The 7th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 15th 2012

SENSITIVE INFORMATIONS MANAGEMENT

Florian STANCU Lieutenant-colonel

General Staff

Abstract:
Since the oldies times it has been known, information means the power. From that we can find out that it is most important to keep sensitive information inside the organization and, on the other hand trying to reach more information from the opposite organizations. This is an informal rule that can involve a very formal issue, information security and sensitive information management. The purpose of this paper is to show to the reader some principles, policies and rules of information security in order to reach a good management of sensitive information. Loss, misuse, modification or unauthorized access to sensitive information can negatively affect the privacy or welfare of an individual, trade secrets of a business or even the security, internal and foreign affairs of a nation depending on the level of sensitivity and nature of the information.

Key words: sensitive information, classifying information, management, policy, responsibilities, protection, risks, threats, vulnerabilities.

1. Introduction

Confidential information which contain high value, and if compromised could result in serious consequences, is considered to be sensitive information. Unauthorized disclosure, alteration, loss, or destruction of sensitive information will cause perceivable damage. Examples include governmental information, information contained in client, case or patient files, information pertaining to security of critical infrastructures, information enabling law enforcement and emergency services.

The security category of a document, file, records series, or system is determined by the most sensitive information it contains. The significance of classifying information due to its sensitivity defines appropriate security controls and reduces the risk of unauthorized disclosure, use, loss or destruction of information.

Examples of classifying information from different countries or organizations:

ROMANIA	NATO	EU
Nesecret	Unclassified	Unclassified
Secret de Serviciu	Restricted	Restricted/Restreint
Secret	Confidential	Confidential/Confidentiel
Strict Secret	Secret	Secret/Secret
Strict Secret de Importanta Deosebita	Cosmic Top Secret	Top secret/ Tres Secret

SENSITIVE INFORMATIONS MANAGEMENT

All personnel who handle or manage sensitive information have to understand their responsibilities and obligations in order to keep sensitive information in original shape inside the organization according whit security policy and law.

2. Areas of Concern

The primary area of concern is that sensitive information may not be adequately protected against security and privacy risks.

There are many factors which can amplify these concerns:

- Personnel may not identify sensitive information holdings and resources;
- Sensitive information may not be handled according to the information classification process resulting in unauthorized disclosure, loss or destruction of information;
- Physical materials (blank forms, tokens, certificates, security badges, etc.) which are used for sensitive information may not be controlled or stored in secure facilities;
- Weak processes for managing sensitive information (removable media devices, paper records, incomplete shredding, documents left unsecured) could result in security breaches;
- Personnel are not adequately trained in special handling requirements;
- Requirements for personnel to complete special confidentiality agreements may not be followed or enforced;
- Strong encryption technology may not be used resulting in information being inadequately protected while in storage or during transmission;
- Logical security controls may not be in place to ensure the protection of sensitive information (network segregation, dedicated servers);
- Contracts with third parties may not specify special security requirements for sensitive information;
- In the absence of regular security reviews or audits it will be difficult to determine if the controls intended to protect sensitive information are effective and functioning properly;
- Poor physical security controls during transportation, storage or destruction of media and records may create security exposures.

3. Intended Outcomes

The policies associated with sensitive information are intended to ensure that sensitive information is identified and protected adequate with its value and sensitivity, to encourage the development and implementation of controls for a good management of sensitive information. Also, most important things are to ensure that personnel are responsive of their responsibilities for protecting sensitive information in order to reduce the probability of inappropriate disclosure, alteration or destruction of sensitive information.

3.1. Responsibilities of all personnel

3.1.1. Things to do:

- Identify information that should be defined as sensitive information;

- Implement approved encryption schemes for sensitive information;
- Keep sensitive information within specially designated physical security zones;
- Be aware of and understand security policy and practices for sensitive information.

3.1.2. Things to avoid:

- Including sensitive information in e-mail, faxes and other forms of electronic messaging;
- Unauthorized storage or transportation of sensitive information away from secure facilities;
- Using sensitive information for testing or training purposes.

3.1.3. Things to pay attention to:

- Special security and privacy controls designed to protect sensitive information.

3.2. Responsibilities of Management

3.2.1. Things to do:

- Ensure that sensitive information is defined and protected;
- ensure that security policy will be, implemented appropriate to the value and sensitivity of the information;
- Ensure personnel responsible for managing, accessing and using sensitive information receive suitable training and regular reminders of special security requirements;
- When a security or privacy breach has occurred, review and revise related policies and processes as needed.

3.2.2. Things to pay attention to:

- Special handling requirements for Cabinet documents;
- Reports from audits or security reviews which identify risks to sensitive information;
- Recommendations from personnel for securing and handling sensitive information.

3.2.3. Things to establish procedures for:

- Conducting periodic reviews or audits to assess the security of sensitive information;
- Reviewing system reports to identify inappropriate access or usage;
- A pre-release approval process for presentations, or articles which may contain sensitive information.

3.2.4 Things to monitor:

- Initiatives to remediate security or privacy concern identified in assessments, audits and reviews.

4. Organizing Information Security

The protection of information assets requires a multi-disciplinary approach that is supported by the information security organization. A management structure needed to coordinate information security activities including required information security activities,

who coordinates them and what agreements are required. This coordination applies to internal organizations and to external parties accessing or managing the organization's information assets.

The information security organization requires the support of a network of contacts in the information security community to bring out advice, trends and to deal with other external factors.

4.1. Management support

It is strongly recommended to establish a security infrastructure necessary to protect sensitive information assets by establishing an information security architecture for standard security controls and defining organizational roles and responsibilities for information security. This concern requires elaboration of the Information Security Policies, developing and reviewing them when is necessary, monitoring and measuring the implementation of them and developing and delivering a program to maintain information security awareness.

4.2. Specialist support

Information security specialists are responsible for:

- Interpreting the Information Security Policies;
- Evaluating information security implications of new organizational initiatives;
- Performing information system security risk analysis activities;
- Performing information security assessments and reviews;
- Evaluating new threats and vulnerabilities;
- Investigating major information security incidents;
- Advising on the information security requirements for documented agreements;
- Analyzing and providing advice on emerging information security standards;
- Providing information security advice for business areas.

4.3. Confidentiality agreements

Information Owners must ensure employees are informed of their obligation to maintain the confidentiality of information and, ensure individuals other than employees accept and sign an agreement to maintain the confidentiality of information.

Confidentiality requirements must be reviewed and updated periodically.

5. Physical and Environmental Security

This chapter identifies requirements for the protection from environmental and man-made threats to personnel and property in information processing facilities. One of the principles used for protection is the use of security zones to place computers, people and information in secure areas. Safety measures for equipment installations are also required.

Requirements for the installation, operation, protection and maintenance of computer equipment are identified to preserve the confidentiality, integrity and availability of government information and information systems.

5.1. Security perimeter

Information owners must establish the appropriate type and number of restricted zones to achieve the necessary conditions for personnel safety, and for the protection of, sensitive or valuable information and assets.

Appropriate security controls must be applied to reduce the level of identified risks and include a structure that prevents external visual and audio observations and complies with all local building codes for structural stability (external walls, internal walls, ceilings and doors). Walls surrounding the facility must be extended from true floor to true ceiling, to prevent unauthorized entry and minimize environmental contaminations such as that caused by fires and floods. Appropriate control mechanisms (e.g., locks, alarms and bars on windows and doors) must be applied to prevent unauthorized access;

All information processing facilities must be equipped with physical intrusion alarm systems that automatically alert monitoring staff to take immediate action. Alarm systems must be continuously monitored;

Access to restricted zones must be controlled, authorized and monitored as required by the applicable zone.

5.2. Secure area requirements for personnel

Information owners must identify and document requirements that apply to personnel authorized to work in secure areas. They are responsible for informing personnel working within a secure area that activities within a secure area are confidential and must not be discussed in a non-secure area, or with persons who do not have a need-to-know and no type of photographic devices, video, audio or other recording equipment is to be brought into unless authorized.

5.3. Other secure area requirements

Information owners must identify and document requirements for other individuals who may need access to a secure area. They are responsible for ensuring that maintenance staff, cleaners and others who may require access on an ongoing basis to the secure area must be screened and their names placed on access lists. Visitors must obtain approval for visits and personnel must escort visitors when they are within the secure area.

Unoccupied secure areas must be physically locked and periodically checked. Physical intrusion alarms must be installed to automatically alert monitoring staff of a breach.

6. Need-To-Know Principle

Need-To-Know is one of the most fundamental security principles.

Knowledge, possession of, or access to sensitive information shall not be afforded to any individual exclusively by virtue of the individual’s office, position, or security clearance.

The responsibility to determine “need-to-know” is the responsibility of the individual who possesses the sensitive information.

On reason to be constantly aware of “need-to-know” is that some trusted insiders have gone badly. When this happens, careful observation of “need-to-know” helps to limit the damage. When someone looks for information that they don’t need-to-know, it may just be simple curiosity, but that is not the only possibility.

Need to know can be really hard. It goes against our natural instincts and everything we have been taught about getting along in groups. Breakdowns in applying the

need-to-know principle don't usually stem from deliberate misbehavior. Instead, they arise from people trying to be helpful and cooperative, things we are educated to do from early childhood.

Need-to-know sounds so simple. The need-to-know principle says that having the clearance for information is only half of the issue. The other half is having the need-to-know.

Individuals with authorized access to classified information are required to limit access to that information only to individuals whose clearance and need-to-know has been verified.

The need-to-know principle dictates that an authorized holder of information, only share the information when two conditions are met.

These are:

- the requester has the appropriate clearance and access.
- the requester needs to know the information in order to perform his or her job functions.

When both conditions are met, the information can be provided.

References:

[1] Government Decision No. 353/2002 - Norms on the Protection of NATO Classified Information in Romania;
[2] Government Decision No. 585/2002 - The National Standards on the Protection of Classified Information in Romania;
[3] Law No. 182/2002 On Protection of Classified Information;
[4] Government Decision No.781/2002 On the Protection of Restricted Information;
[5] Marius PETRESCU, Prof. dr.– Director General of ORNISS, interview in "Gândirea militara românească" magazine, 21.10.2003.