National Center of Excellence for the Advancement of Global IT Security[1]

Habtamu Abie
Norwegian Computing Center
P.O.Box 114 Blindern, N-0314 Oslo, Norway
Habtamu.Abie@nr.no

> "The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable"
> - The art of war, Sun-Tzu

Abstract

The main challenge facing any nation, and indeed the world, presently and in the future, is preparation at the national and international level of methods and measures to deal with a broad range of threats, ranging from natural disasters to electronic intrusions. This will involve making security measures normal, established, standard routine and, the exchange of information on threats, vulnerabilities and best practices. In this paper, we propose the establishment of a National Center of Excellence in IT Security (NCES) whose main aim is to develop, nurture, advance and maintain those practices necessary for the advancement and maintenance of a high level of IT security nation wide in all areas of society with an ultimate goal of advancing international or global IT security.

1 Introduction

During the past few years we have witnessed enormous and rapid changes in our society and developments in its infrastructure, which has become more sophisticated and efficient and, at the same time, correspondingly more susceptible to disruption and vulnerable to threats of various kinds. A laissez-faire attitude in the form of "Let us cross that bridge when we come to it," will inevitably lead to disaster. As Murphy's law states, "if something can possibly go wrong, sooner or later it will, and at the worst possible moment". Potential future problems must be identified in advance, and forestalled. The establishment of a high level of IT (Information Technology) security is an excellent first step, but not by itself an adequate long-term solution. It must also be maintained and updated to keep abreast of current and future developments in the security situation, which must be continuously assessed and reassessed. The ability to spot vulnerabilities must be developed, as must viable strategies to detect, deter and counter threats, thus making our position unassailable. This requires a platform and a framework with all the necessary facilities.

The question is then how this is to be achieved. In this paper we propose establishing a NCES, which is one of the best ways of doing this. The main aim of the NCES will be to develop, nurture, and advance and maintain those practices necessary for the advancement and maintenance of a high level of information security across the Nation in all areas of society, and to make such practices a model for the rest of the world. Hence such national practices are the real stark platforms and framework for

[1] This work has been partly supported by the Research Council of Norway

the practice of security internationally. The aim of this paper is to highlight and point out the need for such a Center, and to urge all actors involved in security, policy-makers and national authorities, academia and the business world to consider the feasibility of establishing this Center by forming a national working group to examine and evaluate the practical sides of carrying out this first step. The paper presents the NCES vision, define some strategic objectives, identify fruitful areas of research, propose a conceptual framework for the maintenance and advancement of IT security, and describe one DRM (Digital Rights Management) scenario as an example.

2 NCES: Background and Vision

Due to changes in environmental factors and advances in technology, the information infrastructure is faced by new threats and is vulnerable in new ways, which makes it difficult to prevent intrusions. As already stated, the main challenge facing any nation, and indeed the world, presently and in the future, is preparation at the national and international level of methods and measures to deal with a broad range of threats, ranging from natural disasters to electronic intrusions. This will involve making security measures normal, established, standard routine and the exchange of information on threats, vulnerabilities and best practices. While security technology and the awareness of the need for security are improving and vendors and providers are becoming better at the implementation of improved protective measures, these measures are still far from foolproof, and there is still an unfortunate dearth of qualified professionals in the area.

The critical infrastructures of, for example, medical services, banking and finance, gas and electricity industries, and telecommunications are making use of the public Internet for communication, not least for the exchange of business, administrative and research information. It must therefore be our aim to make these critical infrastructures totally secure and unassailable.

Consequently, to reiterate, "the ability to spot vulnerabilities must be developed, as must viable strategies to detect, deter, and counter threats, and prepare solid foundations, thus making our position unassailable," and "the main aim of such activities is to develop, nurture, and advance and maintain those practices necessary for the advancement and maintenance of a high level of information security nation wide in all areas of society". This on-going maintenance and updating is a skill which might be regarded as a separate discipline in itself, and is one which we shall have to study, develop, learn and pass on to our successors. As shown in Figure 1, for this skill to be practiced constructively, it must be accompanied by an attitude, an attitude of alertness, enquiry, unblinkered receptivity to new ideas and impulses, etc. It is not enough merely to identify, describe and discuss this attitude. It must be fostered, cultivated and lived as a real experience.

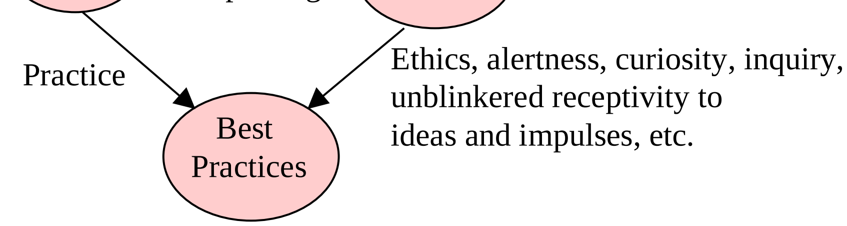

Figure 1 Conceptual Framework for best Skill Practicing

Anyone with skill and expertise can do the job, but to do it well one needs to be committed to it, to be personally involved, to have a genuine emotional attitude to it. One has to be genuinely interested in it, and to like it. One has to enjoy it for its own sake. One has to have a real relationship to it, and a love for it. One has to have a genuine curiosity, one of the most important things. Thus, being technically able to do it, and actually doing it, are not the same things.

Consequently, there is a need to establish and maintain a high level of training, knowledge and expertise both individually and as a group. The development of the individual should be nurtured, and cooperation between individuals within the group should be developed and practiced as a skill and as an attitude, not only in connection with a given project, but also in connection with the development of the individual – colleagues should share knowledge and expertise and help each other develop, rather than indulge in non-productive petty rivalry about who is best, which can, in the worst case, lead to members of the group withholding information from their colleagues for the purpose of increasing their own personal prestige by enhancing the appearance of their own competence relative to their colleagues' ignorance. This kind of attitude retards the development of the individual in general, and can seriously foul up a specific project.

The question is then how all this is to be achieved. As mentioned above one of the best ways of doing this is by establishing a National Center of Excellence in IT Security (NCES) with the necessary platform and framework, and with the ability to

- Develop, nurture, and advance and maintain those practices necessary for the advancement and maintenance of a high level of information security across the Nation in all areas of society.
- Establish and maintain a high level of training, knowledge and expertise both individually and as a group (through research, development, education and leadership development [CAEIA, CIAO]).
- Present the resulting national platform and framework as model for international security practice.

The NCES will thus be the national Center for the training of leaders, the development of vision, and the long-term strategic planning necessary for the development of an adequate national security capability. It will be a place from which to recruit professionals in the area of security who will enter the workforce better equipped to meet the challenges facing the IT community [CAEIA], contribute to the development of a climate which will encourage independent research, will be an advisory body to which other research institutions and industries can turn, and will make recommendations as to what is desirable and useful security management, technology and practice. For the Center to fulfil its primary mission, its activities will be geared to achieving two main broad objectives essential to IT security: (a) spot vulnerabilities, prevent, detect and counter threats, and (b) build strong foundations, as described in the "NCES: Strategic Objectives" section.

Information systems, both governmental, public and private, are increasingly faced by the danger of intrusion and attack, as are other national infrastructures such as finance, air traffic control, energy industries etc., which also depend on reliable and secure information systems. Since information technology and threats to it affect all sectors of society, all sectors should be represented, and should be involved in the establishment of the Center as a national body. State support is necessary to ensure stability and immunity to the vagaries of business bankruptcies, and to ensure a high level of operation and its ability to deliver tangible national benefits.

In summary, the establishment, maintenance and development of information security, an important part of national security as a whole, depends on the systematic, creative and stable co-operation of all sectors, and the best way of ensuring this is the establishment of a National Center of Excellence in IT Security.

3 NCES: Strategic Objectives

It is the purpose of the Center to achieve the following two main broad objectives:

1. To spot vulnerabilities, prevent, detect and counter threats, and
2. To build strong foundations [NSTAC].

3.1 Spot Vulnerabilities, Prevent, Detect, and Counter Threats

This objective can be achieved by the application of two main strategies.

The first consists of identifying critical and vulnerable potential targets of attack, making society aware of the need for improved security by the dissemination of information, and training qualified teachers of security and providing expert advice [NSTAC, ISRC, Congress, CIAO]. In the long term this will result in a robust and impregnable IT system that will withstand attacks and remain effective in the face of them, which will minimize the possibility of attacks succeeding. Attention will have to be paid both to technical defense (e.g., protecting the information infrastructure, cryptography, intrusion prevention systems, etc.), and to the human element (e.g., security policy guidelines, security awareness, ethical decision-making, operation security and production, working with law enforcement, etc.).

The second consists of identifying an attack as and when one occurs, and dealing with it. This will involve identifying the fact of an attack and assessing its nature quickly and in time, containing and blocking the attack, and recovering from and repairing whatever damage may have been caused. A very important factor will be the prompt and timely sharing of information. The specific basis of these activities will be, for example, application controls, systems for the assessment of vulnerabilities, for the detection of intrusions, and for monitoring and control, computer emergency quick response teams, data backup recovery, business continuity planning, dissaster recovery, forensics, insurance relief, etc. It is worthy of mention in this context that a recent survey [Disaster] found that good recovery procedures and backups were the most important security strategy.

This broad objective should be achieved by establishment of a number of specialised sub-centers of excellence (CoEs), as exemplified below.

Risk Analysis, Assessment, and Management Center

The function of this Center will be to develop, deliver and teach important IT system services, with business approaches to preventing and deterring attacks, reducing risks, managing and recovering from crises, developing guidelines for personal responsibilities and liabilities, and developing and implementing standard security policies. It will provide expertise in operations security, technical surveillence as a countermeasure, planning and developing policy, and developing and maintaining the ability to identify threats and vulnerabilities, and will engage in security education generally. The desired result will be the development of cost-effective risk managemnt based security measures that can then be incorporated into the national security policies and procedures [ISRC].

Information Resource and Advisory Center for Security

This Center will provide authentic and authoritative information and advice, and technical support in the areas of information security, assess policy and technology, and develop an array of security techniques and tools. It will render industry assistance in the definition of requirements, in the design and implementation of an overall solution, and the assessment of security technologies already deployed. In order to do this it will have to identify and understand the security requirements of business, and then codify them in the form of a set of precisely specified standard requirements. It will also develop and provide guidelines for the

- Taxonomy of security events, incidents and threats.
- Development of a common standard format and procedure for security incidents which will include instructions as to what data to collect, and when and how, and information as to why the data is necessary for reliable and appropriate responses to a security incident.

Security Professionals Certification Center

No matter how high the quality of the security technology deployed to protect information assets, the security of these assets will always ultimately be dependent upon the expertise of the security professional in charge [ISC2]. To ensure the quality of these professionals, it is necessary to be able to trust the authenticity and reliability of their credentials. It will be the task of this center to certify IT security professionals reliably and in accordance with well-founded, standardised criteria.

3.2 Build Strong Foundations

As described in [Congress, NSTAC] the first step towards the achievement of this objective will be to identify the things that must be done nationally to establish a solid foundation for the achievement of the first broad objective. These things will be in connection with IT interdependencies, the needs of R&D, and information sharing, and will together constitute a solid fundament, and will consist of

a) Enhancing and intensifying the work done by R&D in the areas of the protection of critical information infrastructure, both through its own research, and through the exchange of information between it and other entities, by, among other things, developing a nation-wide, standard IT policy that will emphasize the need for R&D to give attention to security, and for test-beds, laboratories, and standard test procedures.

b) Training and employing a sufficient number of information security specialists, a) by supporting already existing teaching CoEs and by the establishment of new ones under the auspices of academia, b) by providing financial incentives that will encourage students to enter the field of IT security and c) by ensuring that research encompasses other necessary areas like risk management in all its aspects, operations, legal and public policy, and human factors.

c) Passing legislation which will facilitate the protection of critical information infrastructure in our new and still changing environment.

There are already CoEs in education and training at [CAEIA, Hart02, HIG, NRCCL] in various fields at different academic levels.

4 NCES: Potential Areas of Security Research Endeavors, Conceptual Framework, and DRM Scenario

4.1 Potential Areas of Security Research Endeavors

Information Assurance is based on operations whose function is to protect information and information systems. This protection is based on ensuring availability, accountability, confidentiality, and integrity. “This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities“ [CAEIA]. The Church-Turing thesis proves that “any suitably powerful computer can exactly recreate the results of any other one,” which implies that Information Assurance is constantly challenged. This means that research in all areas of information security must be a continuously on-going process, and will necessarily involve:

- identifying a suit of necessary security services (both at the application level and infrastructure level) such as cryptography, key distribution, public key infrastructure (PKI), protocols, algorithms, confidentiality, integrity, availability, accountability, policy, privacy, trust, risk management, forensics, intrusion detection and prevention systems, biometrics, communications security and protection of intellectual property rights (IPR);
- identifying architectures and frameworks for combining security mechanisms and services in effective and reliable ways;
- ensuring that the security mechanisms implemented (e.g., those for interoperable encoding of security attributes) interact effectively and developing techniques to manage the combination of interacting mechanisms, and methods and tools to assess and guarantee the combinations’ security;
- demonstrating how already existing applications and new ones can be protected using high level and generic security service APIs, and how sound security for the protection of the IT infrastructure can be developed and maintained;
- improving techniques and methods for the analysis, assessment, and management of risk by developing a common framework and architecture supporting applications which deal with all five risk cycles [ISTWP] (risk assessment and planning, mitigation, preparedness [Steen], response and recovery), and introducing a software engineering process in which risk analysis and security policy awareness are exercised at each stage (specification, analysis, design and implementation);
- developing a legal framework for the protection of IT systems and infrastructure; it should be emphasized that new legislation to deal with new situations consists not only of passing new laws, but also of repealing obsolete laws which are now actually in the way (one example of obsolete and now counter productive legislation being the regulations that impede and prevent the voluntary sharing of information so essential to the protection of IT infrastructure).

It is common and well-founded practice to apply formal methods, techniques and tools to increase the reliability of, and level of confidence in, the specification, analysis, design, verification, implementation and secure operation of the system. It goes without saying that in the above areas formal methods, techniques, and tools must be applied at all levels. For example, through their application the practice of the identification of risks, threats and vulnerabilities, and the application of the appropriate controls to manage risks, can be formalized and (semi)-automated, which will improve overall risk management.

4.2 Conceptual Framework for Developing and Maintaining IT Security

Another challenge facing the IT community is the building of an overall, flexible (semi)-automated and formalised framework for the development and maintenance of IT security which will allow us to investigate proactively and adapt to new factors as they emerge due to changes in the environment brought about by new policies, new laws, new technologies and, not least, new threats. The framework must be capable of dealing with these factors in whatever combination they present themselves at any given moment, using formal specification and verification methods and computerised tools, and must provide understandability, precision, flexibility, ease of automation, and ease of verification. Figure 2 shows such an integrated conceptual framework for the development and maintenance of IT security.

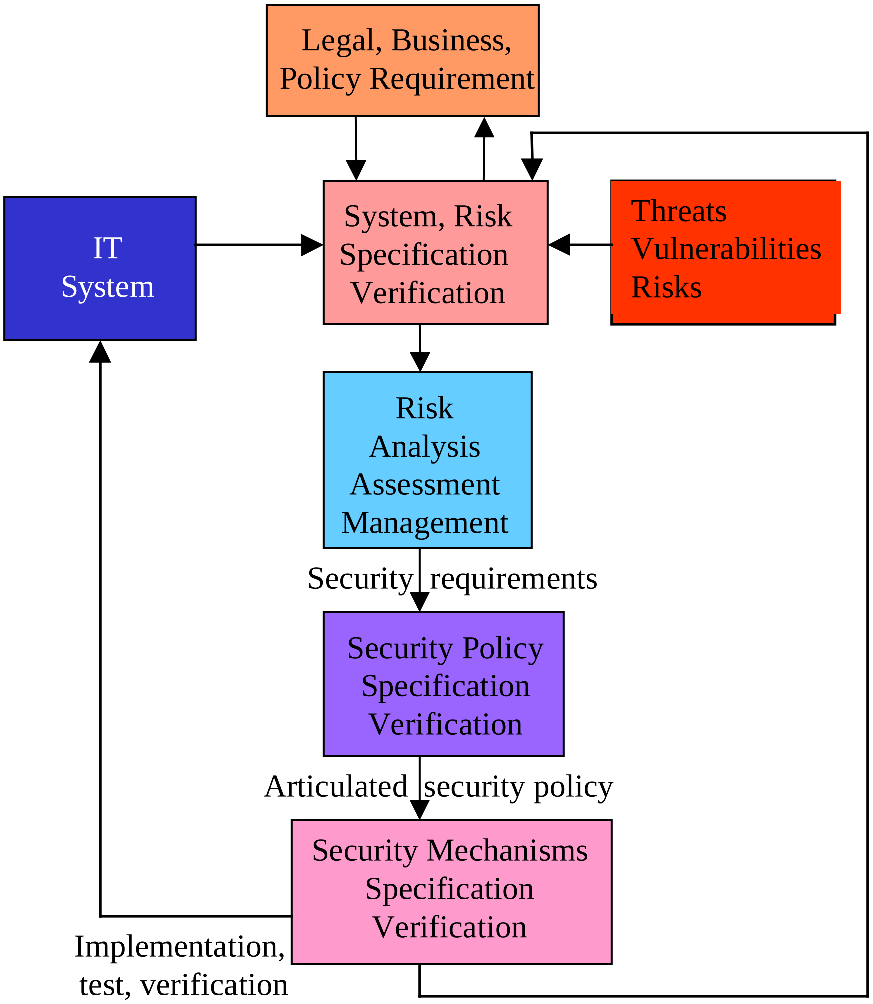
Legal, Business, Policy Requirement
IT System
System, Risk Specification Verification
Threats Vulnerabilities Risks
Risk Analysis Assessment Management
Security requirements
Security Policy Specification Verification
Articulated security policy
Security Mechanisms Specification Verification
Implementation, test, verification

Figure 4-1 Conceptual Framework for Developing and Maintaining IT Security

Such an integrated framework must allow the accurate specification and verification of the IT system, and the vulnerabilities, threats and risks to which it is exposed taking into consideration the legal, business, and policy requirements, thus allowing a precise and unambiguous identification of potentially vulnerable elements in the system, evaluation of which problems may emerge due to these elements, and analysis of the potential consequences these problems may cause, thereby aiding the early discovery of vulnerabilities, inconsistencies and redundancies in security. It must also establish methods to check the consistency of the results of risk analysis, and to present and communicate comprehensibly both these results and security requirements, thus making possible the qualitative modeling, management and documentation of risks [ASNZS, CORAS] in a precise, unambiguous and efficient manner. The result of such activities will lead to the accurate specification and verification of the security requirements which form the basis of establishing security policy.

The specification and verification of security policies must allow security policies to be formulated both comprehensibly and unambiguously in the IT environments, based on the security requirements that are arrived at through a comprehensive analysis of the security needs of the IT system, and must allow security policies to be checked for consistency and correctness. The specification and verification of security mechanisms must also allow precise and unambigous modeling of the individual mechansims based on the articulated policy, and must allow the implementation, testing and verification of all the security mechanisms for the IT system. Additionally, the operations of the overall framework must be maintained and managed, and the consistency of the relationship (communications and feedback) between the different components must be managed as an integral part.

In sum, the overall framework may be composed and assembled from independent formal methods, languages, modeling techniques and tools, risk analysis and evaluation techniques and methodologies and sub-components, and how these sub-components and tools communicate and co-operate (protocols and infrastructure) may be formalized and (semi)-automated to achieve dynamically changing IT security objectives. We believe that this framework will contribute to the objective of the EU FET (Future & Emerging Technologies) work program on “Improved Risk Management” whose main aim is “to develop open platforms, integrated systems and components for improved risk management, improved civil security applications and environmental management” [ISTWP].

4.3 NCES: DRM Scenario

In today's fast changing digital environment, the development of DRM in order to protect IPR is emerging as a formidable new challenge both in the legal, technical, and commercial arenas. The process of DRM includes a number of different business models ranging from the secure sharing, with employees, partners and clients, of content for business collaboration to conducting electronic commerce where trust is absolutely essential. DRM will necessary involve the investigation of methods, techniques, procedures and algorithms for the management of digital rights which will allow the flexible specification of rights, rights policies, conditions and terms of usage, and online negotatiation and contracting of rights and rights policies. Trust is a central issue in all this. We argued in [abie2] that the security infrastructure plays a pivotal role in the preparation, distribution, storage, manipulation, and communication of information contents across organizational boundaries, thereby establishing the necessary trust in DRM applications. Therefore, different trust models must be investigated and integrated into the DRM model. To build reliable DRM security solutions, legal and public policies and human factors must be investigated and the results integrated into the DRM systems.

Consumers are still worried about their privacy, and this unfortunately well-founded concern inhibits the growth of e-commerce. Any DRM system must thus ensure the protection of consumer privacy, and enable consumers to control how personally identifying information is obtained and used. Digital Policy Management (DPM) is becoming a discipline in its own right, whose concern is the design, analysis, implementation, deployment and use of efficient and secure technology that handles digital information “in accordance with the relevant rules and policies” [DRM02]. Different trust and privacy policies must be developed and integrated into the DPM-enabled DRM system. Improvement in the implementation of policy depends on an improved risk analysis, assessment and management process. Thus, DRM systems must be extended with a specialized and improved risk management module containing a risk management process and methodologies for the analysis and assessment of risk.

It is evident from the above that there is a need for an integrated framework for privacy, policy, security, trust and risk management for DRM in which the synergy effect must be investigated, evaluated, formalized and exploited if any IPR business is to flourish. It would therefore be desirable to establish a NCES that will consist of teams of experts on technology and development, business, law, societal questions, policy-making, security, etc., who will organize on-going and future research on those areas of their respective disciplines that apply to DRM at national level. We argued in [abie] that the development of DRM is an increasingly important global issue, where global communications transcend national boundaries, and where digital products are sold on an international market, since the different national laws, policies and practices must interoperate and be reconciled. We also argued that this issue would be best addressed by the international Network of Excellence. Without contradicting ourselves we can argue here that the enhancement of scientific and technological excellence of a national community will form the real stark platforms and framework for the enhancement of the scientific and technological excellence of the international community.

5 Conclusions

In this paper, we have outlined the form and strategic objectives of the National Center of Excellence in IT Security, and demonstrated the need for the development and maintenance of a high level of IT security. We have proposed a conceptual framework for the achievement of this, and identified fruitful areas of research.

The establishment of a NCES will be a much needed shot in the arm for national IT security. All sectors of society must be represented in the NCES and involved in its establishment as a national body, since IT and threats to it affect them all. Since the stability of the Center and its immunity to the vagaries of business bankruptcies are of prime importance, as are ensuring a high level of operation and its ability to deliver tangible national benefits, the support and participation of the state are absolutely essential.

The practices of the NCES will form the real stark platforms and framework for the practice of IT security internationally (global dependability of IT).

References

[Abie] Habtamu Abie, A Synergy Framework for Trust, Privacy, Policy and Risk Management for Digital Rights Management, Extended Abstract, Norwegian Computing Center, to be submitted shortly, 2002

[Abie2] Habtamu Abie, A Rights Management Model for Distributed Object-Oriented Information Distribution Systems, Proceedings of the IFIP WG6.7 Workshop and EUNICE Summer School on Adaptable Networks and Teleservices, September 2-4, pp. 185-194, 2002

[ACISP] ACISP 2003, The Eighth Australasian Conference on Information Security and Privacy http://www.itacs.uow.edu.au/research/NSLabs/acisp03/index.html

[ASNZS] AS/NZS 4360:1999, Risk Management, Australian Standard, 12 April 1999-09-17

[CAEIA] Centers Of Academic Excellence in Information Assurance Education http://www.nsa.gov/isso/programs/coeiae/index.htm http://www.nsa.gov/isso/programs/nietp/newspg1.htm

[CIAO] Critical Infrastructure Assurance Office, http://www.ciao.gov/

[CIPL] Center for Information Policy Leadership, USA, http://www.hunton.com/info_policy/abrams.htm

[Congress] Joint Economic Committee United States Congress, Security in the Information Age: New challenges, Strategies, May 2002 http://www.house.gov/jec/security.pdf

[CORAS] A Platform for Risk Analysis of Security Critical Systems, http://www.nr.no/coras/

[CRIS] The International Institute for Critical Infrastructures http://www.cris-inst.com/

[Disaster] The State of IT security: Disaster Recovery: a survey http://www.searchSecurity.com/originalContent/0,289142,sid14_gci847318,00.html

[DRM02] DRM2002, ACM Workshop on Digital Rights Management, http://crypto.stanford.edu/DRM2002/

[ECSIRT] The European Computer Security Incident Response Team Network, http://www.ecsirt.net/

[Hart02] Hart Votes to Strengthen Cyber Security, Combat Identity Theft, http://www.house.gov/apps/list/press/pa04_hart/20702_cybersecurity.html

[HIG] Gjøvik University College, http://www.hig.no/nyheterinfo/english.html

[ISC2] International Information System Security Certification Consortium, Inc., http://www.isc2.org/

[ISRC] Information Security Resource Center, http://www.pnl.gov/isrc/

[ISTWP] IST – Information Society Technologies, A thematic Priority, Workprogramme 2003-2004, Draft version of 16-09-2002.

[NRCCL] NRCCL - Norwegian Research Center for Computers and Law http://www.jus.uio.no/iri/english/

[NSTAC] The NSTAC's Response to the National Plan, April 2001, http://www.ncs.gov/nstac/NationalPlanReport-Final.htm

[NW3C] National White Collar Center: http://www.iir.com/nwccc.htm http://www.training.nw3c.org/:

[OECD] OECD Guidelines for the Security of Information System and Networks, Organization for Economic Cooperation and Development, July 25, 2002, http://www.oecd.org/pdf/M00033000/M00033182.pdf

[RFC2350] IETF RFC2350, Expectations for Computer Security Incident Response, http://www.ietf.org/rfc/rfc2350.txt

[SIS] Center for Information Security, http://www.norsis.no/index_english.html

[Steen] Roger Steen, A Guide to Information Preparedness, The Directorate for Civil Defense and Emergency Planning (DCDEP), ISBN: 82-993462-3-1), 2000, www.dsb.no