A methodology for managing digital crises using risk analysis and contigency planning – Application for the case of the Y2K Problem in the Greek public sector

E. Loukis
Department of Information and Communication Systems
University of the Aegean
Karlovassi 83200
Samos
Greece
G. Chondrocoukis
Department of Industrial Management
University of Piraeus
80 Karaoli & Dimitriou Str.
18534 Piraeus
Greece

ABSTRACT

Modern private and public organizations make extensive use of digital systems (information systems, electronic systems, etc.), which support significantly their most critical functions. Digital systems can offer important and multidimensional benefits and can contribute highly to organizational efficiency and effectiveness, but at the same time they can create some new threats and risks and can give rise to a new category of 'digital' crises. In this paper a methodology is proposed for managing these digital crises, based on risks identification, quantification and analysis, and also on contigency planning. The proposed methodology is characterized by wide applicability and therefore can be used for all future massive digital crises. This methodology has been successfully applied for managing the Y2K problem in the information and the electronic systems of the Greek public sector.

1. INTRODUCTION

The last decade of our century is characterized by an extensive and continuously increasing penetration and use of digital systems by

Journal of Information & Optimization Sciences
Vol. 21 (2000), No. 3, pp. 369-384
 0252-2667/00 $2.00+.25

private and public organizations, in order to support their most critical functions and increase their efficiency and effectiveness. A lot of important economic activities rely critically on digital systems and generally the whole economic and social life becomes more and more "digital" [(25)]. The most important categories of digital systems used today by organizations are:

(a) Information Systems, for storing, processing and distributing their data

(b) Electronic Systems, for monitoring and controlling critical production and safety equipment.

According to the findings of a research carried out recently by Spectrum ICT ([24]), commissioned by the Department of Trade and Industry (DTI) of the United Kingdom, the percentage of companies using PCs for supporting their functions was 94% in the USA, 100% in Japan and 93% in the United Kingdom. The percentage of companies having PCs with modems, which enable electronic connection to networks and to other companies (e.g. customers, business partners, suppliers, etc.), was 81% in the USA, 76% in Japan and 79% in the United Kingdom. At the same time the percentage of companies having access to the Internet was 68% in the USA, 78% in Japan and 62% in the United Kingdom, while the percentage of companies having their own Web Site was 54% in the USA, 50% in Japan and 51% in the United Kingdom.

The benefits from using digital systems are numerous and multi-dimensional, starting from small or bigger cost reductions and extending up to strategic and competitive advantages ([8], [23], [27]). According to Farbey ([8]) information systems can be classified, based on the main benefits they offer, into the following eight categories:

- Mandatory Systems,
- Automation Systems,
- Direct Value Added Systems,
- Management Information Systems (MIS) & Decision Support Systems (DSS),
- Infrastructure Systems,
- Inter–organizational Systems,
- Strategic Systems,
- Business Transformation Systems.

However digital systems create not only the above benefits, but also some new threats and risks, which under certain circumstances can give rise to a new category of 'digital' crises. A massive interruption of operation or malfunction of one or more categories of digital

systems can create big disruptions and problems to numerous economic and societal activities. Such a digital crisis, if not properly managed, can have quite negative consequences. So far we have already experienced some digital crises, the most important of them being the Y2K problem in the information and electronic systems. Taking into account the continuously increasing penetration and use of digital systems in private and public organizations in most economic and societal activities, such digital crises, or even much bigger ones, may happen in the future. Therefore a methodology is required for managing these digital crises, in order to minimize their negative consequences on the private and public organizations and generally on the whole economic and social life.

In this paper a methodology is described for managing digital crises, based on risks identification, quantification and analysis, and also on contigency planning. Next the application of this methodology is described for the case of the Y2K problem in the information and electronic systems of the Greek public sector. The proposed methodology is characterized by wide applicability and therefore can be used for all future massive digital crises.

2. DIGITAL CRISES

As digital crisis is meant a massive partial or full interruption of operation or malfunction of one or more categories of digital systems, in private and/or public organizations, in one or more economic sectors and/or geographic regions, due to a specific technical defect. In the most difficult cases, in advance (before the manifestation of any interruption of operation or malfunction) we may have only some small indication about a possible technical defect, but no indication at all as to which of our numerous digital systems and which of their numerous components really have this defect.

Such an interruption of operation or malfunction of digital systems may cause significant problems to critical internal functions of the user-organizations relying on them, and therefore have quite negative consequences, such as:

- Lower quality and/or delays in the production process.
- Reductions or even interruption of production.
- Damage to critical organizational assets (e.g. production equipment, building, etc.).
- Safety problems.
- Inability to fulfill contractual obligations to customers, business partners, banks, etc.

- Inability to fulfill obligations to the state authorities (e.g. taxation authorities, social security organizations, etc.).

Also organizations today rely heavily not only on their internal functions, but also on raw materials, products, services, data, information, etc. provided by their external environment, e.g. suppliers, business partners, etc., on the orders placed on them by their customers asking for various products, services, data, information etc. and on critical utility infrastructure services e.g. energy supply, communications, transportations, water supply, etc. Therefore in the case of a digital crisis, all private and public organizations may have additional negative consequences if:

- Their suppliers or business partners, due to interruption of operation or malfunction of their own digital systems, either supply them with lower quantities and quality and/or with significant time delays, or even stop supplying them at all.
- Their customers, due to interruption of operation or malfunction of their own digital systems, reduce or even interrupt their production and respectively reduce or even interrupt their orders.
- The above critical utility infrastructure service providers, due to interruption of operation or malfunction of their own digital systems, either provide their services at lower quantities and quality, or even interrupt their provision.

Finally all citizens and organizations rely to a great extent on some critical government organizations. Therefore, in the case of a digital crisis, interruptions of operation or malfunctions of digital systems of critical government organizations may have severe negative consequences, such as:

- Mistakes, delays or even inabilities, concerning the collection of taxation, the management of public revenue, the welfare and pensions payments, the public expenses management and payment, etc.
- Disruptions in critical areas, such as defense, public order, emergency services, health care, etc.

From the above it is concluded that, because of the increased penetration and use of digital systems, a wide digital crisis may have quite significant negative consequences on core state functions, private and public organizations, citizens, etc. and generally on the whole economic and social life. Also due to the high and continuously increasing interdependencies, both at the national and the international level, the above negative consequences of a digital crisis in a specific economic sector and/or geographic region can rapidly propagate to other

economic sectors and/or geographic regions, and cause them significant negative chain consequences, which then may be further propagated to others, etc. In the case of wide and severe digital crises, even major disruptions might be caused, such as Domino-Effects or global economic recessions, similar to the ones examined in the most pessimistic scenarios of the studies carried out by many banks for the case of the Y2K Problem ([28], [29]).

3. A METHODOLOGY FOR MANAGING DIGITAL CRISES

For all the reasons mentioned in the previous section all private and public organizations require a methodology for managing effectively such wide digital crises, in order to minimize their negative consequences and ensure an acceptable level of functional continuity.

Such a methodology, in order to be useful, should have the following characteristics:

a) Because the digital systems of an organization and their components that might have the specific technical defect, which causes the digital crisis, may be quite numerous, a general methodology of wide applicability should be based on a selective approach. Our attention and our limited resources should be focused on the riskiest digital systems. Therefore a general and effective methodology for managing such crises should be based on risks identification, quantification and analysis.

b) A general methodology of wide applicability should offer the capability of managing all the risks created by a digital crises, not only the internal risks, originating from the interior of the organization, but also the external risks, originating from its external environment (suppliers, business partners, customers, infrastructure, etc.).

c) The methodology should be based on contigency planning for managing the external risks, and on a combination of corrective actions and contigency planning for managing the internal risks.

In the following the proposed general methodology for managing digital crises is described. First are given the basic definitions, followed by a description of the structure and the phases of the methodology.

3.1 *Definitions*

The proposed methodology views each private or public organization as a collection of processes $P1, P2, \ldots, Pn$, performed in order to produce/deliver its products/services. These processes can be divided into primary processes (the ones which are directly part of the produc-

tion/delivery of the product/service of the organization) and support processes (the ones which are required for supporting the primary processes, e.g. procurement of required goods and services, financial management and accounting, human resources management). Each of these processes depends on a number of inputs (Fig. 1), coming both from the external environment (external dependences) and from the interior of the organization (internal dependences).

The most important external dependences (EDs) of a process *Pi*, *EDij* ($i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, ki$) belong to the following categories:

- Customers, suppliers and business partners.
- Infrastructure (e.g. energy, communications, transportation, water supply).
- External IS providing useful data or information (e.g. stock market information).

The most important internal dependences (IDs) of a process *Pi*, *IDij* ($i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, mi$) belong to the following categories:

- Internal digital systems supporting the process.
- Products/services coming from other processes of the organization.

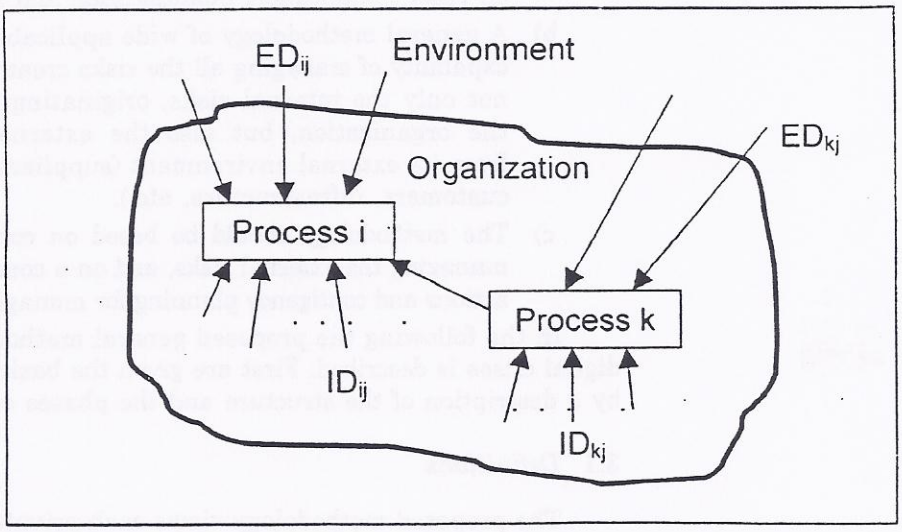

Figure 1. Processes of an organization and their internal and external dependences

Each of these external and internal dependences may fail or have significant disruptions due to interruptions of operation or malfunctions of digital systems, which may be caused by the digital crisis under study. Therefore each of them creates a risk to the process, which is related to the digital crisis.

This risk for external dependences can be calculated with the following formula:

$$R(EDij) = P(EDij) \cdot I(EDij), \quad i = 1, 2, \ldots, n, \quad j = 1, 2, \ldots, ki$$

where

$P(EDij)$ = the probability of failure or significant disruption of the external dependence $EDij$ due to the digital crisis,

$I(EDij)$ = the impact of the above failure or significant disruption of the external dependence $EDij$ on process Pi,

$R(EDij)$ = the risk created to the process Pi by the external dependence $EDij$.

The same formula can be applied for the internal dependences as well:

$$R(IDij) = P(IDij) \cdot I(IDij), \quad i = 1, 2, \ldots, n, \quad j = 1, 2, \ldots, mi.$$

3.2 *Description of the Methodology*

The proposed methodology consists of the following eight phases (Fig. 2):

Phase 1: *Awareness-initiation*

This first phase includes rapid awareness raising in all the hierarchical levels of the organization concerning the digital crisis and its possible negative consequences for the organization, if not properly managed. A special project team must be established, with domain experts, contingency planning and disaster recovery experts and also representatives of the organizational units responsible for the most important processes of the organization and of the IT unit. Also the mission, the objectives, the work plan and the budget of this project are determined.

Phase 2: *Analysis of Basic Processes*

The basic processes of the organization are analysed. For each basic process Pi its main external dependences $EDij$, $j = 1, 2, \ldots, ki$ and its main internal dependences $IDij$, $j = 1, 2, \ldots, mi$ are deter-

Based on $R(Pi)$ and $r(Pi)$, $i = 1, 2, \ldots, n$, the riskiest processes, concerning the specific digital crisis are determined (the ones having the highest R and r). Also from the above analysis the dependences creating the highest risks to the processes of the organization are determined, so that the appropriate level of priority can be given to them.

Finally, all the above can be organized in a risk register, with the basic external and internal dependences and the risks they create to the processes of the organization.

Phase 4: *Contingency Planning for the External Dependences*

In this phase, for each of the riskiest external dependences, contingency plans are developed for the case of its failure or significant disruption due to the digital crisis, in order to minimize the negative consequences and ensure an acceptable level of functional continuity of the process and more generally of the organization. Any existing contigency plan should be taken into account and be exploited to the highest possible extent.

For developing each of these contingency plans the following steps have to be followed:

- Identification of existing alternatives, which can minimize the negative consequences of a failure or significant disruption of the corresponding process and ensure an acceptable level of its functional continuity.
- Assessment of the capabilities, the functionality, the deployment time, the cost and the risks of each of these alternatives.
- Selection of the optimal alternative, based on the above criteria.
- Implementation of the selected alternative (negotiations and contracts with alternative suppliers, customers, infrastructure providers, external IS and generally sources of data and information, procurement of all required equipment, etc.).
- Documentation of the contingency plan and development of its activation plan.
- Training of the personnel involved.
- Testing and validation.

Phase 5: *Correction of Internal Digital Systems*

During this phase, which can be performed in parallel with phase 4, are corrected as many internal digital systems as possible in the

available time, giving priority to the riskiest ones. Special emphasis should be given on testing and validating all digital systems that have undergone corrections.

Phase 6: Contingency Planning for Internal Digital Systems

In parallel with phases 4 and 5, during this phase further contingency plans are developed, for the case of failure or significant disruption due to the digital crisis of significant internal digital systems, which can not be corrected in the available time, in order to minimize the negative consequences and ensure an acceptable level of functional continuity of the process of the organization.

Next, if there is time available, we can proceed to the development of contingency plans for the case of failure or significant disruption due to the digital crisis of the riskiest corrected internal digital systems, for the case that their corrections turn out to be incomplete.

For developing each of these contingency plans, the same steps described in phase 4 have to be followed. The alternatives, which can be considered for the above internal digital systems, are either manual (which usually require more personnel and have lower throughput), or semiautomatic, or even fully automatic (based on independent digital systems of similar functionality).

Phase 7: Activation of Contigency Plans

Immediately after the:

- manifestation of interruption of operation or malfunction of any internal digital system,
- or failure or significant disruption of any external dependence (supplier, business partner, customer, infrastructure, etc.),

the corresponding contigency plan must be activated, according to its activation plan.

Phase 8: Restoration of Normal Operation

After the activation of the above contigency plans, immediate action has to be taken for the restoration of the normal operation as quickly as possible. For this purpose, the internal digital systems, which either do not function or malfunction, are corrected and tested. Also we must cooperate with the organizations responsible for the external dependences, which either failed or had significant disruptions, for their restoration.

Y2K teams were also established within the most important public organizations and private sector associations.

A 'General Guide for Addressing the Y2K Problem' ([16]) was developed and was sent to the whole Greek public sector, followed by a number of specialized Guidelines. One of them was the adaptation of the proposed general methodology for managing digital crises, which was described in section 3, for the special case of the Y2K Problem. Also short training courses were organized by the National Center of Public Administration about this methodology and its practical application.

In September 1999 the managers of the Problem Y2K vertical teams of the most important public organizations were asked to evaluate the above proposed methodology. Nearly all of them agreed on the following :

- The methodology was very useful for developing coherent and integrated business plans for managing the Y2K Problem in their organizations and had short learning curve.
- It contributed very much to adopting an effective and balanced approach in managing the Y2K Problem, focusing not only on their internal IS and ES (which was their initial tendency), but also on the relevant risks originating from their external environment, e.g. the risks associated with energy supply (electricity, fuel, gas, etc.), communications, transportation, water supply, etc. (which had been initially underestimated or even ignored).
- Also the methodology contributed very much to adopting a selective approach in managing the Y2K Problem and focus their limited resources (e.g. financial, human, technical, etc.) and time on the riskiest IS and ES and on the riskiest external dependences. The opposite would be catastrophic, taking into account the limited human and financial resources and the limited time available.

5. CONCLUSIONS

A general methodology for managing digital crises has been developed, based on risks indentification, quantification and analysis and on contigency planning. The methodology includes eight phases : Awareness – Initiation, Analysis of basic processes, Risk analysis, Contigency planning for external dependences, Correction of internal digital systems, Contigency planning for internal digital systems, Activation of contigency plans, Restoration of normal operation. The

proposed general methodology is characterized by wide applicability and therefore can be used for all future digital crises.

The methodology was applied for the case of managing the Y2K Problem in the information and the electronic systems of the Greek public sector. The results were very good, proving the suitability and the capabilities of the methodology for managing difficult and extensive digital crises, concerning numerous digital systems with numerous components and characterized by complex interdependences, having only limited amount of resources available (e.g. financial, human, technical, etc.) and also limited time.

REFERENCES

1. Athens Technology Centre, *Annual Evaluation Report of the Integrated Mediterranean Program on Information Technology*, Athens, 1994.
2. Basle Committee on Banking Supervision, *The Year 2000 – A challenge for financial institutions and bank supervisors*, 1997.
3. Canada Task Force 2000, *A call for action*, available at http://strategis.ic.gc.ca/SSI/yk/eng.pdf, 1998.
4. Canada Task Force 2000, *A call for action: the eleventh hour*, available at http://strategis.ic.gc.ca/SSI/yk/neweng.pdf, 1998.
5. G. Doukidis, *Information Systems in the National Context – The Case of Greece*, Avebury Ashgate Publishing Company, London, 1995.
6. European Commission, *The year 2000 computer problem*, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, COM (1998)102, 1998.
7. European Commission, *The year 2000 computer problem*, Directorate General III, European Commission, 1999.
8. B. Farbey, F. Land and D. Targett, A Taxonomy of Information Systems Applications : The Benefits Evaluation Ladder, *European Journal of Information Systems*, 1995, Vol. 4, pp. 41-50.
9. General Accounting Office of the USA, *Year 2000 computing crisis: potential for widespread disruption calls for strong leadership and partnerships*, US GAO/AIMD-98-85, 1998.
10. ICAP, *The year 2000 problem in the Greek private sector*, ICAP Special Report, Athens, May 1998.
11. Institution of Electrical Engineers (IEE), *The millennium problem in embedded systems*, Available at http://www.iee.org/2000risk, 1999.
12. International Air Transport Association (IATA) *IATA expands year 2000 effort with IATA project 2000*, 1998.
13. E. Loukis and N. Michalopoulos, Information technology and organizational structure of the Greek public administration, *International Journal of Public Administration*, Autumn 1993.
14. N. Loukis and Al. Leventidis, The Y2K Problem in the Information and Communication Systems of the Greek Public Sector, *Administrative Information*, Athens, Autumn 1999. Also publication of the National Press, Athens, August 1998.

15. R. M. Martin, Dealing with dates solutions for the year 2000, *IEEE Computer*, Vol. 30, 1997.
16. Ministry to the Presidency of the Government, *General guide for addressing the Y2K problem*, Athens, 1998.
17. Ministry of National Economy, *Final report of the integrated Mediterranean Program on Information Technology*, Athens, 1994.
18. Ministry to the Presidency of Government, *Program of Administrative Modernization 1993-1995*, 1993.
19. New Zealand Government Administration Committee, *The Y2K inquiry: inquiry into the year 2000 date coding problem*, 1998.
20. OECD (1998a), *The year 2000 problem: impacts and actions*, Organization for Economic Cooperation and Development.
21. Office of Management and Budget of the USA, *Progress on year 2000 conversion: 5th quarterly report*, 1998.
22. PA Consulting Group, *Defusing the millennium bomb: the embedded software threat – A survey of UK awareness and readiness*, 1998.
23. R. Sabherwal and P. Tsoumpas, The Development of Strategic Information Systems : Some Case Studies and Research Proposals, *European Journal of Information Systems*, 1993, Vol. 2, pp. 249-259.
24. Spectrum ICT, *Moving into the Information Age 1999 – International Benchmarking Study*, 1999.
25. P. Tapscott, *The Digital Economy*, Mc-Graw Hill, USA, 1996.
26. N. Tsouma, *A study of the information technology actions of the second community support framework*, Final Degree Project, National Academy of Public Administration, Athens, 1997.
27. I. Ward, P. Taylor and P. Bond, Evaluation and Realisation of IS/IT Benefits : An Empirical Study of Current Practice, *European Journal of Information Systems*, 1996, Vol. 4, pp. 240-259.
28. ED. Yardeni, *Year 2000 recession*, Deutsche Bank Research, 1998a, also available at http://www.yardeni. com/y2kbook.htm.
29. Ed. Yardeni, *The Y2K reporter*, Deutsche Bank Research, 1998b, available at http://www.yardeni.com/y2kreporter.html.

Received November, 1999