STATISTICAL COMMISSION and
ECONOMIC COMMISSION FOR EUROPE

Working Paper No. 12
English only

CONFERENCE OF EUROPEAN STATISTICIANS

Joint UNECE/EUROSTAT Work Session on Electronic Data Reporting
(Geneva, Switzerland, 13-15 February 2002)

Topic (ii): Security, confidentiality and privacy issues

INFORMATION SECURITY WITH REGARD TO THE INFORMATION SYSTEMS IN THE GOVERNMENT SECTOR

Submitted by the Central Bureau of Statistics in Israel[1]

Contributed paper

I. INTRODUCTION

1. In Israel's government offices, the Information Technology (IT) Division was in charge of information security until late 1990s. At that time, government procedures were published which required the organization to appoint a special entity that would be in charge of handling information security. In addition, the appointment of a ministerial committee was required. This committee would include the entity in charge of information security, the Deputy Director-General of the respective ministry, and a representative of the IT Division.

2. Accordingly, each government ministry in Israel now includes three entities that handle this area:
   - ?? A unit known as the Information Commission's Office;
   - ?? The Information Security Committee (ISC), which is in charge of approving the overall policy of information security;
   - ?? The IT Division, which also participates in the ISC.

3. In each of the government offices, the relationship between these units is different. Furthermore, the definition and responsibilities vary. In some of the ministries, the ISC's Office is an independent unit; in others, it is part of the security team (facilities and personnel); in others, it is still part of the IT Division.

4. In this document, I will describe the activity regarding security of the IT Division in the CBS and its attitude toward the security entity. I will focus on the points in which they overlap and the points in which they differ. I will also refer to the changing responsibilities in the IT Division for information security over the years. All of these changes were followed by an increased awareness of the importance of information security and the technological tools available.

5. Also I will describe the considerations and the difficulties facing the persons in charge of purchasing information system products, information security products, or products which share both functions in Israel's government ministries.

[1] Prepared by Shifra Har.

II. THE IT DIVISION IN ISRAEL'S GOVERNMENT MINISTRIES AND THE RELATION WITH ISC

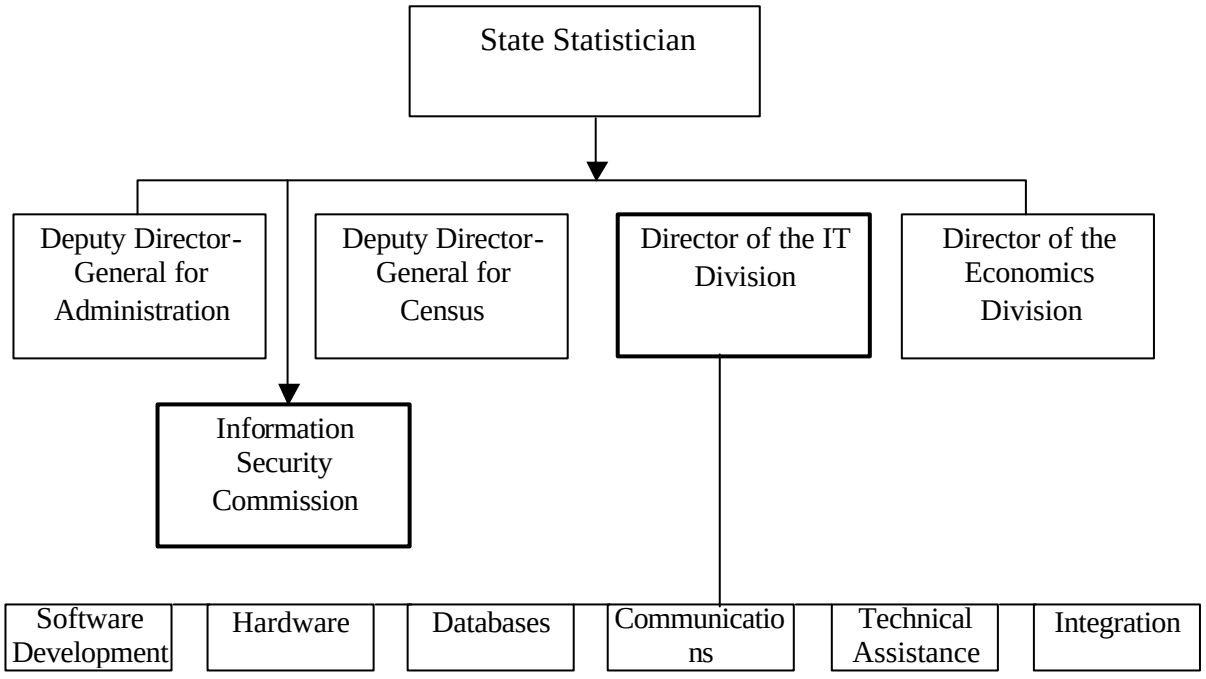
II.1 IT Manager and ISC status in Israel Government

6. In every government ministry in Israel, there is an IT Division. The level of the IT Division Manager within the ministerial hierarchy is not constant: in some ministries, he/she is subordinate to the Director-General of the ministry. In others, he/she constitutes a second echelon, being subordinate to the Deputy Director-General of the ministry; and in some ministries he/she is even in the third echelon. Moreover, in some of the ministries, especially the larger ones, the IT Division Manager serves as a member of the Extended Executive Management. Each of the Division Managers within the ministry is involved in the Extended Executive Management. In addition, there is also a function known as the Restricted Executive Management, in which all of the operative decisions of the organization are reached. Only a few ministries involve the IT Manager in their Restricted Executive Management.

II.2 IT Manager and ISC status in the CBS

7. In the Central Bureau of Statistics, the ISC is directly subordinate to the Director-General. The IT Division Manager is also subordinate directly to the Director-General, and is a member of the Extended Executive Management as well.

Organizational structure of the CBS with reference to the subject of this document (figure 1)



.

8. In 1999 a decision was made to separate the functions of these two entities:
   - ?? The ISC unit is now in charge of the policy of information security;
   - ?? The IT Division is now in charge of implementing that policy;
   - ?? The ISC unit is in charge of supervision to ensure that the implementation is properly carried out.

9. The Information Security Unit in each government ministry, and in CBS as well, does not include organizational employees; rather, it avails itself of the services of outside expert consultants. The IT

includes permanent employees for the performance of the tasks required of it, with regard to both development and ongoing maintenance.

10. The IT Division has several units which handle subjects related to information security. How does this work? The IT Division includes a number of units such as software development, technical assistance, and databases. In each of these units, there are several employees who provide all of the required services in the area, including services required in the field of information security. For example: in the area of software development the employees are in charge of the security activities performed in the framework of the application; in the area of databases, the DBA personnel are in charge of handling database security. As a result, each specialized area in the IT division provides the service required for information security for the framework of the other functions within its sphere of responsibility (see figure 1).

II.3 IT manager and his responsibilities with regard to information security

11. Computerized information systems are becoming more complex. As a result, the information security requirements are growing. Accordingly, the number of experts required within the organization is in direct proportion to both the quantity of technology tools required for IT and the quantity of security tools required for security. As the required security increases, there will be a need for more experts to handle them.

12. However, in contrast to the ISC Unit, which should be aware of what tools exist and their usage, the IT Division needs a deeper understanding of the tools. They require both theoretical knowledge of the tool and its characteristics and an intense practical knowledge and familiarity with its capabilities. In addition they need to study the uses of its functions and to examine the possibility of its integration into the systems existing within the organization. They must also implement it within the organization and be able to maintain it.

13. What are the areas for which the IT Division Manager is responsible (in spite of the existence of ISC)?

- ?? Integrity – ensuring the information will not be lost;
- ?? Assets – day-to-day handling and maintenance of the computers and the UPS;
- ?? Efficiency – correct and efficient use of computer resources in the workplace;
- ?? Availability – ensuring the information is available and the systems are functional;
- ?? Confidentiality – storage of information, use of safes when necessary;
- ?? Survivability.

14. As noted above, the IT Division Manager is actually responsible for all activities performed within the organization with regard to information security. If one of these activities is not carried out properly and a problem arises, it is the IT Division Manager who will be responsible for the outcome. Any malfunction requires intensive work at all levels of the Division; scheduled work is postponed, planned development work comes to a halt, and the reputation of the Division is harmed. It may be clearly stated that the IT Division Manager's interest in all aspects of information security is especially great.

15. The basic assumption is that both units mentioned have a common interest, which is for the good of the organization; neverless, the points of view of the two units are different.

16. The organization has a budget for IT. Of this budget, a certain percentage is directed to the implementation of information security activities (in the CBS, 8% of computer purchase expenses are allocated to information security).

17. The ISC's goal is to attain 100% security, and if this is not possible, to attain the maximum possible level of security. The greater the level of security, the lower the risk of security breaches. By contrast, the IT Division is interested in achieving a balance between security and productive work; it is interested in maximum security, but maybe under certain conditions it will compromise optimum security. After all, information security was invented in order for the work to be done in a secured manner, but if there is no work, there is no need for information security. The IT division should not be suspected of lacking the awareness, the knowledge, or the desire to handle the subject of information security; after all, as stated above, the IT manager is the one who will bear the consequences.

18. The problem becomes more acute when the ISC makes use of the services of consultants from outside the organization. These consultants will constantly strive to attain maximum security, especially because they are not prepared to take risks and are looking for coverage in the event of malfunctions. The management of the organization cannot allow itself to lower the security level, once the security consultants have expressed their opinion. This, in fact, creates pressure, which results in security activities being carried out. I believe that if there had been experts within the organization who considered information security as a means and not as an end, the Information Security Unit might have acted otherwise.

19. It should be noted that I have no intention of criticizing these security consultants. I am certain that they are doing their jobs faithfully, and if I were in their position, I would perhaps also strive to attain maximum security and avoid risks. What I am saying is, there is a need for a functionary specializing in information security within the organization. Such a person would be able to cope with the consultants and give his/her opinion of the risks, analyse the costs and benefits of each of the activities required, and take the responsibility even when the security level is less than 100%. In addition, such a person would be able to provide the ISC with objective data, to enable it to reach decisions.

20. An additional point to note is that the ISC, along with consultants from outside the organization, is also responsible for control of performance of activities. Accordingly, the greater the level of security, the more activities will be performed by the IT Division; this, in turn, will increase the need for control which is given by those consultants.

III. WORK PROCESS REQUIRED WITH REGARD TO INFORMATION SECURITY ACTIVITY

III.1 The process

21. The information security staff are guided by professional considerations to block any possibility of damaged information. With these considerations in mind the process can begin.

21.1 The ISC prepares a general document for discussion by the Information Security Committee with regard to strategy, planning, or handling of an isolated issue.

21.2 The Information Security Committee approves the working paper in principle.

21.3 The ISC submits a document of requirements from the IT Division (hereinafter: referred to as the "Project").

21.4 A representative of the IT Division should act as the coordinator for the managers within the division and SHOULD be responsible for the consideration of the overall significance of the requirement. When the system is new or the technology is new, he/she should enlist an outside consultant, who must be familiar with the technology of the organization. Then, the IT Division representative should submit a document including a detailed list of the activities required in the Division for the implementation of the Project, including the required schedules and costs. The

IT Division should take into account the functionality of the system, the ease of operation, integration with existing systems, and the implications of adding the Project to the networks.

21.5 The document should be put before the Executive Management for discussion and approval.

21.6 Priorities should be determined for implementation of the Project within the planned activity for the IT Division.

21.7 Work schedules should be determined.

21.8 Study, acquisition of know-how and assimilation of the new products/technology should then be implemented.

21.9 The IT Division should perform the activity – with the assistance of outside experts if necessary.

21.10 Ongoing maintenance should be done by the IT Division.

21.11 Supervision and control should be done by ISC.

22. An additional point of conflict in the relationship between the two entities can arise during the preparation of the list of activities required by the organization for implementation of the Project (item 4 above). Within the ISC Office, there is a person whose main role is to write the requirements. In the IT Division, there is no such person whose principal role is to serve as an integrator of all information security activity. This activity is long and complex and requires a great deal of time, because it involves most of the IT units.

23. The conflict may become even more severe as a result of the time required to respond to the Project. Response times are relatively long, because they depend upon many functions within the organization and were not included in the original work schedule of the Division.

IV. CHANGES OCCURING IN THE RESPONSIBILITY FOR INFORMATION SECURITY

24. In the past, the IT Division Manager was in charge of the central computer. The computer was located in a closed room, and every entry and exit to/from that room was written down. There was no physical possibility of removing information, whether as hard copy or on magnetic media (such as tapes), without the knowledge of the persons in charge. In addition, the databases in the central computer were managed by means of central tools that were subject to supervision and control.

25. Today, the computers and printers are distributed throughout the organization. The organizational policy enables any employee to set up his/her own information systems on personal computers by means of user-friendly software. Therefore it has become necessary to address the question of whether the responsibility of the IT Division Manager includes responsibility for the confidentiality of printed material and for the confidentiality of material on magnetic media, as defined in the procedures. Enforcement of this responsibility, and the activity for which the IT Division Manager is responsible can be checked and controlled.

26. An interesting aspect can be raised in such a situation where it must be ascertained that the organization's computers, which are linked by network, are not simultaneously connected to a telephone by means of a modem. Who is responsible for ascertaining this? Logically it seems to be the responsibility of the ISC. However, in CBS, because the ISC does not have employees able to perform these tasks, the IT Division Manager – within the framework of the Technical Assistance Center, which serves the consumers and maintains day-to-day contact with them – initiates these checks whenever the Technical Assistance Center provides service to a user.

27. In addition, ministerial policy enables each employee to act independently and to create his/her own information systems by means of user-friendly tools such as Access. In this state of affairs, the IT Division Manager cannot ascertain how information security operations are implemented within the Project in general and on the databases in particular.

28. In fact, while the responsibility is incumbent upon the IT Division Manager, he/she has neither the capability nor the authority to control and enforce the entire subject of information security within the organization.

29. Above and beyond all of the new computerization tools and the new security resources which are implemented and must be studied, two additional subjects have lately come under the responsibility of the IT Division:

- When the Central Bureau of Statistics moved into a modern building, it was necessary to prepare tenders for products such as UPS and rooms containing fireproof safes for cassettes. These subjects were transferred to the responsibility of the IT Division for preparation of the tenders. These products, however, are not within the area of specialization of the IT Division Manager, but require recourse to electrical and electronics engineers. Nonetheless, in all government ministries, the IT Division is actually responsible for these areas in practice. Even when consultants are employed, the Division must study and monitor the needs and must prepare a framework for the tender. The IT Division Manager is the one who must study and learn the new subjects.
- One new subject which is gradually being adopted by government ministries is voice over IP. This subject requires the IT Division Manager to become involved in the area of telephony, which, up to now, was the responsibility of the administrative units. Technology is transforming the telephone into a computer in all respects, and Israel's government ministries have begun to study and learn this subject, for the purpose of making decisions with regard to future activity, from both the organizational and the technological standpoints.

30. The Central Bureau of Statistics has recently become aware of these needs, on the occasion of the move to the new building and the preparation of the new communications infrastructure, which is shared by telephone and data systems. This has given rise to cooperation between administrative units and computer units for the purpose of maintenance of the new exchanges.

V. PURCHASING OF INFORMATION SECURITY EQUIPMENT

V.1 Laws and procedures

31. The selection of products and services in Israel's government ministries is governed by a series of laws and procedures that are binding for all government institutions. There are two main laws and a large number of procedures which apply to all purchasing activity:

31.1 Public expenditure requires the maintaining of fair contacts. Those involved in this area must be sure to maintain fairness, confidentiality and equal opportunity for all suppliers; this includes non-disclosure of any details with regard to the proposals received.

31.2 The Duty of Tenders Law. This law states that no engagement is to be concluded with an entity that provides a product or service, other than by means of a public tender, which gives any person or entity an equal opportunity to participate therein.

31.3 A public tender is a tender published in the media which includes the conditions required for the purchase of a product, with the possibility of weighting the quality of the product against its price, and where the costing parameters are known and published. There are two basic forms for the preparation of a public tender:

- ?? A tender in which the problem is described and the suppliers are asked to provide a solution.
- ?? A "price list" tender, in which the products are listed and the suppliers are asked to list their prices.

31.4. Procedures which govern the possibilities of purchasing, other than within the framework of the tender. For example, with regard to sums of money less than $4,000, it is necessary to ask three different companies for proposals and to select the least expensive; in the case of a sole supplier – that is, where the product is sold by only one manufacturer – it is possible to approach the Committee and receive an exemption from the duty of tender.

31.5 An additional procedure requires that all computerization purchasing, including information security, must be implemented by the IT Division.

32. The time estimated for the activities required for the implementation of a public tender is about one calendar year. This period includes definition of the requirements, study of the products existing on the market, publication of the tender according to established procedure, examination of the proposals, selection of the winning proposal and signing of the contract.

33. In Israel's Ministry of Finance, tenders are prepared for various products which may be purchased by all government ministries; the main intention of this procedure is to enable reduction of costs for utilization of the advantage of scale. The more items of one product included within the tender, the more sharply the price of the products drops. These tenders are implemented by interministerial committees. In this way, it is possible to shorten processes and facilitate the work of the IT Division with regard to the purchase of a large number of products, such as PCs, passive/active infrastructure, and so forth. The Committee is currently engaged in preparing a public tender for information security products.

V.2 Entities involvment in the purchasing

34. Which entities handle the purchase of equipment/services by means of the information security tender?

34.1 The Information Security Unit, possibly assisted by professional experts from outside the organization, is responsible for preparing tenders that address security-related needs. This requirement may result from a work schedule, or from a change in the computerization array due to the discovery of a security breach, or from the appearance of a new product on the market that is compatible with the organization's needs.

34.2 The IT Division, which is extensively familiar with the information systems, is responsible for ensuring the functionality of the products, examining the products and implementing the purchase.

34.3 The Information Security Committee is responsible for approving the policy of the Project.

34.4 The Ministry controllers are responsible for the expenditures made by the Ministry and must ensure reduction of expenses.

34.5 The Legal Advisor is in charge of preparing the contract with the supplier and ensuring fair and egalitarian handling of all suppliers.

34.6 The ministerial purchasing committees, each of which consists of the controller, the IT Division Manager, and an entity in charge of coordinating the committee are responsible for all of the administrative aspects and for the submission of documents as required.

34.7 The ministerial tenders committee handles only the large tenders. The role of each committee is to re-examine the processes, to ensure that the tenders are written according to procedures and that they are necessary for the respective ministry, and to recheck the state of the budget and determine whether more than one supplier is capable of fulfilling the requirements.

35. Information security products are multi-layer products which handle a large number of areas, and which give rise to challenges in all strata of the information systems. Accordingly, implementation of information security throughout the organization requires the cooperation of a large number of units and entities within the organization, and especially that of the IT Division. After all, the entire subject of information security is intended to provide security solutions for the IT systems throughout the organization. When these two entities work in parallel and perform a proper analysis of needs throughout the lifetime of the Project from planning to integration, and of the significance of Project operation, there is a good chance that the products will be successfully integrated and absorbed.

VI. SUMMARY

36. This document has described the activities required of the IT Division Manager with regard to information security and has pointed out the interfaces between IT and information security, as well as the points of conflict.

37. Policy is set by the Information Security Unit, approved by the Information Security Committee, and implemented in practice by the IT Division.

38. The functions of the IT Division Manager have changed over the years, and especially in recent years, in light of increased awareness of the subject and the technology which is now available to us. These changes have also affected the concept of information systems.

39. In the not-so-distant past, a small group of persons was responsible for handling all aspects of this area; in the 1980s, all that was necessary was a single team which dealt with the totality of these applications – hardware and software alike – with the assistance of communications experts. In the late 1990s, information security experts were added to the development team. The more complex the application and the more extensive security means required, the larger the information security team must be, because each type of tool has its own experts.

40. The result is that every project must expand to include the requisite number of personnel. As a result, the cost of the project increases and the schedule for its implementation is extended.

VII. CONCLUSION

41. The relation between ISC and IT units regarding information security responsibilities is still unbalanced. The goal of both units is the good of the organization but they have different approaches.

42. As noted above, it seems that in addition to the ISC unit we need a sub-unit in the IT Division that will be the contact person with the ISC unit and will manage as an integrator for all the Information Security activities that are undertaken by the IT Division. This unit will also be responsible for giving the ISC the organizational point of view, the risks, analysis and cost benefit of each of the activities required.

REFERENCES

Charles S. Kamen , Control of Statistical disclosure versus needs of data users in Israel, March 2001.