GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

The Regulatory Environment In Information Security

By Husin Jazri

(As part of the requirement of GSEC Examination)

Regulations in information security cover many areas including data protection, data privacy, computer misuse, official controls on cryptography, software copyright, security evaluation and criteria, certification, standards and guidelines. Fundamental reasons for these regulations are protections of the rights of all parties in line with public policies, national security and sectoral benefits. Public policies include rules of monopoly, health and safety, consumer protection, minority protection, personal privacy, environment protection, intellectual property protection, public order, harmonization as well as prevention of corruption. National security on the other hand deals with secrecy, money-laundering, anti-drugs, anti-terrorists, communication protection and national independence and sovereignty. Sectoral benefits provide self-regulation, professional associations and standards that include cross-sectoral interactions. Regulations in information security always evolve on balancing between the individual and organization protection.

Data Protection

The objectives of data protections are to protect personal privacy and enable international free flow of personal data by harmonization. Different countries would have their own version of the Act - notably the American and European continents leading the arena. Here, the attempt is to generalize the main features of the act that are not disputed by many.

The main purpose of the Act is to preserve privacy and enable the enforcement of information processing standards. Two main players involved are the data users and the data protection registrar. Data users are responsible for the personal data. These personal data must be :

1. Obtained fairly and lawfully.
2. Used only for registered purposes.
3. Disclosed only to registered disclosees.
4. Adequate, relevant and not excessive.
5. Accurate, and where necessary, up-to-date.
6. Kept for no longer than necessary.
7. Accessible to the data subject.
8. Kept appropriately and securely.

On the other hand, the powers of the registrar are :

1. Refusal of registration.
2. Enforcement notice to comply with principles.
3. Transfer prohibition notice.
4. De-registration notice.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5. Prosecution.

The registration process includes identification of all computerized personal data and details about the data usage such as to whom disclosures are planned. Registration can be rejected if information furnished to the registrar is incomplete, false or misleading. Exemptions from the provision of the act are granted for national security, individuals, clubs and preparations of the text document. Partial exemption is allowed for crime tracking, statistics, research studies, examination marks and backup data. These partial exemptions should be allowed in a controlled manner and usually with the authority of the jurisdictional entities.

The Computer Misuse Act

The growth of computer hacking, trojan horses, emergence of virus threat, and the growing dependencies of computer usage has forced the birth of Computer Misuse Act. The activation of this Act varies from country to country - with many more countries, among the poor and the developing nations, not adopting yet.. Among others, the act covers the followings :

1. Unauthorized access to computer program or data.
2. Unauthorized access with intent to commit further offence.
3. Unauthorized modification of the contents of any computer, with intent to impair operation or hinder or impair reliability.

4. Definition of Unauthorized :

    a. Objective test :
        - Not entitled to control access of the kind in question or modification.

    b. Subjective Test :
        - Must know he is unauthorized.

5. Definition of access includes display, use, copy, move, alter and erase.

6. Definition of intent need not be specific as to computer, program, modification, etc.

In summary, the Act covers attempts, incitement, conspiracy and cross-border offences. It also provides for search warrant signed by the Circuit Judge. Experience on the effect of this Act to date indicates that they are still low understanding of the Act at large but improving at an acceptable rate. The Act gives deterrent effect and reduce hacking levels. It induces better moral and ethical climate. Few prosecutions were found initially but on the increase due to greater understanding of the act. Nevertheless, the act still has its shortcoming in controlling the propagation of computer viruses and denial of service attack.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In some countries, the Act also covers official controls on cryptography. It includes export controls where licenses are needed. The rationale of the control is always national security. The objective of the control at first was to restrict algorithms but it was not quite successful and now the trend is going towards enabling access to keys (under warrant) known as key escrow.

Software copyright on the other hand, is covered under the Software Copyright Act. Business Software Alliance (BSA) and Federation Against Software Theft (FAST) are two examples of the responsible parties to prosecute those involved in software piracy. Usually big names are preferred to be made as target due to wide publicity gathered.

SECURITY EVALUATION CRITERIA

Security evaluation criteria started with the introduction of TCSEC known as 'the Orange Book' targeted at evaluating military security. It has been later expanded to include government security due to the need for the commercial-off-the-shelf (COTS) security products. These criteria stands as an independent, third-party entrusted source that inspects, verifies, and accredits security standards essential for customer needs.

The US 'Orange Book'

In 1983, the Orange Book which is also known as TCSEC was published and the National Computer Security Center evaluations began. This book provides guidelines on the formulation of security policy, accountability, assurance in the operating system design such as reference monitor, trusted kernel, trusted computing based and documentation. Security policy covers areas like mandatory access control, discretionary access control, Bell/LaPadula model and labeling. The levels ranged from low to high, from D (minimal security), C (discretionary protection), B (mandatory protection), and A (verified design). Within some of these levels are sublevels. There are C1 and C2, for example : discretionary protection and controlled access protection with the latter being more secure. B with its sublevels, and A levels were thought to be more suited to military systems.

The main criticism on TCSEC are that the DoD Security Policy is assumed throughout. This may not be suitable to the 'non military' organization. It emphasizes stringently on confidentiality, has no commercial involvement and mainframe oriented. Also, the Orange Book only applied to stand-alone systems, and ignored the connectivity requirements. Whatever the criticisms are, it is obvious that the Orange Book has become an important reference for security evaluation and formulation of the later standards.

The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

This security evaluation criteria originated from Canada and is an attempt to update the 'Orange Book'. It adds some coverage on integrity and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

availability which are missing in the Orange Book. It has a more flexible function but is still structured. Basically it carries the same language and style of the Orange Book.

The Information Technology Security Evaluation Criteria (ITSEC)

This security evaluation standard is the initiation of four nations - UK, Denmark, France and the Netherlands. It has eight recommended headings that is access control, accountability, audit, object re-use, accuracy, reliability of service, identification and authentication and data exchange. It also covers assurance of correctness which includes the development process, development environment, operational documentation and the operational environment. It has security levels from E1 which is the strongest to E6 (the weakest) and E0 – fail. It also includes assurance of effectiveness which address the issue of suitability to counter threats, binding strength of mechanisms and effect of known vulnerabilities.

The US Federal Criteria

The Criteria is a joint project between NIST and NSA to replace the 'Orange Book'. It leads to a new Federal Information Processing Standard. This criteria can be used as a standard for design and development of trusted products and systems. It also has protection profile which covers development, analysis and registration.

The Common Criteria

This criteria is formulated based on the input from the TCSEC, CTCPEC and ITSEC. It was formed as a mutual agreement arising from the close coordination and experience of existing security evaluating bodies, with focus of resolving existing conceptual and technical differences. In 1998, the Common Criteria established a Mutual Recognition Agreement, which means that different countries agree to recognize each other certifications. So far Australia, Canada, France, Germany, New Zealand, Finland, Greece, Spain, Italy, Norway, United Kingdom, and the United States have signed on. The draft version 0.9 was first issued the end of 1994 and subsequent drafts were released after that. The Common Criteria incorporates functional requirements defining desired security performance of an IT product and assurance requirements that confirm security measures are effective and correctly implemented. While establishing security requirements, the Common Criteria's Protection Profiles (PP) define a standardized set of security objectives where individual products can be tested against that protection profile. A Target of Evaluation (TOE) is a specific IT product or systems that is subjected to the evaluation. A Common Criteria Security Target (ST) contains the IT security objectives and requirements as pertaining to a specific TOE with the definition of functional and assurance measures of the TOE. The Common Criteria evaluates and certifies databases, firewalls, networks, operating systems, smart cards, access control, and other Internet security products.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

PROFESSIONAL ACCREDITATION

There are initiatives by some quarters to ensure quality of professionals in the field of information security is established and possibly enhanced. Some of the accreditation initiatives are from the International Information Systems Security Certification Consortium, Inc (ISC2) and System Administration and Network Security (SANS), both are initiated from the U.S. Example of accreditation programs are CISSP from ISC2, GSEC and GIAC from SANS. CISSP is focusing on the 'big picture' sweeping through multiple disciplines in science of information security, suitable for technical managers while GSEC and GIAC is approaching from a slightly different dimension where skill competencies are also being emphasized. For an organization's security to be complete, both kinds of skills are important. Different job responsibilities have different skill requirements and both are needed to build the competent team.

CONCLUSION

It can be concluded that the importance of regulatory security environment is growing and has room for further improvements before the standardization of secured and harmonized information environment can be agreed upon by the entire world community. Protection of information through laws such as computer misuse and illegal software copyright acts is only part of the overall tasks that needs to be performed. Whatever that may come in the near future, the regulatory of information should be made to nurture the free flow of valuable information, transcends the geographical and political boundaries and provide benefits to mankind without any prejudices and limitations to some and advantage to the other.

References:

1. http://www.mycert.org.my/crime.html
2. http://www.commoncriteria.org/cc/cc.html
3. http://www.itsec.gov.uk/docs/formal.htm
4. http://www.dynamoo.com/orange/index.htm
5. Secrets and Lies, Digital Security in a Networked World, Bruce Schneier, Wiley Computer Publishing; 2000. (ISBN 0 -471-25311-1)
6. Internet Security Advisor Magazine, November/December 2000.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.