increase public's awareness of Information Security.
It is essential to ensure the public awareness about Information Security and how to defend themselves from vulnerabilities and threats. The importance of security-related awareness has increased with the new e-government transaction initiative in Saudi Arabia where transactions will be made electronically; this will attract more and more people to use the Internet with time to come. The center will utilize different types of media to increase the awareness such as public lectures, conferences, books, posters, websites, articles and contributions to textbooks of general education.

4.3.5 Provide world class post graduate programs in Information Security.
The center works in concert with local universities to enrich its curricula with Information security courses. Highly-ranked PhD programs are ensued by joint ventures with local and international universities. A post graduate program (Certificate, Master of Science Degree) in Information Security is established by building a partnership with international universities.

4.3.6 Provide professional services in Information Security.
The center provides specialized professional services in Information Security to government agencies and companies by utilizing its wide range of expertise.

4.3.7 Establishing a society for Information Security professionals and experts.
The center aims to encourage the specialization in the field of Information Security and to provide the proper infrastructure to group together the professionals in Information Security by having regular meetings and job portal.

4.3.8 Partnering with industry to enhance and develop solutions.
The center refutes the policy of competition with other companies but rather complements their efforts and encourages them to develop innovative ideas jointly for industrial and national development.

4.3.9 Assessment of information security policies, law and regulations.
The center helps to assess the current national policies, laws and regulations related to information security and

provide recommendation toward enhancing current laws and/or introducing new laws.

4.3.10 Encouraging the research and development in information security.
We encourage researchers and graduate students to perform researches and developing new products and services in information security in order to be recognized as one of the best world research centers in information security that will also attract international companies to cooperate with the center.

4.3.11 Enriching content in Arabic in the field of information security.
We intend to encourage and develop Arabic content in the field of information security either in translating or developing new local specific content in the form of website, newsletter, brochure, books, papers, etc.

5. CoEIS alignment with the National Plan

This Section highlights the relationship between the CoEIS and the National Plan for Information and Communication Technology (NICTP) in Saudi Arabia. The vision of NICTP is "To change to informatics society, digital economy, improve productivity, provide communication and information technology services to all spectrum of society in all over the country, and to build a strong industry in this sector to be one of the main sources of income". The CoEIS is working toward meeting this vision by helping in producing Arabic content in the field of information security, helping people, government and companies working with technology in a secure way that protect their investment (economy), sustain their productivity and building trust in communication and information technology services. In addition, the CoEIS will work on educating qualified engineers to be specialized in information security, encouraging talented people and transforming fruitful ideas of information security to entrepreneurs and products (Made in Saudi Arabia). Also, CoEIS aligns generally with the 7 main goals of the NICTP and specifically with two of them as follows:

1. Building ICT industry that is strong and competitive locally and globally through scientific research, innovation and improvement in strategic areas, and local and global collaboration, to be a main source of income.
2. Providing trained human resources from both genders in ICT fields by proper training, education from the expert in the fields.

The mission and goals of CoEIS aim at fulfilling the above two main goals in specific and all other main NICTP goals in general in the field of information security. Moreover, CoEIS will fulfill several execution policies of the NICTP in specific as follows:

- Securing the network and the information of individuals and organizations.
- Supporting the localization of ICT.
- Funding innovation projects in ICT.
- Sponsoring talents and encouraging their efforts in ICT.
- Supporting ICT studies and research.
- Increasing the local digital content.
- Supporting the electronic translation and arabization.
- Providing qualified and specialized workforce in ICT.

Finally, NICTP named 24 projects to fulfill the plan; CoEIS can effectively play part or full role of 12 of them as follows:

1. National center of public key infrastructure.
2. Cyber crime law.
3. Privacy law.
4. Cyber crime unit.
5. Saudi Arabian Computer Emergency Response Team (CERT).
6. Technology transfer centers.
7. Specifying funds for research and innovation projects in government sectors.
8. Encouraging young people to develop ICT products.
9. Establishing ICT research center.
10. Digital local content initiative.
11. Establishing higher education institute of excellence in ICT.
12. Developing Master degree jointly with ICT and other fields.

6. CoEIS Advantages

6.1 To KSU

- Enhancing research in information security.
- Enhancing the graduate studies in KSU.
- Encouraging students to focus on information security.
- Filling the gap between academia and industry.
- Supporting the learning capabilities by having hands-on labs.
- Exposing the students to top quality expertise in the information security.

- Providing an environment for multi-disciplinary graduate program.

6.2 To the Society

- Increasing the awareness among the society.
- Providing information security guidelines for protecting computers.
- Providing trustworthy source of knowledge regarding information security.
- Supporting organizations in securing their systems.
- Improving the information security bylaws.
- Improving the national security.
- Encouraging talents and innovations.
- Solving national problems.
- Supporting collaboration and communication among information security professionals.
- Promoting information security professionalism.
- Encouraging the applied research in information security.

7. KSU Strength

KSU is the first and largest university in Saudi Arabia. It was established 50 years ago and holds:

- 22 colleges (Multi-disciplinary).
- 36 scientific societies.
- 15 research centers.
- Specialized centers:
  - Prince Sultan Research Center for Environment, Water and Desert.
  - Earthquake Studies Center.
  - Nano Technology Center
  - Center of Excellence in Engineering Material
- 3,000 faculty members.
- 70,000 students.
- The first and largest computer college in Middle East.

KSU is located in the capital of Saudi Arabia where all the government ministries and gencies and the main business and corporate sectors are located. The co-existence of such vast IT-dependent establishments in the capital city strongly favors the initiative of KSU to establish a top-quality Center of Excellence in Information Security that will be the first of its kind in this region.

8. Operation Philosophy and Methodology

8.1 Scope of work

The center plans to concentrate on three main areas: Research & Development, Consultation and Education (Figure 1). Each division will have its own leader and team and all of them will complement each other for smooth and well-organized running of the center towards achieving the common goals.

Figure 1. Main concentrations of CoEIS

8.2 The philosophy

After surveying the status and pace of research in Saudi Arabia, we have found that interest in research is not high for different reasons that can be summarized in three main categories:

1. Low incentives and funds for research.
2. Insufficient research supporting staff and infrastructure.
3. Lack of links between researcher and industry and poor marketing.

Thus, our proposed project of CoEIS will effectively tackle these obstacles and boost the overall research and development in information security. The philosophy behind running the center is summarized in Figure 2.

The philosophy is based on three pillars: Excellence, Knowledge Transfer and Collaboration. The significance of these pillars is highlighted below:

8.2.1 Excellence

As the name of center implies, the output of center must be highly ranked in parallel to a certain level of excellence with a keen ambition of reaching par excellence. However, achieving excellence is a highly

challenging task which requires creation of a suitable environment to attract, harbor and sustain excellent personnel (employees) for executing long-term policies. Today the demand for IT people in Saudi Arabia and other regions of the world is much higher than their availability rendering quick transitions of IT professionals from one company to other for better incentives. Thus owing to scarcity of experts, competitive salaries and benefits are provided to ensure sustained services from highly competent and dedicated researchers in the field of IT, particularly in the specialty of information security.

Having the pledge of building and maintaining excellence activities in the center, we will specifically recruit top-notch professionals and well-established researchers in information security. We intend to meet this challenge by three solutions:

1- Running the center with enough flexibility with regard to financial and human resources bylaw, but with proper control and accountability. Thus, having its own laws and regulations approved by the university.
2- Offer lucrative compensation for the center's employees above the market average.
3- Investing in new blood by providing them with proper training and environment, in addition to taking advantage of the current and visiting experts in the center.

Figure 2. Philosophy pillars of CoEIS

8.2.2 Knowledge Transfer

It is an obligation on the center to further and transfer knowledge and encourage its dissemination. The center will try to achieve this by the following:

- Holding or participating in public events such as national/international conferences and workshops. Or holding public meetings for interested individuals and organization to discuss hot topics and encourage networking people and organizations to transfer the knowledge.

- Providing consultation to individuals and organizations in the field of information security, trying to provide best practices and recommendations.
- Encouraging and playing an active role in teaching information security at the higher education level and incorporating important parts of information security in the general education textbooks for the younger generation.
- Running awareness campaigns about information security in different levels and channels such as posters, screensaver, brochure, books, radio, TV, workshops, executive awareness sessions, etc.
- Offering world-class training to individuals who would like to change their career to information security, and to those who would like to be more competent in information security. The center aims at cooperating with leading institutes and/or instructors.

8.2.3 Collaboration

For a strong and optimized development, the center aims at collaborating with different bodies, such as research centers, universities, government and industry either local or international (Figure 3). The goals of this collaboration are as follows:

- To start from where others reached.
- Learn from others' faults and successes.
- Providing excellent research, services and products.
- Working on people/organization needs.
- Transferring the knowledge.

8.2.4 Overlap

Overlapping these pillars result in five outputs:

- Discovering talents and encouraging them.
- Tackle all the real problems of industry or government rather than out focusing less important or individualized problems.
- Encouraging research and development in information security and be a competent and trustworthy center specialized in information security.
- Offering Master Degree and Diploma in information

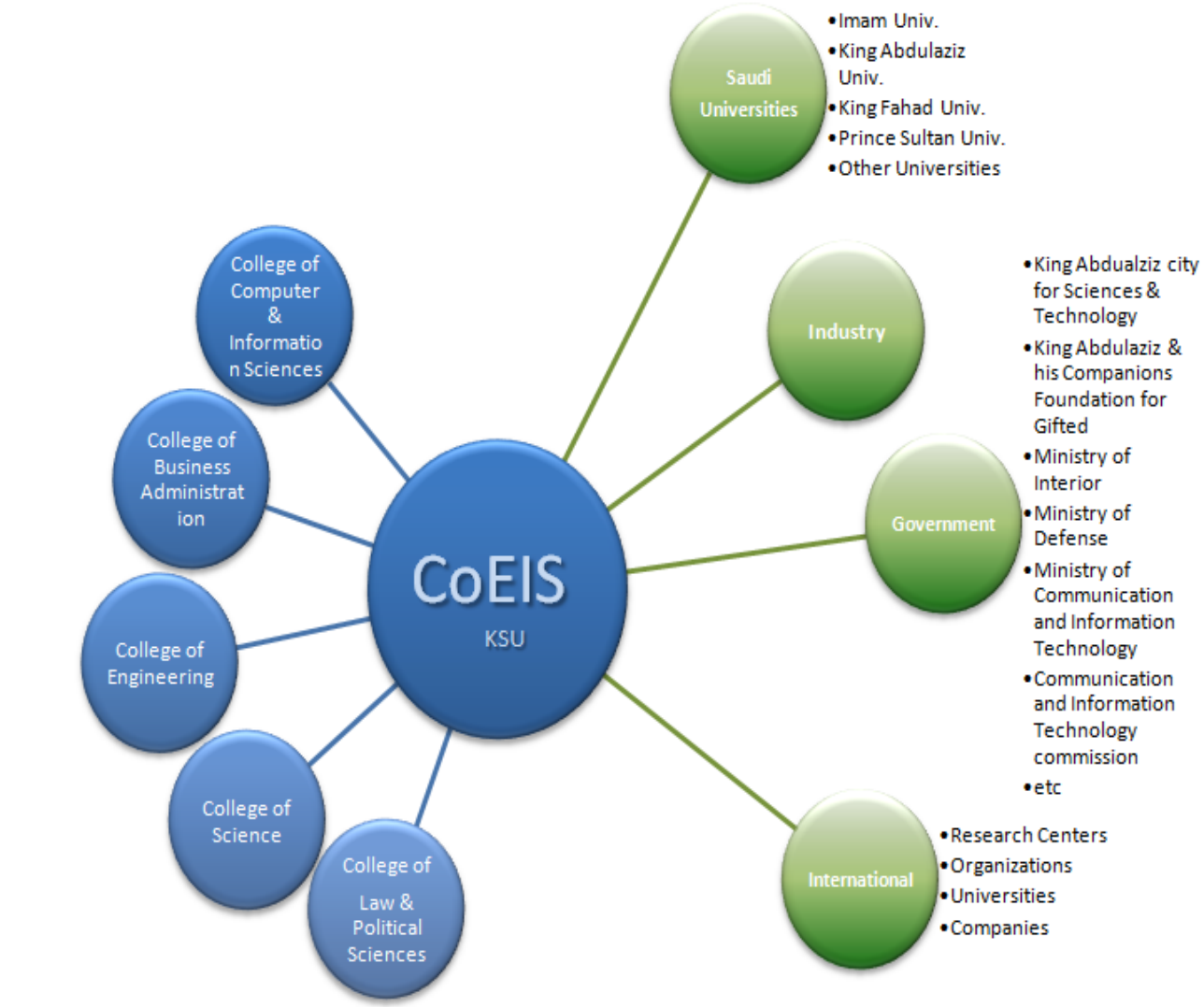


Figure 3. Collaboration entities

security by twining with other leading institutes and universities around the world.

9. Research Programs, Activities and Focus

9.1 Research Programs

9.1.1 Information Security Management and Governance

Security management and governance ensure that the information security measures implemented meet and align with the organization needs and goals; those measures can be people, product and process combined together. It not only focuses on product and technology but also on management and their involvement and integration in supporting IT security. The program will concentrate on research related to information security governance and on encouraging local government and companies to adopt and implement it. The program will cover security standards like ITIL, ISO 17799, COBIT and Six Sigma, and applying them to information security program management and governance. Also, the program will research on the regulatory compliance management and planning such as Sarbanes-Oxley, HIPAA. In addition, the program will focus on designing and implementing effective information security policies, procedures and guidelines and ways to integrate them into organization.

9.1.2 Risk Assessment and Management

Most aspects of information security are not absolute rather include varying degrees of multiple factors and situational diversity. Risk assessment involves identifying potential security threats and their likelihood. Risk management attempts to improve the security, reliability and availability of IT functions by developing safeguards to protect against viable security threats and drafting detailed security policies and procedures to eliminate or mitigate the potential threats. Risk assessment and management can provide a unified way of viewing and modeling various degrees of information assurance, and can be used as basis to detect anomalies and predict possible compromises. Security requirements are often situational and may change with system load, with the value of communicated data, with ongoing activities, etc. This research program will focus on exploring dynamic risk management techniques which allow the system to adapt to changing situations in a unified systematic fashion while taking into account the cost of loss. The program will study risk assessment and management techniques and develop automated tools for assessing and analyzing risk. These tools will check audit trails, measure various security parameters in a distributed fashion, and react appropriately by deploying effective countermeasures to respond to perceived exposures.

9.1.3 E-Government and E-Business Security

Every government and business that introduce computing services is subject to E-Government and E-Business Security which include identity management (identification, authentication and authorization), logging and auditing actions, protecting data on transit and at rest, the availability of services and information and trust (digital signature, encryption and non-repudiation) in addition to secure programming and designing.

9.1.4 Cryptography

Researching new cryptographic methods and applications, theoretical foundations of cryptography, design and implementation of cryptographic protocols and focus on developing secure product for encryption and authentication.

9.1.5 Testing and Validating Security using High Performance Computing

Many cryptographic algorithms and security prototypes cannot be accurately tested and validated without substantial computing resources for modeling and simulating different attack patterns and subversion techniques. This research program aims at establishing collaboration between the security research community and high performance computing (or grid computing) community in order to develop high-performance test-beds that are suitable for testing and validating advanced security techniques. High performance computing will be a key in providing the necessary processing power for fully assessing operational system security including penetrability and complexity of secure systems and components.

9.1.6 Intrusion Detection

Intrusion detection indicates the possibility of compromised data or the existence of compromised data in the network and indicates the possibility of security attacks upon the network. This research program will focus on system monitoring and intrusion/anomaly detection using conventional tools and new techniques like “compromise containment” which prevents propagation and typically involves the manipulation and change of firewalls, access lists, capabilities, encryption algorithms and keys. The research will include “damage assessment” for evaluating the costs, impact, and sources of intrusion. The research will cover “damage repair”

and "compromise isolation," where the compromised components of the network are returned to a secure state or are prevented from compromising the other components.

9.1.7 Forensic and Computer Crimes

The usage of the computer and the Internet increases day by day, so does the crimes over the cyber world as it provides new dimension for criminals to launch new crimes or use it as a new channel of communication. Thus, there is a need for research on computer forensics from policy, procedure and strategy to recovery, evidence reconstruction and analysis to countermeasure cyber crimes and finding evidence in an electronic form.

9.1.8 Security for Ubiquitous Computing Environments and Embedded Devices

The confluence of high-speed networks, mobile devices, intelligent environments, high-resolution displays, smart spaces, sensors, actuators and embedded real-time systems promises a new model for distributed interaction and information sharing, with all the concomitant security and privacy challenges. The research vision in this program aims at developing context-aware adaptive security services and mechanisms that are suitable for these types of environments. In dynamic, adaptive distributed systems, like smart spaces, various components may join and leave the system extemporaneously. New control elements, as well as new types of objects may introduce relationships that are not part of the existing security policy ontology. The research involves developing theories and toolsets for the fusion, analysis and understanding of composite, heterogeneous and potentially orthogonal policy domains. Furthermore, the research will focus on building security mechanisms that adapt themselves according to the current situation and context, while supporting the emerging models for distributed interaction and information sharing.

9.1.9 Security for Ad-hoc and Sensor Networks

A sensor network consists of spatially distributed wireless autonomous devices that use sensors to cooperatively monitor physical or environmental conditions, such as temperature, pressure, motion or pollutants, at different locations. Sensor networks represent an active research area with many useful applications including environment monitoring, healthcare applications, home/office automation, traffic control and military reconnaissance. Security for sensor networking is both essential and challenging. The aim of this program is to develop adaptive security services and mechanisms that will protect such distributed multi-domain environments from subversion, malicious code and other attacks. Key issues will include how to manage the balance among quality of service (QoS), bandwidth, power consumption, and multilevel security to enable the network to adapt dynamically to changes in environmental conditions such as security policy, network situational mode and resource availability.

9.1.10 Network Security and Security for Next Generation Networks

Next Generation Network (NGN) promises to revolutionize networking and telecommunication, and provide enhanced services and improved connectivity, through the deployment of ubiquitous IP-based networks. Such digital infrastructures are expected to be constructed using widely-spread heterogeneous components. As many valuable assets are expected to be stored and transmitted electronically over these IP-based NGNs, it is essential to ensure that such networks are designed with proper security and privacy provisions and protocols, in such a way that advanced services can be provided in a secure and private manner. Research in this area aims at exploring communication protocols and behavioral measurement both for IP-based wired and wireless networks and developing the necessary security mechanisms and protocols to protect such networks.

9.1.11 E-trust

Building and maintaining trust between individuals over the internet is a tough task. Even though, most individuals trust whoever has a high score in the third-party website. This kind of trust is dependable and can not be transferable to other parties. There are several models that discuss this subject. However, this subject represents an active research area with many useful applications including, healthcare, auctions, stock markets and so on.

9.1.12 Security Awareness, Education, and Training

The main goal of this research program is to raise security awareness and develop training materials in the field of security and information assurance and to assist and train instructors in conducting courses on relevant topics. This will be achieved by (a) designing and developing course materials for education about information security and related disciplines. The course materials will target undergraduate and graduate students, high and elementary school instructors, university faculty members, as well as system and network administrators; (b) developing web-based and video-based training materials for information security and related disciplines; (c) conducting workshops for training IT managers and practitioners; and (d) collaborating with other national and international centers and universities that share these goals to develop materials and design courses.

9.1.13 Smart Card Research

This program conducts research about Smart Cards' applications and related technologies, particularly in areas related to security including authentication, authorization and proximity detection. In most cases, Smart Cards are plastic cards, about the same size as a credit card, fitted with a chip and, in some cases, with biometric data. Some vendors offer Smart Cards that perform both an authentication function and the function of a proximity card (through RFID technology). Smart Cards are powerful tools for providing strong authentication of users and resources, which allow sites to secure resources while allowing users maximum flexibility in a distributed environment. As the Kingdom has already introduced Smart Card based National IDs, it is essential to establish a research program for exploring integrated biometrics, Smart Card technologies, relevant applications, and active data techniques for authenticating users and systems for secured data access.

9.2 Activities

The current and proposed activities at CoEIS are summarized in Table 1.

Table 1. Ongoing and proposed activities are CoEIS, Riyadh, Saudi Arabia.

Main activity	Sub category and description
Research and Development	Assessing client problems
	Assessing national problems
	Solving client problems
	Solving national problems
	Developing new services
	Developing new product
	Open source development
	Open source training
	Open source support
Consultation	Consultation to industry
	Consultation to government
Academic Education	Special focus program in Information Security in the PhD level
	New Master of Sciences in Information Security
	Teaching Information Security for undergraduate level
	Diploma in Information Security
	Assisting/ Developing Information Security curricula for universities
	Embedding Information Security content in the General Education textbooks
Training	Conversion Courses in Information Security
	Specialized courses in Information Security
	Customized courses
	General Awareness sessions
	Special awareness sessions for top management
Publication	Scientific papers
	Books
	Studies
	Reports
	Newspaper articles
	Magazine articles
	Website
	Newsletter
	Video
Public Events	Organizing/ co-organizing conferences
	Workshops
	Awareness sessions
Public relations	Jobs portal for Information Security
	Peers links
	Social meetings
Partnership	With government
	With industry
	With similar centers
	Visiting other centers
	Having others visiting us
Innovation, talents and incubation	Discovering talents and innovation
	Encouraging talents and innovation
	Supporting talents and innovation through incubators

9.3 Success Indicators

The CoEIS aims to add value in different dimensions and restricted to just pure research, the following are examples of success indicators that show the progress and the success of the center:

- Number of research projects conducted.
- Number of publications.
- Number of public events (Workshops and conferences)
- Number of consultation to local government and private sectors.
- Number of training session and number of trainees.
- Number of companies and government agencies collaboration and partnership with the center.
- Number of awareness methods.

10. Conclusion

The Centers of Excellence play a prominent role in providing platforms for quality research and education in various fields including information technology. The fast growing digital world is now highly vulnerable to constantly changing security threats resulting in serious consequences. Thus, establishing a CoEIS is a need of time to efficiently tackle information security threats and to educate our young generation for sustainable use of IT resources.

In this report, we not only emphasized the importance of information security but also discussed our experiences in establishing a CoEIS at KSU, Riyadh, Saudi Arabia. The strategies described herein together with the features of various international centers included in this report would be helpful to new planners and serve as a guide to establish centers of excellence in information security.

11. Acknowledgment

We would like to thank Dr. Mohammed Alabdulkareem, Dr. Fahd Alotabi, and Dr. Jalal Almuhtadi for their input and comments.

References

[1] Center for Applied Cybersecurity Research, http://cacr.iu.edu/

[2] Center for Secure Information Systems, http://csis.gmu.edu/

[11] T. Frost, J. Birkinshaw, P. Ensign, “Centers of excellence in multinational corporations”, Strategic Management Journal, 23, 11 , 997 – 1018.

[4] Georgia Tech Information Security Center, http://www.gtisc.gatech.edu/

[5] Information Security Institute, http://www.isi.qut.edu.au/

[6] Information Trust Institute, http://www.iti.uiuc.edu/

[7] J. D. Lawrence Pat S. Bodger, Practices of Successful Organisations Applied to Centres of Excellence in New Zealand, in proceedings of the Management of Innovation and Technology, 2006 IEEE International Conference, June 2006.

[8] National Information Assurance Training and Education Center, http://niatec.info

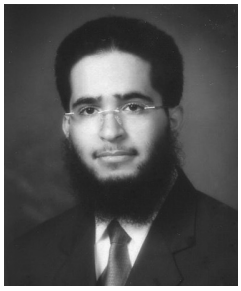
[9] National Information and communication technology plan of Saudi Arabia, www.saudi.gov.sa

[10] National Research Foundation, http://www.nrf.ac.za/

[3] D. Rank, D. Williams, “Partial benefit/cost in the evaluation of the Canadian Networks of Centres of Excellence”, Evaluation and Program Planning, Volume 22, Number 1, Spring 1999 , pp. 121-129(9)

[12] The Center for Education and Research in Information Assurance and Security, http://www.cerias.purdue.edu/

[13] “The Top 10 Reasons that the Best Researchers in the State of Utah want to participate in the Utah Centers of Excellence Program”, http://goed.utah.gov/COE/Top10ReasonstoParticipateintheCentersofExcellenceProgram.html



Khaled Alghathbar,CISSP, CISM, PMP, BS7799 Lead Auditor, is an assistant professor in the Information System Department at King Saud University, Riyadh, Saudi Arabia. He is a security advisor for several government agencies. His main research interest is in information security management and design. He received his M.S. and PhD in Information Technology from George Mason University.