Information systems security in the Greek public sector

Euripidis Loukis
University of the Aegean, Karlovasi, Greece
Diomidis Spinellis
University of the Aegean, Karlovasi, Greece

Keywords
Security, Public sector, Information systems, Greece

Abstract
The security aspects of public sector information systems are important as the respective systems are often part of critical infrastructures or deal with personal or sensitive data. A set of 53 Greek public sector organizations were investigated by means of a structured questionnaire concerning important aspects of information systems security. We present the relevant theoretical background, the methodology of our research, and an analysis of the obtained results. Greek public sector organizations have only a basic level of information system security awareness. Most care about digital data confidentiality; however, only a small percentage have developed a systematic, complete, and integrated approach towards the security of their information system, including internal audit procedures. The importance of proper training and generally the importance of the human factor for achieving high levels of information systems security is often underestimated.

Information Management & Computer Security
9/1 [2001] 21–31

[ISSN 0968-5227]

Introduction

The security aspects of public sector information systems are important as these are often part of critical infrastructures or deal with personal or sensitive data. Although the size of the public sector varies between different countries, it usually includes the central government, which consists of a number of individual ministries (departments in the USA), and also the various levels of local government, which consist of a large number of smaller organizations (regional administrations, prefectures, municipalities, etc.) distributed all over the country. In most countries the public sector performs numerous critical functions for their economic and social life and development and sets the legislation, the rules and the whole framework for all economic and social activities. Public sector also includes the armed forces, the police, the social security, the emergency services, the legislative and judicial authorities and numerous independent oversight authorities, all of them being of critical importance for the whole economic and social activity. Additionally in some countries there are public organizations (public sector enterprises) providing services and goods, which are considered essential for strategic reasons, and therefore fall under the state umbrella. This category can be very wide and can include banks, hospitals, research institutes, educational establishments, state-owned lotteries, energy, telecommunications and transport organizations, as well as industries processing critical raw materials, handling nuclear power, and defence equipment manufacturers.

Public sector organizations have increasingly relied on the use of information systems for collecting, processing, and analysing data, in order to support their functions (Swain and White, 1992; Willcocks, 1992; Loukis and Michalopoulos, 1995). In most cases information systems are used for:

- administrative support functions, such as handling personnel, payroll, budget, inventories, and office automation tasks;
- service provision and relevant operations associated with their core functions, such as tax collection (Ministry of Finance), driver licence issuing and maintenance (Ministry of Transport), agricultural production subsidy management (Ministry of Agriculture);
- internal coordination and control;
- public policy analysis, design; implementation and monitoring;
- management and decision making; and
- interorganizational coordination and cooperation between the various public organizations.

Recent generations of public sector information systems are much more outwards looking; they support the electronic delivery of public services to the citizens and the enterprises, enabling them to make most of their transactions with the government via electronic channels, such as the Internet (Bellamy and Taylor, 1998; Bekkers and Zouridis, 1999). New concepts are being developed based on the above advanced capabilities, such as the "New Electronic Customer Focused Government", and the "Virtual Public Enterprises".

Public sector information systems differ in a number of qualitative aspects from systems found in the private sector. The strategic and pervasive nature of many public sector organizations means that failures of their information system can lead to large-scale disruptions to many economic and social activities and even endanger human lives (e.g. failures in emergency service systems).

Information Management &
Computer Security
9/1 [2001] 21–31

Their *availability* is therefore often an important aspect of their operation. In addition, a number of information systems, such as those used for providing health-related services or for managing tax collection, deal with personal, confidential, or sensitive data. Such systems must guarantee a high level of *confidentiality* of the data they handle. The possibilities that exist for exchanging and combining data between public sector organizations create opportunities for violating individual *privacy*, which should be managed effectively. Furthermore, because of the importance of the data stored in the public sector information systems, their *integrity* is a critical requirement. Finally, the modern outwards looking public sector information systems, which support the electronic delivery of public services, are typically accessed via the Internet not only by a limited number of public servants but also by numerous citizens and enterprises, posing additional network-related security issues.

It should also be emphasized that information system planning, development, operation and management in public sector organizations is performed in a uniquely challenging context. Public sector organizations are often burdened with inflexible procurement, hiring and rewarding procedures and operate in an inflexible institutional framework; they are rarely subjected to the rigours of the market economy, while they are often encumbered by having to respond to political pressures. These factors contribute towards a set of unique, demanding, and sometimes difficult issues regarding information system security (ISS).

Although much research has been performed on the development of technical and organizational measures for achieving higher levels of ISS, limited research has been done on measuring and investigating the actual application of these measures in the real-life information systems, especially in "difficult" and challenging contexts, such as the one of the public sector. Also limited research has examined the complete organizational and technical context in which ISS measures, policies and procedures are designed and implemented. This research is very important, in order to determine the organizational and technological context factors affecting the application of the above ISS measures and to find contexts favouring the application of them. In these research directions the present study attempts to contribute. The pervasiveness of information systems in the public sector, coupled with the importance of availability, confidentiality and integrity in their operation, prompted us to investigate the current state of the art in the Greek public sector concerning ISS and the context factors affecting it. A set of 53 public sector organizations were investigated by means of a structured questionnaire concerning important aspects of ISS and its context. In the following sections we present the theoretical background concerning ISS, the methodology of our research, the results we obtained, and our interpretation. As Greece is currently advancing in a number of economic benchmarks from a "developing" to a "developed" nation, we believe that these findings are relevant – and can be of particular interest – to the large number of economies undergoing a similar transition.

Theoretical background

The security of an information system involves the availability, confidentiality and integrity of its data and its functionalities (INFOSEC, 1993). As information flows through a corporate or public network environment, in any instant, it can be in one of the following states (Pfleeger, 1996):

- Storage: the data are either in volatile memory or in permanent storage, on either the client, or an intermediate proxy, or the server computer system.
- Processing: operations are performed on data by the client or the server computer system.
- Transmission: data are conveyed through a certain medium, which is part of a LAN or a WAN.

In each of these discrete states, the potential threat agents may be (Meyer *et al.*, 1995):

- *Malicious authorised users*. Users, who are definitely authorised to access some information, may perform an illicit action, behaving as intruders, in order to access or to modify information in an unauthorised manner.
- *Negligent authorised users*. Users, who are definitely authorised to access some information, may accidentally do something wrong, resulting in the modification of that information or disclosing it to another user who is not unauthorised.
- *Outsiders*. Users, who are not authorised to access or modify some information, acting as intruders, may attempt to achieve this goal.

The main threats can be classified, with respect to the potential result, as (Meyer *et al.*, 1995):

- *Disclosure*. Loss of confidentiality and privacy.
- *Modification*. Loss of integrity.
- *Fabrication*. Loss of authenticity.
- *Repudiation*. Loss of attribution.

Following this classification, in the following paragraphs we present the way these specific threats can apply to data on clients, in transit, and on servers.

Disclosure: loss of confidentiality and privacy
For data on servers a threat agent may exploit inadequate access control, programming errors, or use impersonation. Legitimate users may disclose data to third parties who do not have access rights. This threat applies particularly to private corporate data distributed on an Intranet. Data in transit can be observed via wiretapping, misrouting, or accessing server and proxy logs and cache structures. Unprotected networks and applications are vulnerable to all threat agents, but protected ones are only exposed to vulnerabilities by authorised agents. Data on clients are vulnerable to disclosure when residing on an insecure operating system, or when executing Web-obtained software. Client masquerading may also be used to cause disclosure.

Modification: loss of integrity
Weaknesses on servers, at the application or the operating system level, can be (and have been) exploited to cause server data modification. Wiretapping may also be used to modify or destroy data packets in transit. In addition, data on clients are vulnerable to modification when executing Web-obtained software.

Fabrication: loss of authenticity
Threat agents may create masquerade servers or documents on a server. For data in transit a threat agent may falsify the source of information (server or individual). A threat agent may also falsify the user or host identity presented to the server.

Repudiation: loss of attribution
Users sending information to a server may repudiate their actions, and document authors may falsely claim not to be the document's true author. The first threat is particularly relevant to Web-based transactions used e.g. for on-line transactions, while the second one applies to the distribution of illegitimate content.

In addition to the above, a number of threats are related to the environment and include natural disasters, power failures, physical attacks, and accidental physical damage.

A public organization or private enterprise cannot reasonably develop efficient security policies and procedures, without clearly understanding the systems that must be protected, as well as how valuable they are to its activities. In addition the probability that the assets will be threatened must be determined. Therefore, the objective of a risk analysis review is to identify and assess the risks to which the information system and its assets are exposed, in order to select appropriate and justified security safeguards (Commission of the European Communities, 1993).

The analysis of risks is performed in four stages (Eloff *et al.*, 1993; Wilsher and Kurth, 1996):

1 Asset identification and valuation.
2 Threat identification and assessment.
3 Vulnerability assessment.
4 Risk assessment.

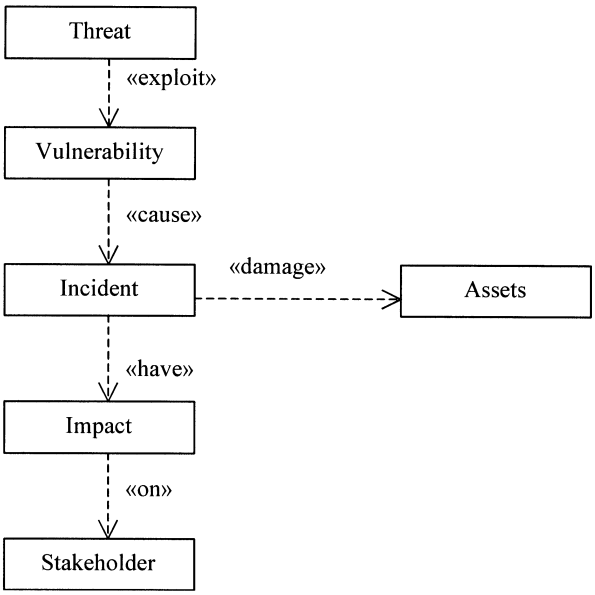
Assets are the elements of an information system that possess a value. A *security incident* that will affect an asset, will also have an *impact* on the *owner* of the asset (i.e. the organization, the enterprise, or the individual) and generally of a *stakeholder* of it. Assets are evaluated according to the impact of a probable asset impairment. *Threats* need to exploit a certain *vulnerability* in order to cause a security incident. Therefore, threats, vulnerabilities, and impacts should be combined together to provide a measure of the risk an information system is exposed to (Spinellis *et al.*, 1999). The relationship between the above entities is illustrated as a UML dependency diagram in Figure 1.

Following the risk analysis, the public organization or private enterprise should develop a security plan to address its vulnerabilities, which present a high level of risk. The security plan should be implemented by a security policy, which defines how security will be handled. The security policy should address the appropriate use of the organizational resources, the requirements on individuals who request and maintain accounts, the acceptable methods of remotely connecting to the organizational LAN, the ways information is protected from unauthorised access, disclosure, corruption, and loss, the procedures for adding new devices to the network, and the rules regarding the use of privileged system accounts (Oppenheimer *et al.*, 1997). The security policy should be periodically reviewed, in order to ensure that an appropriate assurance level is maintained. In addition, the security policy should include appropriate procedures for handling and responding to security

incidents and natural disasters, and appropriate hiring practices for minimizing employee-related threats.

Countermeasures that a security policy can utilise to deal with the threats outlined above, include at the hardware level the use of environmental controls and alarms for dealing with the corresponding threats, the use of uninterruptible power supplies for dealing with power failures, and the physical protection of equipment and redundant planning of network routes for mitigating physical attacks and damages. At the software level passwords, hardware tokens, and biometric information combined with the use of cryptography for authentication and properly configured firewalls can be used to guard against undesired system access, while a proper back-up plan (including off-site back-ups), the use of RAID technology, and the organization of a back-up data processing site can be used to recover from physical damage. Cryptography plays a major role in countermeasure implementation, as it can be used to guard against network snooping and active network attacks. Also, IS audit procedures should be established, audit logs should be used to detect undesired system access, while user training will help prevent accidental physical damage and – more importantly – attacks based on social engineering. Finally, having a properly trained full-time IS security officer will result in better coordination and monitoring of the above security countermeasures.

Figure 1
Security-related entities and their relationships



Methodology

To investigate ISS in the Greek public administration and the context factors affecting it, we selected a representative sample of 90 public sector organizations. The sample includes central government organizations (e.g. ministries and general secretariats), local government organizations (e.g. regions, prefectures and municipalities), public sector enterprises (providing goods and services of strategic importance) and social security organizations of various sizes (small, medium, and big ones) and of various computerization levels and IS sizes.

Next, a structured questionnaire was constructed, pre-tested, and sent to these 90 organizations, in order to measure:

- a number of ISS variables concerning the ISS measures taken, and
- a number of information systems security context variables, concerning the whole organizational and technical context in which ISS measures, policies, and procedures are designed and implemented.

The questionnaire included 14 questions of yes/no type, asking whether 14 basic ISS measures M1-M14 were implemented in the specific public sector organization. We selected the measures based on the relevant literature and the theoretical background presented in the previous section. The basic ISS measures investigated can be grouped into four categories outlined in Table I.

The corresponding variables M1-M14 take value "0" if the corresponding ISS measure is applied in the specific organization and value "1" if it is not applied.

It is also important to focus on the whole organizational and technical context, in which ISS measures, policies and procedures are designed and implemented, in order to determine the organizational and technological context factors which affect the application of the above ISS measures, and to find contexts favouring their application. The selection of a first set of possible context factors, which might be associated with the application of the ISS measures, was based on the framework for information systems development risks assessment, which was proposed by Willcocks and Margetts (1994). This framework classifies the risk factors into four categories: internal context risk factors, external context risk factors, process risk factors, and content risk factors. Adapting the above framework to the needs of the present study, the following seven organizational and technological context factors C1-C7, outlined in Table II, were

Table I
Investigated ISS measures

Analysis measures
M1: Analysis of the risks from a security violation
M2: Analysis of the confidentiality of the data electronically stored in the IS

Organizational measures
M3: Recovery procedures from a violation of data confidentiality
M4: Written and approved ISS plan
M5: Written and approved ISS policy, with specific roles and procedures
M6: Security zones, both at logical and physical level
M7: Procedures for back-up copies
M8: Procedures for IS internal audit

Technical measures
M9: Physical access control (via entrance cards, cameras, etc.)
M10: Firewall system operational

Human resources measures
M11: Full-time IS security officer
M12: Full-time network administrator
M13: Proper training of the IS security officer and the network administrator
M14: Proper training of the IS users in the correct and secure usage of the IS

Table II
Organizational and technological context factors

Internal use context factors
C1: Number of IS users
C2: Number of supported functions of the organization by the IS

Internal IT unit context factors
C3: Number of specialized IT staff of the IS organizational unit
C4: Hierarchical level of the IS organizational unit

External context factors
C5: Previous incidents of electronic data confidentiality violation
C6: Access to the IS by external users (e.g. external contractors)
C7: Connection of the IS (at least of one of its computers) to the Internet

selected to be measured via corresponding questions.

The anwers to the above 21 questions were analysed in three phases. In the first phase we calculated the statistics of the application of the 14 ISS measures M1-M14 (showing what percentage of the investigated public sector organizations use and apply each of them), and the statistics of the seven context factors C1-C7. Also for each of the investigated organizations, a total Information Systems Security Index (ISSEI) was calculated, defined as the percentage of the above 14 ISS measures M1-M14, which are applied in this organization:

$$ISSEI = \frac{\sum_{i=1}^{14} M_i}{14}$$

In the second phase cluster analyses were performed, both at the case (public organization) level and at the variable (ISS measure) level, in order to investigate whether there is clustering of the public organizations concerning ISS measures, and also whether there is clustering of the ISS measures concerning their application. Finally in the third phase multivariable analyses were performed (Analyses of Variance and X^2 Independence Tests), in order to examine the association between the above ISS measures application, and the above context factors.

Results

From the 90 public sector organizations, to which questionnaires were sent, we received a total of 53 responses, giving an overall response rate of 59 per cent. However it should be mentioned that even these 53 organizations, which finally completed the questionnaire, initially were not willing to complete it, because they believed that data about the security of their information systems should not be disclosed outside their organizations. They finally agreed to complete the questionnaire after we signed a non-disclosure agreement and we committed ourselves to publish only aggregate data from a large number of public sector organizations. This is a typical difficulty when measuring and investigating the actual application of various ISS technologies and measures in the real-life information systems.

Context factors

The statistics of the context factors C1-C7 in the above 53 public sector organizations are shown in Table III.

We can see that more than half (53 per cent) of the respondents have less than or equal to 100 IS users, while 24 per cent of them have between 100 and 400 IS users and the remaining 23 per cent have more than 400 IS users. From the descriptions of their IS, it was concluded that 39 per cent of them have a complete integrated IS supporting all their functions, 39 per cent have a fundamental IS supporting their most important functions,

Table III
Context factors C1-C7 statistics

C1: Number of IS users		C2: Supported functions by the IS		C3: Number of Staff of the IS Unit		C4: Hierarchical level of the IS Unit		C5: Incidents of confid. violation		C6: Access by external users		C7: Connection of IS to the Internet	
0-100	53%	All functions	39%	0-10	48%	Directorate	58%	Yes	4%	Yes	31%	Yes	53%
101-400	24%	Most important	39%	11-40	29%	Section	42%	No	96%	No	69%	No	47%
> 400	23%	Small number	22%	> 40	23%								

while 22 per cent have a smaller IS supporting only a small number of their functions. As to their specialized IT staff of their IS units, about half of the respondents (48 per cent) have less or equal to ten, 29 per cent have between 10 and 40 and the remaining 23 per cent have more than 40. The hierarchical level of the IS unit is a good indicator of the importance for the organization of its IS; in the majority of the respondents (58 per cent) the IS unit is a directorate, while in the remaining 42 per cent it has a lower hierarchical level, being a Section of another directorate, such as the financial or personnel directorate.

Only a small percentage (4 per cent) of the respondents replied that they had in the past incidents of data confidentiality violations; however it is possible that this percentage is higher, because some of these public sector organizations might not want to disclose such incidents. In 31 per cent of the respondents their IS are accessed by some external users (e.g. external contractors), and in 53 per cent of them their IS (at least of one of its computers) are connected to the Internet.

Information systems security measures

The percentage of the respondents, which apply each of the ISS measures M1-M14, is shown in Table IV.

Concerning the ISS analysis measures, we can see that less than one-third (30 per cent) of the respondents have prepared a complete analysis of the risks from security violations. However, more than half of them (53 per cent) have prepared at least a subset of such a complete analysis, limited to the analysis of the confidentiality of the data, which are electronically stored in their IS. This is probably due to the personal and sensitive data stored in the IS of many public sector organizations, whose confidentiality is very important and in most cases protected by law.

Concerning the ISS organizational measures, we can see that most of the respondents (89 per cent) have established procedures for taking back-up copies, which is the ISS measure with the widest application among the ones investigated. More than half (55 per cent) of the respondents have established procedures for recovery from a data confidentiality violation, probably for the reasons explained above. Also more than half of the respondents (51 per cent) have established security zones at a logical and physical level. However, much lower is the percentage of the respondents, which have prepared a complete written and approved ISS plan (only 19 per cent) or a complete written and approved ISS policy with specific roles and procedures (only 23 per cent). Therefore, though the majority of the respondents take some well-established ISS organizational measures (back-up copies, security zones, recovery procedures), only a small percentage of them (about one-fifth) have developed a systematic, complete and integrated approach towards the security of their IS, such as an ISS plan and an ISS policy. Also, only about one-quarter (26 per cent) of the respondents have established procedures for IS internal audit.

Concerning the ISS technical measures, we can see that 38 per cent of the respondents use firewall systems. If we take into account that 53 per cent of the respondents have their IS connected to the Internet (Table III), we come to the conclusion that a big majority of them (38 per cent/53 per cent = 71.7 per cent of them) use firewall systems. Much lower is the application of physical access control; only about one-quarter of the respondents (26 per cent), take physical access control measures, based on entrance cards, cameras, etc.

Finally, concerning ISS human resource measures, we can see that, although 24 per cent of the respondents have a full-time IS security officer and 38 per cent of them have a full-time network administrator, in only 34 per cent of the respondents the IS security officer and the network administrator (full-time or part-time) have proper training. In addition, limited emphasis has been put on the training of the IS users; in only 38 per cent of the respondents users have proper training in the correct and secure use of the IS. This is

probably due to an underestimation of the importance of proper training and generally of the importance of the human factor for achieving high levels of ISS.

Information Systems Security Index

The statistics of the Information Systems Security Index (ISSEI) in the respondents are shown in Table V.

We can see that the mean of the ISSEI in the respondents is 0.39, which means that on average the investigated public sector organizations use only 39 per cent of the above 14 basic ISS measures M1-M14. However the standard deviation of the ISSEI has a value of 0.26, which is quite high compared with its mean. Also the range of the ISSEI values (i.e. the difference between its maximimum and its minimum among the respondents) has the highest possible value of 1.0000 indicating large differences between the respondents. This is confirmed by the distibution of ISSEI values (Table V), where we can see that about half of the respondents (47 per cent) use less than 30 per cent of the above 14 basic ISS measures, while about one-third of them (34 per cent) use between 30 per cent and 60 per cent of these measures. Only a small percentage of the respondents (19 per cent) use more than 60 per cent of these 14 basic ISS measures.

Cluster analyses

Given the observed big differences among the respondents concerning the application of the above 14 basic ISS measures we proceeded to further examine the results using cluster analysis. A series of cluster analyses were performed, both at the case (public organization) level and at the variable (ISS measure) level, in order to investigate whether there is clustering of the public organizations in a number of types concerning ISS measures, and also whether there is clustering of the ISS measures concerning their application.

At the case (public organizations) level, hierarchical clustering analysis of the investigated public organizations was initially performed based on all the ISS variables M1-M14, in a fully unsupervised way without specifying the number of clusters. As measure of similarity between public organizations concerning ISS, we used the Euclidean distance. From this analysis two clearly distinct clusters of public organizations were detected. Next a K-means clustering analysis was performed. The number of clusters was specified to be two, according to the above hierarchical clustering analysis results. The results of these two analyses concerning the cluster membership of the investigated public organizations were similar, which was one more indication of the validity and the robustness of the detected clusters. The centers of these two clusters in the 14-dimensional space of the 14 ISS variables are shown in Table VI. Each of these centers has as components the average values of the 14 ISS variables in the corresponding cluster. Also in the last column of Table VI we can see for each of the 14 ISS variables the corresponding *F*-ratio, which is the ratio of the variance between the centers of the clusters to the mean variance within the clusters for the specific variable.

The first cluster consists of 12 public sector organizations, mainly critical public enterprises, banks, hospitals, social security organizations, etc., while the second cluster consists of the remaining 43 public organizations, mainly of the central and the local government. We can see from Table VI that the first cluster is characterized by much higher average values of the 14 ISS variables than the second cluster, which means much higher application percentages

Table V
ISSEI statistics

Descriptives		Distribution	
Mean	0.39	< 0.30	47 %
St. deviation	0.26	0.30 – 0.60	34 %
Minimum	0.0000	> 0.60	19 %
Maximum	1.0000		

Table IV
ISS measures M1-M14 application percentages

	Application percentages
ISS analysis measures	
M1: Analysis of the risks from a security violation	30
M2: Analysis of the data confidentiality	53
ISS Organizational measures	
M3: Recovery procedures from a data confidentiality violation	55
M4: Written and approved ISS plan	19
M5: Written and approved ISS policy (roles and procedures)	23
M6: Security zones, both at the logical and the physical level	51
M7: Procedures for back-up copies	89
M8: Procedures for IS internal audit	26
ISS technical measures	
M9: Physical access control	26
M10: Firewall system	38
ISS human resources measures	
M11: Full-time IS security officer	24
M12: Full-time network administrator	38
M13: Proper training of the IS security officer and the network administrator	34
M14: Proper training of the IS users in the correct and secure usage of the IS	38

Table VI
Centers of the clusters and *F*-ratio

	Center of cluster 1	Center of cluster 2	*F*-ratio
M1	0.83	0.16	29.72
M2	0.92	0.44	9.89
M3	0.92	0.46	8.78
M4	0.75	0.02	77.28
M5	0.67	0.10	23.65
M6	0.92	0.41	11.14
M7	1.00	0.87	1.65
M8	0.75	0.13	26.30
M9	0.67	0.15	16.46
M10	0.67	0.32	4.95
M11	0.75	0.10	34.39
M12	0.92	0.22	27.98
M13	0.75	0.24	12.64
M14	0.67	0.30	5.61

of these 14 ISS measures. Therefore these two clusters of public organizations differ to a large extent concerning ISS: the organizations of the first cluster put much more emphasis on ISS and take more measures for managing the relevant threats than the ones of the second cluster. Also we can see that the biggest differences between these two clusters lie in the variables M4 (written and approved ISS plan), M11 (full-time IS security officer), M1 (analysis of the risks from a security violation), M12 (full-time network administrator), M8 (procedures for IS internal audit), M5 (written and approved ISS policy, with specific roles and procedures), and which are characterized by the highest *F*-ratio values. In the other variables the differences between the two clusters are lower, as indicated by the corresponding lower *F*-ratio values. Therefore, the main difference between these two clusters lies in the application of the above more "advanced" ISS measures, and much less in the application of the other measures.

From the above cluster analyses we draw the conclusion that there are two quite different and distinct typologies of public organizations concerning ISS. The first of them can be described as critical public enterprises, banks, hospitals, social security organizations, etc., applying most of the investigated ISS measures including the more "advanced" ones. The second typology can be described as central and local government organizations, applying only some of the investigated ISS measures, but not the more "advanced" ones.

At the variables (ISS measures) level we performed in addition an hierarchical clustering analysis of the 14 ISS measures based on their application or not in the investigated public sector organizations, again in a fully unsupervised way without specifying the number of clusters. As a measure of similarity between these ISS measures concerning their application, we used the Euclidean distance between their corresponding values in all the investigated public sector organizations. In Table VII we can see the normalized squared Euclidean distances (NSEDij) between the ISS measures M1-M14, which are equal to the corresponding Euclidean distances between them divided by the total number of the respondent public sector organizations. In this sense, the NSEDij between any two ISS measures Mi and Mj lies in [0,1] and represents the percentage of the respondents taking different action for these two measures (apply one and not apply the other), while (1 – NSEDij) represents the percentage of the respondents taking the same action for these two measures (either apply both of them, or apply neither of them).

From Table VII we can see that the NSEDs between the investigated ISS measures vary significantly. The lowest NSEDs are the ones between M4 (written and approved ISS plan), M5 (written and approved ISS policy, with specific roles and procedures) and M11 (full-time IS security officer), namely between some of the most "advanced" ISS measures, indicating that the application of one of them is highly associated with the respective application of the others and the opposite.

From the cluster analysis we performed based on the above distances, two basic clusters of ISS measures were detected. The first cluster consists of M2 (analysis of data confidentiality), M6 (security zones at the logical and the physical level) and M7 (Procedures for back-up copies), which according to the section discussing information systems security measures are the most widely applied and very basic ISS measures, while the second cluster consists of the remaining ones. This second cluster includes a subcluster, with very low distances between its members, according to the discussion of the previous paragraph, consisting of the most "advanced" ISS measures M4 (written and approved ISS plan), M5 (written and approved ISS Policy, with specific roles and procedures) and M11 (full-time IS security officer). Therefore we draw the conclusion that there are two distinct typologies of ISS measures: the first are the very basic ISS measures, coexisting in most of the investigated public organizations; the second are the remaining ISS measures, including as a subtypology the most "advanced" ones.

Table VII
Normalized squared Euclidean distances (NSEDs) between the ISS measures M1-M14

	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14
M1	0.00	0.37	0.28	0.21	0.28	0.42	0.51	0.33	0.33	0.47	0.30	0.33	0.42	0.35
M2	0.37	0.00	0.47	0.44	0.42	0.28	0.42	0.47	0.42	0.37	0.44	0.51	0.47	0.40
M3	0.28	0.47	0.00	0.40	0.42	0.56	0.33	0.37	0.47	0.51	0.49	0.37	0.47	0.49
M4	0.21	0.44	0.40	0.00	0.16	0.40	0.67	0.21	0.26	0.35	0.19	0.30	0.21	0.28
M5	0.28	0.42	0.42	0.16	0.00	0.37	0.70	0.23	0.33	0.37	0.26	0.33	0.28	0.26
M6	0.42	0.28	0.56	0.40	0.37	0.00	0.42	0.42	0.37	0.37	0.35	0.47	0.47	0.44
M7	0.51	0.42	0.33	0.67	0.70	0.42	0.00	0.60	0.56	0.56	0.58	0.51	0.60	0.53
M8	0.33	0.47	0.37	0.21	0.23	0.42	0.60	0.00	0.37	0.42	0.26	0.28	0.33	0.35
M9	0.33	0.42	0.47	0.26	0.33	0.37	0.56	0.37	0.00	0.28	0.30	0.23	0.37	0.40
M10	0.47	0.37	0.51	0.35	0.37	0.37	0.56	0.42	0.28	0.00	0.35	0.42	0.37	0.40
M11	0.30	0.44	0.49	0.19	0.26	0.35	0.58	0.26	0.30	0.35	0.00	0.30	0.30	0.33
M12	0.33	0.51	0.37	0.30	0.33	0.47	0.51	0.28	0.23	0.42	0.30	0.00	0.33	0.40
M13	0.42	0.47	0.47	0.21	0.28	0.47	0.60	0.33	0.37	0.37	0.30	0.33	0.00	0.35
M14	0.35	0.40	0.49	0.28	0.26	0.44	0.53	0.35	0.40	0.40	0.33	0.40	0.35	0.00

Association between the application of basic ISS measures and the context factors

In order to examine the association between the application of the above basic ISS measures and the context factors, we performed analysis of the variance (ANOVA) of the ISSEI. Seven separate One-way ANOVAs of the ISSEI were performed, versus each of the seven context factors C1-C7; each of these seven ANOVAs had as factor one of these context factors in order to examine whether different levels of this context factor result to statistically significant differences in the mean of ISSEI. For each of these ANOVAs the final significance of the *F*-ratio is shown in Table VIII.

For all ANOVAs the usual 5 per cent level of significance was used. From Table VIII we can see that for the cases of context factors C1, C2 and C3 the *F*-ratio significance (0.001, 0.033 and 0.034 respectively) is lower than the above 5 per cent threshold level of significance, therefore these three context factors have a statistically significant impact on ISSEI. Therefore, we can conclude that the total ISSEI, which quantifies the application of basic ISS measures in an organization, is affected by the number of IS users (C1), the number of the supported functions in the organization by the IS (C2) and the number of staff of the IS unit (C3).

Table VIII
Results of the ANOVA of ISSEI versus context factors C1-C7

Context factor	Significance of the *F*-ratio
C1: Number of IS users	0.001
C2: Supported functions by the IS	0.033
C3: Number of staff of the IS unit	0.034
C4: Hierarchical level of the IS unit	0.132
C5: Incidents of confidentiality violation	0.994
C6: Access to the IS by external users	0.211
C7: Connection to the Internet	0.542

The first two factors, C1 and C2 quantify two different dimensions of IT usage in the organization, namely users and supported functions. Therefore as the IS usage in an organization increases, the IS assets, threats, threat agents and therefore the ISS risks also increase, giving rise to the design and application of more ISS measures, in order to face and manage these ISS risks. The third of these internal context factors C3 quantifies the size the IS unit responsible to design and apply ISS measures based on its headcount. Therefore, as the headcount of the IS unit increases, the available person-hours for designing and implementing the required ISS measures also increase, allowing more ISS measures to be designed and applied. On the contrary, IS unit understaffing, which is a usual problem in the public sector (Tsouma 1997), results in giving the main priority to the operation of the existing IS or to the development of necessary new ISs, and much lower priority to the design and application of ISS measures.

We also examined the association between each of the above 14 basic ISS measures separately and each of the seven context factors. For this purpose the corresponding 98 ($= 14 \times 7$) X^2 Independence Tests were performed. For cases of tests, where the validity requirement of the X^2 Independence Test (at least 80 per cent of the cells should have expected frequencies greater than or equal to five) was not fulfilled, a merging of categories was done. The associations discovered from these tests between individual ISS measures and context factors are shown in Table IX, with the symbol (+) in the corresponding cells.

Table IX
Associations between ISS measures and context factors

	C1	C2	C3	C4	C5	C6	C7
M1			+				
M2							
M3			+	+			
M4		+					
M5	+	+	+	+			
M6			+			+	
M7		+					
M8							
M9	+		+				
M10	+	+					+
M11	+	+	+				
M12							
M13							
M14	+						

From Table IX we can also see that the design and application of a written and approved ISS policy with specific roles and procedures (ISS measure M5) is associated with the number of IS users (C1), the number of functions in the organization supported by the IS (C2), the number of staff of the IS unit (C3), and the hierarchical level of the IS unit (C4), i.e. with all the investigated internal context factors. We can also see that having a full-time IS security officer (ISS measure M11) is associated with some internal context factors: the number of IS users (C1), the number of the supported functions in the organization by the IS (C2), and the number of staff of the IS Unit (C3).

Conclusions

From the above investigation we conlude that Greek public sector organizations have only a basic level of ISS awareness and adopt mostly basic ISS measures, such as back-up copies, recovery procedures, security zones, and firewall systems. Most of them have a special interest in digital data confidentiality, probably because the ISs of many public sector organizations contain personal and sensitive data. However, only a small percentage of them have developed a systematic, complete and integrated approach towards the security of their IS, such as an ISS plan and an ISS policy. In addition, only a small percentage of them have established systematic procedures for IS internal audit. The importance of proper training and generally the importance of the human factor for achieving high levels of ISS is often underestimated.

Using cluster analysis two quite different and distinct typologies of public organizations concerning ISS were detected. The first can be described as critical public enterprises, banks, hospitals, social security organizations applying most of the outlined ISS measures, including the more "advanced" ones (written and approved ISS plan, written and approved ISS policy with specific roles and procedures, and full-time IS security officer). The second typology can be described as central and local government organizations, applying only some basic ISS measures, but not the more "advanced" ones. Also using cluster analysis two distinct typologies of ISS measures were detected; the first consists of basic ISS measures (analysis of data confidentiality, security zones at the logical and the physical level, procedures for back-up copies), coexisting in most of the investigated public organizations; the second comprises the remaining ISS measures, including as a significant subtypology the most "advanced" ones.

The application of basic ISS measures, which is quantified by the total ISSEI, varies significantly among the investigated public sector organizations. It is affected by internal context factors, such as the extent of usage of IT in the organization (the number of IS users and the number of the functions supported by the IS) and the size (from the staff number viewpoint) of the IS organizational unit responsible to design and apply ISS measures. Very often due to the prevalent IS unit understaffing the design and application of ISS measures receives lower priority, the main priority being given to the operation of the existing ISS or to the development of necessary new ISS. This tendency also increases due to the distinct nature of ISS: the ISS measures do not quickly yield clearly visible results to the users and the management, similar to the results obtained by the IS development or operation activities (systems up and running delivering useful services to the users, the management, the citizens, and the enterprise).

Given the above results, we can safely conclude that the ISS awareness level and the priority given to ISS have to be raised throughout the public sector. The result should then be a wider application in the real-life information systems of the various technical and organizational measures that have been developed through extensive research and development activity in this area. A critical positive factor towards this direction can be the contribution of the central supervision and coordination ministries (such as the Ministry to the Presidency of Government in Greece) via the central organization of relevant educational

activities such as seminars targeted towards IS and administrative staff, the issue of relevant guidelines and regulations, and the organization of ISS audit activities.

References

Bekkers, V. and Zouridis, S. (1999), "Electronic service delivery in public administration: some trends and issues", *International Review of Administrative Sciences*, Vol. 65 No. 2, pp. 183-95.

Bellamy, C. and Taylor, J.A. (1998), *Governing in the Information Age*, Open University Press, Buckingham.

Commission of the European Communities (1993), *Risk Analysis Methods Database*, DGXIII, INFOSEC Programme/S2014.

Eloff, J.H.P., Labuschagne, L. and Badenhorst, K.P. (1993), "A comparative framework for risk analysis methods", *Computers and Security*, Vol. 12 No. 6, pp. 597-603.

INFOSEC Business Advisory Group (1993), *The IBAG Framework for Commercial IT Security*, Frankfurt, version 2.0.

Loukis, E. and Michalopoulos, N. (1995), "Information technology and organizational structure of the Greek public administration", *International Journal of Public Administration*, Vol. 17 No. 1.

Meyer, K., Schaeffer, S. and Baker, D. (1995), "Addressing threats in World Wide Web technology", in *11th Annual Computer Security Applications Conference*, IEEE Computer Society Press, pp. 123-32.

Oppenheimer, D.L., Wagner, D.A. and Crabb, M.D. (1997), *System Security: A Management Perspective*, Short Topics in System Administration, USENIX Association, Berkeley, CA.

Pfleeger, C. (1996), *Security in Computing*, Prentice-Hall, Englewood Cliffs, NJ.

Spinellis, D., Kokolakis, S. and Gritzalis, S. (1999), "Security requirements, risks, and recommendations for small enterprise and home-office environments", *Information Management and Computer Security*, Vol. 7 No. 3, pp. 121-8.

Swain, J. and White, J. (1992), "Information technology for productivity: may be, maybe not: an assessment", in Holzer, M. (Ed.), *Public Productivity Handbook*, Marcel Dekker, New York, NY, pp. 643-63.

Tsouma, N. (1997), *Study of the Information Technology Actions of the Second Community Support Framework*, Final Thesis National Academy of Public Administration.

Willcocks, L. (1992), "The manager as a technologist", in Willcocks, L. and Harrow, J. (Eds), *Rediscovering Public Services Management*, McGraw-Hill Book Company, Maidenhead, pp. 170-96.

Willcocks, L. and Margetts, H. (1994), "Risk assessment and information systems", *European Journal of Information System*, Vol. 3 No. 2, pp. 127-38.

Wilsher, R.G. and Kurth, H. (1996), "Security assurance in information systems", in Katsikas, S.K. and Gritzalis, D. (Eds), *Information Systems Security: Facing the Information Society of the 21st Century*, Chapman & Hall, London, pp. 74-87.