**James Grey**

**Essay**

**Implementing network and security measures**

**Introduction**

Securing your network requires continuous work and close attention to detail. A security service may consist of a typical set of services:

The first direction is legal protection of entrepreneurial activity, which is a legally competent registration of duties, rights and conditions for doing business (property rights to a patent, license, property, maintaining accounting documents, registration documents, agreements, leases, charters and other documents). The implementation and implementation of this protection for the safety of business is obvious, since the regulatory framework in these conditions is unstable and requires some legal protection (Denning, D. E. R. (1999).

The second direction is the physical security of entrepreneurs. In this case, not only entrepreneurs, but also the resources they use — material, financial, and information — can be participants or business entities. Intellectual resource security is also included in this category. These are service personnel, employees of the enterprise, shareholders.

The third area is information and commercial security, which is the protection of the information resources of an entrepreneur and his intellectual property.

The fourth area is the safety and security of personnel and people working at the enterprise. This is compliance with safety, labor protections, the environment, sanitation, business relationships, personal safety of employees. Based on this information, it can be concluded that a universal or ideal method of protection does not exist today, although the need for quality security is obvious, and in some cases is critically necessary.

**Problem statement**

The paper discusses the problematic issues of applying security measures in relation to participants within the local government facility. This study addresses the problematic issues of applying security measures to participants in cyber security.

**Management plan**

*“Top management should establish a clear policy direction in line with business objectives and demonstrate support and commitment to information security through the development and support of an information security policy within the organization”.* If necessary, you should provide for a contact person dealing with information security issues within the organization, which interested employees can contact.

**Measure and means of control and management**

*“The information security policy should be approved by management, published and brought to the attention of all employees of the organization and relevant third-party organizations”.*

**Risk Management**

The risk assessment process consists of the following steps:  
**1. Security Risk Assessment**

Safety requirements are determined using a systematic risk assessment. The costs of measures and means of control and management should be commensurate with the possible damage to the business as a result of the refusal to provide security.

a) Inventory and categorization of communication network resources:

1) The inventory involves the compilation of a list of all resources (assets) requiring protection (information, software, hardware and service);

2) Categorization consists in assigning to each resource a qualitative or quantitative parameter of its importance in terms of its impact on the overall functioning of the communication network;

b) Identification of the main threats;

c) Identification of vulnerabilities.

d) Analysis of the possible impacts of threats during the implementation of vulnerabilities in network resources, calculation of the probability of these impacts and the risk of damage to the network, analysis of existing security measures;

e) Determination of additional (recommended) security measures that can counteract possible impacts;

e) Documentation of the results.  
**Main security categories**

Each major security category includes:

a) The goal of management, which formulates what, should be achieved;

b) More detailed information is provided to support the implementation of measures and means of control and management and achieve the management goal.

c) Additional information is provided that may be considered, such as legal issues and references to other standards

**Physical activity**

The following methods are used to ensure information security:

**1) Obstacle.** The method is the use of physical force in order to protect information from criminal acts by intruders by banning access to information media and equipment.

**2) Access control** - a method that is based on the use of regulatory resources of an automated system that prevents access to information media. Access control is carried out using functions such as:

a)      Identification of the identity of the user, working personnel and information resource systems by such measures as the assignment of a personal identifier to each user and object;

b)      Authentication, which establishes the affiliation of a subject or object to the identifier declared by him;

c)      Checking the compliance of authorities, which consists in establishing the exact time of day, day of the week and resources for carrying out the procedures scheduled by the regulation;

d)     Access to carry out work established by the regulations and create the necessary conditions for their implementation;

e)      Registration in the form of written recording of access to protective resources;

f)       Responding to an attempt of unauthorized actions in the form of a noise alarm, shutdown, refusal of a request and a delay in work

**3) Regulation -** a method of information protection in which access to the storage and transmission of data in case of an unauthorized request is minimized.

**4) Coercion** is a method that forces users to access certain information when accessing sensitive information. Violation of the established protocol leads to penalties, administrative and criminal liability.

**Physical security vendors**

1. Physical means of protection are used as external security for monitoring the territory of the facility and protecting the automated information system in the form of special devices. Along with conventional mechanical systems, for the operation of which human participation is required electronic fully automated physical protection systems are being introduced in parallel. Using an electronic system, territorial protection of an object is carried out, access control, security of premises, surveillance, fire safety, and signaling devices are organized Bishop, M. (2003).

2. The most elementary electronic protection system consists of sensors whose signals are processed by microprocessors, electronic keys, biometric devices for identifying people and other intelligent systems. The protection of equipment included in the general automated information security system and portable devices (magnetic tapes or flash drives) is carried out using such mechanisms as:

a)      Lock systems (mechanical, radio-controlled, code, with microprocessor), which are installed on safes, doors, shutters, system units and other devices;

b)      Microswitches with which the opening and closing of windows and doors is fixed;

c)      Inertial sensors, which are used in the power supply network, telephone wires, telecommunication antennas;

d)     Stickers made of special foil are glued to devices, documents, system units, nodes, which serves as protection against removal from the territory of the organization or premises. Any attempt to transfer documents or devices with a protective stickers through the access devices will be alerted.

e)      Metal cabinets and special safes, which are used to install individual devices of the information automated system - file servers, printers and portable information carriers.

**Safety of human resources**

It is  a set of measures aimed at preventing and eliminating threats and risks, as well as negative economic aspects for the the organization, related to the work and behavior of the staff, it's intellectual potential, socio-psychological component, maintaining the health and dignity of the individual. It is clear that the security of human resources is central to other elements of the organization’s security system, since personnel ensure the functioning of all business processes.

All areas of personnel work (search, selection, reception, adaptation, development, staff motivation, etc.) are more or less connected with ensuring safety. And each decision made by the HR manager either enhances or weakens the security of the organization as a whole.

The human resources security policy includes the following technologies.

1. Management of information about employees (information management of personnel). A modern, especially large organization is impossible without establishing systematic dissemination of information using computer systems and technologies. At the same time, the task of personnel management is to receive in the optimal volume and disseminate the necessary information.

2. Legal regulation of ensuring the safety of human resources, ensuring the safety of personnel, which is based on the use of labor legislation and organizational norms, usually fixed in regulatory documents in the field of ensuring labor safety and life.

3. Establishing partnerships and cooperation with trade unions, councils of labor collectives and other organizations affecting personnel.

This implies both monitoring the situation at workplaces and taking into account individual requests and wishes of workers related to their state of health, for example, transferring to easier work or part-time for the period of final labor adaptation after an illness.

**Flow diagram**

II

Government agency network

Firewall

Internet

Internet router

Remote users

 The remote users are connected to government agencies through different internet security measures.

II

Government agency network

Firewall

Internet

Internet router

Remote users

 In this second diagram show that the patch of network devices travel beck to the remote users

**Best practices in Cyber security**

Cyber security is the protection of data that is located in electronic form and it is also related to determining the most important data, where they are located, and what technologies should be used to protect them. We all live in a world that is connected by a network and information technologies, from internet banking to the state infrastructure and that is why cyber security is a necessity. Planners and strategists are concerned about cyber attacks which are on the rise and their effects are global in nature. Hacker’s attacks are capable to undermine the world economy or inflict huge damage to the image of a country.

**Ethical concern**

 The Internet is increasingly entering the life of modern society and brings many benefits, but, on the other hand, it opens up the possibility for cybercriminals to spread malicious content and commit attacks on individuals, organizations and even the government. The cross-border nature of the Internet allows criminals, while in any place where there is a connection; to hit any unprotected sections of networks (Von Solms, R., & Van Niekerk, J. (2013). That is why ITU is taking steps to find a global solution that would help to combat this global threat. Military hackers have the right to broadcast some computer code to the network of another country. With its help you can track the quality of communication.

In one particular case, you will have to make a special emphasis (but in no way at the expense of protecting other components of the IT system), say, on protecting the website, in another - on protecting the workstation park, and somewhere will have to allocate additional funds for the creation of a fault-tolerant data store. In the end, it all depends on which type of cyber threat is the most dangerous for this particular company.

**Conclusion**

It is not easy to answer the question of how much the security of the critical infrastructure facilities are adequate at the moment because of unknown information or techniques that can be used by cybercriminals, and therefore cannot be 100% safe. What can be improved is protection against known attacks, for the prevention of which it is necessary to apply a number of effective measures:

**Recommendations**

a)      Checking systems for vulnerabilities, especially those systems where security holes have already been fixed and they have been known for some time.

b)      Adequately monitor the networks used to monitor critical infrastructure objects and, if necessary, completely isolate them from external connections, which will detect external attacks and prevent access to systems controlled from the internal network.

c)      Control of removable devices, which is important in any infrastructure, not only because they are the direction of such attacks, as in the case of Stuxnet.

d)     After having discussed the various aspects of Cyber Warfare and threat perception, the following recommendations, are offered.

**References**

Denning, D. E. R. (1999). Information warfare and security (Vol. 4). Reading, MA: Addison-Wesley.

Bishop, M. (2003). What is computer security?. IEEE Security & Privacy, 1(1), 67-69.

Tipton, H. F., & Nozaki, M. K. (2007). Information security management handbook. CRC press.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H., & Sastry, S. S. (2010, December). Cyber security analysis of state estimators in electric power systems. In 49th IEEE conference on decision and control (CDC) (pp. 5991-5998). IEEE.