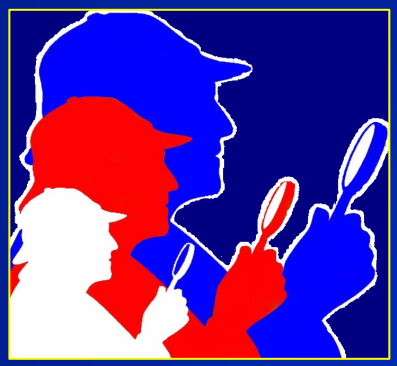
ENISA Workshop On Risk Management

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator



George Constantinopoulos

Management Consultant

OTE S.A.

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

- A national telecommunications operator is usually a public organization where
  - No clear strategy exists
  - Profit is not always the first priority
  - Organization image is not the best possible
  - Human resources management bears a lot of constraints
    - Overstaffing and understaffing
    - No adequate training and awareness
    - No motivation (bonus, promotion, age)
    - Unions
  - Accountability is not always feasible
  - Resources allocation is not possible if not budgeted
  - Technological infrastructure is not always as recent as necessary

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

- In many countries the national telecommunications operator is also an operator who owns and is responsible for the operation of the nation's core telecommunications infrastructure.

  This infrastructure is also partially or as a whole used (under certain terms and conditions) by a number of other operators called Other Line Operators.

  The co - location and common use of the infrastructure introduce a significant security issue related to the responsibility for the security of this infrastructure.

  One of the most significant security principles is that security Responsibility and Accountability should belong to the same role

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

- **Information Security Risk Management is a business process that :**
  - **Should be linked and aligned to the Corporate Mission and Strategy**
  - **Should be a never ending recurring process, based on the participation and awareness of the whole enterprise**
  - **Should be supported and backed up by a concise and clear legal and regulatory framework specifying the operational environment of the company or organization**
  - **Should fully incorporate and implement all of its fundamental sub – processes i.e :**
    - **Assessment**
    - **Evaluation**
    - **Treatment**
    - **Audit**
  - **Should be open and cover the whole extent of the enterprise without accepting exceptions, “restricted areas” and pre-decided compromises**

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

But ...

The fundamental prerequisite and the cornerstone for the development and implementation of any Risk Management Process

is

Understanding the background and the operational environment of the organization and its risks

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

- The scope of security management in telecommunications is much wider than in other sectors as it is also responsible for :
  - Ensuring privacy of communications (interception) which is carried out through various means and platforms, like
    - Fixed and mobile telephony
    - Internet
    - Satellite communications
  - Maintaining enormous quantities of information related to communications (call detail records, internet traffic etc) not only for business reasons (billing) but also to provide Police and Justice authorities with one of the most useful and regularly used mean of investigation and crime detection and prevention.

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

- **Besides the above requirements, a National telecommunications Operator is usually on of the most significant parts of the nation's Critical Infrastructure.**

  This fact simply means that the Operator should be held exclusively accountable for :

  - **Uninterrupted Service availability under all circumstances (and especially under adverse conditions)**
  - **Protection and ensuring of confidentiality of information of the highest classification level (military information, diplomacy etc)**

- **As it is already pointed out :**

  One of the most significant security principles is that security Responsibility and Accountability should belong to the same role

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

- In European Union country members, information security is an area where Regulatory Authorities, responsibilities and guidelines overlap very often.

  For example, in Greece there are three authorities arguing for their role and responsibilities in regard of information security issues in telecommunications. I.e

  - National Telecommunications and Post Committee
  - Personal Data Protection Authority
  - Authority for the Ensuring Privacy in Telecommunications

- Besides those three, there are also other regulatory bodies whose regulations strongly affect information security issues. Typical such regulations are Competition Regulations

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

- **What should the Operators do ?**
  - **Perform staff training and promote awareness on security issues both internally (to their staff) and externally to their clients (and the society in general)**

    (Security is mostly a matter of training and awareness and not a technical issue)
  - **Ensure full compliance to the applicable legal and regulatory framework**
  - **Incorporate Risk Management in their business process model and ensure its continuous operation and feedback**
  - **Promptly and substantially inform local and European regulatory authorities and ENISA for any inconsistencies, conflicts and overappings in the legal and regulatory framework**

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

- **What should each local government do ?**
  - **Promote society awareness on security issues**
    (Security is mostly a matter of training and awareness and not a technical issue)
  - **Ensure the existence of a specific, complete, clear and effective legal framework for the protection of privacy and information security**
  - **Supervise the operation of the necessary Regulatory Authorities and intervene whenever necessary in order for them to avoid overlapping responsibilities and conflicting regulations**

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

- **What should the European Union Regulator for Security do ?**
  - **Incorporate and make use of the Operators' experience**
  - **DO WORK with the Operators for the development of a common security regulatory framework across Europe that will be able to successfully address all other issues arising from regulatory requirements in other areas as well**
  - **DO NOT WORK with other Regulators for the development of a framework in which Operators will be asked to work**
  - **Exploit ENISA to operate as a Partner and a liaison (and not just a consultant) in the information and network security in Europe**

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

- **How could ENISA help ?**

  ENISA should or could :

  - **work as a central point of reference for all enterprises, bodies, authorities and any one in the public or private sector in Europe seeking experience, knowledge, guidelines and top level training on information security and awareness issues**

    (RA/RM Workgroup job is excellent and should be followed by other similar initiatives as well as communicated to a much wider target group)
  - **cooperate with Standardization Organizations in preparing, updating and promoting international standards**
  - **Collect and distribute case studies and best practices from around Europe (or the world) and communicate them to any interested party**

Restraining Factors and Prerequisites For Implementing Security Risk Management In A National Telecommunications Operator

- **How could ENISA help ?**

  Besides being an Advisory Body, I would expect ENISA to ask and fight for a more energetic and effective role.

  It can and should be a liaison between all involved parties (on a local and Community Level) like

  - **Enterprises (or market segments)**
  - **Local Regulatory Authorities**
  - **Governments**
  - **European Commission**

  In order to make sure that all of them share the same vision, speak the same language and march towards the same direction