Security of Data in the Utilization of E-Government
Abdulrahman Ahmed Alzand
Ministry of Science and Technology, Iraqi University, Baghdad, Iraq.

ABSTRACT
Both the computer and the software and data essential elements of a system of information in the digital environment associated with e-government. Computer may be associated with devices and services in the communication network terminal ends or other accounts or specific network facilities. Computing network may be a LAN or private network extended the scope of the government department or ministry concerned as a network intranet, or wide area WAN network as extranet or international information network such as the Internet, may also be linked to external contact is open to any individual provider technological means that enable access to her. The aim of this research is the security of information systems, protection and availability of resources and its components and work their confidentiality and integrity. Where in the absence of adequate security systems and information and communication technologies, do not use all their capacities and energies. The absence or lack of security in a loss of confidence in the system to stop and not to make the most of it, making it a burden on the organization. On this basis it must protect the system and information from damage that can lead to system failures and loss dating back to their organizations and their staff.

Introduction
You can identify three main dimensions of the target of various information in security systems, (I) definition: who is allowed to enter the system? Must check it out through three main entrances (II) dependence: once you learn the rules of the real user, the natural next question is what allowed for this person? Thus, an accreditation process based access to resources for this user (iii) Management: representing management saving the user attributes, in addition to the security of a given resource definition. It includes on activities such as the exclusion of the advantages of the arrival of the user or employee leaving the service.

The search results are in four axes task, first (Security Policy: The purpose of information security policy relates to provide appropriate guidance and administrative support to the security of the information and recommendation (II) Security organization: This dimension aims information security management focus in the organization (iii) the security of individuals: the purpose of the after the security of individuals to reduce the risk of human error, theft, embezzlement or misuse of facilities (iv) control of access to information).

Concludes research is the establishment of political, regulatory and legal frameworks to address the matters relating to the dangers of security such as piracy and management of domain names and the protection of citizens, the development of information security policy and encourage the application and adaptation programs and records of e-government, strengthen the expertise and Practice better for the security of information systems through the development of guidance and technical standards on a large scale and use including is a global developer, organize public campaigns to raise awareness aims to improve public knowledge and understanding of the importance of information and intellectual property rights and the protection of security software.

Both the computer and the software and data essential elements of a system of information in the digital environment associated with e-government. Computer may be associated with devices and services in the communication network terminal ends or other accounts or specific network facilities. Computing network may be a LAN or private network extended the scope of the government department or ministry concerned as a network intranet, or wide area WAN network as extranet or international information network such as the Internet, may also be linked to external contact is open to any individual provider technological means that enable access to her.

And include a lot of information networks on the collection of internal and external links, and contact networks include contact information, in addition to phone and fax modem. And other devices with printers, computers and communications may be linked. Computer software may include the operation and software applications that are designed specifically for a particular client reformer or a particular government agency systems. Software has been installed in the computer or stored on CD-ROMs, or any other storage media available. And supports paper or documentary evidence phones and read electronic hardware and software and the use and maintenance operation.

It arises full structure of the systems and applications of information in the digital environment in order to store the data and information processing and retrieval and send or transfer target for the user. And brings together all these different elements together and the many to form the information system in the digital environment, which represents a dynamic information and communications technology developed in supporting the digital environment.
and the associated electronic developments as the government and e-learning and telemedicine.

Figure 1. information security system components.

1. Operations: Possesses operations are considered indispensable for any security system; they are substantial and continuing nature. And it governs information security operations tool set of standards such as those established by the International Organization for Standardization ISO, which is of great value to any security information system. And apply processes in an orderly way as constantly declining in the context of accumulated experience in order to exclude errors and risks.

2. Humans: People who represent workers, consultants, contractors, technicians and perform all operations and services, and require their presence by developing relevant disciplines and skills, experience and motivation occasion.

3. Technology: Technology is considered available and ready, but its products are relatively short life cycles. Technology market is competitive edition, available with a large number of producers and suppliers, vendors and distributors who come and go, they have been integrated into the larger firms or they may lose in and out of the business market. This makes it difficult to technology than it was in the past evaluation.

4. Culture: Culture linked to the interpretation relating to the business environment and the ethics of the organization to the community, where it is to manage the organization a key role to play in keeping compliant organization's culture with the culture of their community

In this context, the ruling could determine the following factors

1. Increase the use and effectiveness of the value of computers and communication facilities, networks of computers and communications, and data and information that is stored and treated and recovered and sent through which included programs, specifications and procedures.

2. The global nature of the systems and applications of information and spread to all levels of local, national and international.

3. As a result of the increasing role of systems and applications of growing importance and dependence growing in the economy, trade, management and learning any in all aspects of social, cultural and political life of information, it has led to special efforts to ensure trust and credibility of these systems and applications in terms of security and transparency to users.

4. Data and information available in the systems and applications of electronic information additional features make them different and distinct from the paper or traditional documentary systems, makes it imperative that there should be as follows:

• Suitable ways to increase awareness of the risks surrounding information systems and applications.

• Directives, standards and methods codified to protect the security and transparency of information and its system and its applications in the digital environment.

• Appropriate measures to criminalize compromising the confidentiality and privacy, and availability of data and information to its users.

• Standards and procedures reflect the principles pertaining to electronic information security.

On this basis, the strengthening of trust and security in the use of information and communications technology will enhance the trust framework, including information security and security checks and safeguarding privacy and confidentiality and protect the user citizen, which is a precondition for the establishment of e-government projects for the development of the information society to build trust among ICT users.

Modern society has seen a lot of developments, including:

1. Proliferation mechanism and complexity of computers and spread in all aspects of the life of contemporary society.

2. Cohesion and complexity of information and communication technologies.

3. Continue greatest technology of computers, communications and interoperability of their systems and applications.

4. Do not centralized functions of computers and communications increased.

5. The growth of the use of computers to the extent that each individual is an actual user or unexpected information and communication networks, especially in developed countries, technology.

The aim of research

The aim of this research is the security of information systems, protection and availability of resources and its components and work their confidentiality and integrity. Where in the absence of adequate security systems and information and communication technologies, do not use all their capacities and energies. The absence or lack of security in a loss of confidence in the system to stop and not to make the most of it, making it a burden on the organization. On this basis it must protect the system and information from damage that can lead to system failures and loss dating back to their organizations and their personnel.

Security systems and is one of the essential pillars of the ruling to protect individuals and organizations from damages resulting from the lack of security, where both individuals and organizations to support the performance of their information systems by ensuring their security minute ways, convenient and reliable. A clear example of the security of information systems can be seen in hospital information systems, the control of traffic systems or aeronautics, nuclear power plants, etc. And moving security to preserve the effectiveness and efficiency of information systems, and to confirm the level suitable for the availability, confidentiality and integrity, as well as facilitate the development and use by individuals concerned new purposes unconventional differ from those that have already applied, and facilitates the exploitation of information technology at full capacity and potential. Thus contributing to the field of security systems to protect the rights and interests of all accredited handled protect and maintenance of the damage resulting from the availability, confidentiality and integrity procedures to fail.
The Methods
- Some processors security (verification of security operations): Four main dimensions of the target of various information which is to determine the following security systems:
  (1) Definition: Identification and Authentication
Who is allowed to enter the system? Should check it out through three entrances essential and achievable is:
1. The need to inform or to tell the computer about Shi ID: person's name or password. In spite of that passwords easy application and implementation, but they include some of the palaces, where they can give it to a third party. It can also be the subject of complex rules associated with the number of letters and numbers, and change in each time period, etc. In these cases there is a strong trend in the writing of passwords that can survive and not disclose their content even when found by someone else.
2. Provide something that belongs to the person to engage in identity-card system or a personal identification code, or what, where it can increase the security of the system that are required in addition to the password of some types of natural equipment or identity or a particular letter code to allow access card.
3. Give something special system the user is linked to personal properties, such as a fingerprint or voice pattern personal pulse-called biological Biometrics where measurements can be used in a secure environment. In spite of that associated with the technology so complicated and expensive, but its use is growing.
(2)Accreditation: Authorization
Once you know the real user's system, the next question naturally is what allowed for this person? Thus, an accreditation process based access to resources of this person. For example, to identify transactions or data that allows him to them, and those that the user can be modified or added. And embrace the advantages of access based on user and determine its responsibilities and the role of his rights by the system. In the case of information services providers such as libraries, e-commerce companies, etc. These advantages decide specific criteria determined by contracts, agreements, contributions, or credit rights, etc.
(3) Management: Administration
Saving the management is user attributes, in addition to the security of a given resource definition. This includes activities such as the exclusion of the advantages of the arrival of the user or employee leaving the service, change the attributes, determine the order list as permitted by a particular user after the upgrade or transport.
3. Information security considerations:
Can identify three main dimensions of information security are:
(1) lack of security investigator presence completely:
Any system or device information There is no one way to adoption. And limited knowledge of how to use the system or tool on a very limited number of individuals, which do not appear or discover many non-qualified and trained. In the area of information security, which does not accept 100% of the industry, can be observed the following:
• While the software is designed to perform certain functions, the developers of experts (including hackers like all of Hackers, Crackers and) they can do so for the performance of other things as well.
• there are still no complete software perfection 100%, as each software include Bugs errors in the encryption or coding in computer programs.
The following four statements are true in a practical way in practice:
• The new software includes means new errors.
• the old mistakes are not always suitable.
• Do not apply corrections always Fixes.
• It may include corrections to new errors.
(2) the balance between risk and cost:
Both take various measures to protect property and lives and the degree to which implemented these measures are affected by the extent of the risks surrounding the appreciation and the desire to accept the restrictions that will be imposed by these actions in our daily lives and cost.
It must identify it in real life can be the following occurs:
• Despite the protection that we take action, there is no guarantee that it will not be effective all the time.
• risks change over time against what we seek measures to protect ourselves. It needs assessment and action taken to protect the security of information to be changed by extension to be effective.
• Security measures include the continuous investments and expenses.
The core component of information security practice in the evaluation and assessment of the value of assets required to protect vulnerable with her threats and raised these penetrations and gaps of information security. And as such, it becomes necessary to accept the risk inherent possible level of definition.
(3) balance the need for security and dissatisfaction with the status quo:
As already mentioned, there is nothing in today's world full and nicely College. This is a true and real in relation to the information and property and selves. It includes all the added process or activity an additional prompt to end users the security procedure. Whenever added these procedures have become, at the same time, the obstacles to be overcome by each end user, regardless of the many remember the words of the passage and similar security measures. As a result, increasing download manager or administrative burdens of a new system it absorbed and implemented.
Results: suggested solutions
(1) Security Policy:
The purpose of information security policy relates to provide appropriate guidance and administrative support to the security of the information and recommendation, including the following:
• Provide campaigns and educational programs and training to information security.
• Risk management as an entry point of the entrances to the administrative process in the organization.
• Compatibility with the appropriate laws and regulations.
On this basis, any document or report information security policy should include the following:
• Organization's need for a contingency plan Contingency Plan.
• The need to support the preservation of data and information effectively and efficiently.
• Avoid infected software.
• Provide oversight procedures access to information systems and data.
• Events experienced by the organization with regard to the security of their information report.
This principle is intended to assist individuals interested in legal security systems to learn and get information security system. It is not limited to just the success of an information system or certain security standards, and should not be established as a trend for the security risky. In this context, the level of information that the corresponding sought to this principle, should help to get it without the lax security procedures. This includes the principle owners and presenters, where there may be cases where the need to supply information about the system's security. For example, you may enter information network owner in the agreement or the participation in the service of another organization might want to use to provide services to third parties. System owner may require, as part of the agreement, or is available to provide a certain security levels. In this case, this person may wish or organization that owns the recognition system for the security of its information system. By analogy with this, you may hire any organization with information or computer network owner to provide certain services may require special independent security and the ability to achieve security and reviewed on an ongoing basis for the assertions.

Includes users of the information system is also in the principle of awareness. For example, the end-user or customer who chooses a particular bank may have a legitimate interest in knowing the security policies of the Bank and other banks. Depending on the security policies used to promote shopping and banking services as a tool to attract customers.

(3) Ethics: Ethics

In the modern era, it became information systems permeate our societies and our cultures, was accompanied by expectations and rules associated with the appropriate security in supply growth and the use of these systems. This principle is supported by the development of social standards linked to the security of information that are important aspects in the expression of standards and guidelines for all members of society at all levels and ages in addition to instill in the minds of students, youth and workers it included in the applicable customs since childhood. This means that information systems and security must be provided and used in the manner that respects the rights and legitimate interests of others.

Conclusion

Accept this work-related trends the security and transparency of information under the e-government, a major expansion in the use of electronic information services charged to systems of all types of information systems applications (local area networks, intranets, extranet networks, wide area network and the Internet), some of which rely on some, and their vulnerability to various damage and the need to build confidence in them, has led both to expand the topic of information security and systems in digital environments. And select the concept of information security and different classes, and under it, and its components and themes linked with threats to information security and damages that may result from the lack of security measures, while enhancing the security of existing information systems.

The following set of results derived from this work:

1. The establishment of political, regulatory and legal frameworks to address the matters relating to security risks such as piracy and management of domain names and the protection of citizens and expand this protection in the digital environment.
2. Develop information security policy and encourage the application and adaptation programs and records of e-government.
3. Practice and strengthen the experience better for the security of information systems through the development of guidance and technical standards on a large scale and the use of what is a global developer.

4. Organize public campaigns to raise awareness aims to improve public knowledge and understanding of the importance of information and intellectual property rights and the protection of security software.

5. Promote initiatives that ensure a fair balance between intellectual property rights and interests of the users of the information in the fields of software and e-commerce and e-government, etc.

6. Identification and allocation of risk and liability related to the failure of information security, and the associated administrative sanctions and criminal penalties associated with improper use or intentional damage.

7. Awareness of information security and the need to work on the problem of protecting and securing information and networks of transport systems.

References


2. IEEE 8012.10 Standards for Interoperable Local Network Security (SILS).

3. IETF. IPSEC Working Group.


5. IETF. SAAG (Security Area Advisory Group).


