ZRÍNYI MIKLÓS NATIONAL DEFENSE UNIVERSITY
FACULTY OF MILITARY SCIENCE

PH.D. THESIS

Dr. József Beinschróth

Questions of information systems supported operation continuity in the defense sphere

A short summary of the thesis

2007.

Introduction

Generally known and accepted, that the operation of civil and defense sphere organisations became dependent on their applied information systems during the huge evolution of information in the last decades. Their available information systems and these correct and sufficient operation decisively affect the maintenance and operation continuity of their own operation processes.

Although, it may as well occur some operation processes and methods which do not have any information support systems, and it is getting more and more generally that the operation processes based on different operations of information systems, consequently the computers, networks, and communicaton systems become increasingly mission-critical systems.

Well-known, the information systems are playing critical part in the operation of organisations apparent that the first aim of these organisations is not the safe operation of their information systems but rather the continuity of operation of their operation processes (first of all their critical processes) without break of continuity consequently the high standard of operation of information systems is not an aim but just a necessary condition. Accordingly, operation of the technolgy does not guarantee - by all means - operation continuity of processes supported by IT systems, that is the operation continuity has further organisational, regulational, human etc. conditions. At this point this is apparent that the operation continuity is not negotiable exclusively as a technological question it will be needed a complex approach which is able to take in account the technological, organisational, regulational and other source of disasters (threats) alike, and proceeding from this it defines their risk factors as well as the applicable defence methods against them.

Because it may not be such defence method in practice which is able to protect the operation processes without break of continuity during different events (For instance: wide heavy natural disasters, terrorist attacks etc.), so we have to count the preparation for disaster situations into the problems of operation continuity.

Aims of my research

1. Working-out of the basic concept of operation continuity, composition of its approach and sum up their functions into a system that way the standard laws of operation continuity can be discussed by its systematized functions.
2. Analysis of standards relative to information security and information systems-based operations in such a way that as a result can be chosen from them those, which can be relevant in point of the operation continuity in the defense sphere.
3. Analysis of disasters and contingencies which endanger operation continuity and the definition of protection parts of operation continuity.
4. Development of final concept of qualification system relative to operation continuity.

Assimilation of the thesis and my applied research methods

The dissertation was created as many years achievement of research working, connecting to the thesis I made several publications which were appeared in different science newspapers.

During the work I could assimilate and analyise relevant literature (technolgical, law, regulational, control-management books, documents, notes, studies, and standards) on the area of operation continuity and on other specialities.

My research was published as different forms of media and can be found as printed form or electronical on the Internet.

I collected the literature - relative to this theme – with the help of Internet and use of printed articles and conference materials (sources).

In point of the usage of research methods I tried to create formal and science unit of the dissertation, and the logical superimposition of chapters.

Ordinary and unusual research methods (analysis, syntesis, induction, deduction) were applied during the whole research process.

Those practical observations were built into the dissertation, which I had collected during works (projects of information and information security and operation continuity) at different organisations as an international certified information specialist (I have CISA and ITIL certifications).

Experiences were also built into the dissertation which I had gained as a professor during lectures for postgraduate MBA course (Information security - business continuity) at Corvinus University of Budapest and for course (Data and information protection) at Budapest Tech Kandó Kálmán Faculty of Electrical Engineering**.**

According to the interdiscipline feature and style of the research work, consultations and shared results with professionals working on same and connecting research and science sections have been played important part during the whole work.

Overview of the structure of the thesis

The main structure of the thesis follows the ambitions, it is divided into four parts (chapters) and all of them are connected to one research aim.

The first chapter was written conception, explanation, meaning of the operation continuity and unites base ideas and base principles, which can be found in relevant literature, furthermore it contains an analysis which can explain that in many viewpoints defense and civil sphere can mean different challenges to the protection of operation conitinuity, and it is extremely typical in operation-oriented process works and systems than normal and everyday routinish activities.

The chapter also sum up that operation continuity can overlap other different science specialities and can connect to them.

It systematizes features of operation continuity so that according to the established system laws and conventions of operation continuity can be discussed in relatively easy way.

The second chapter contains well-known and widespread used analysis and comparison of recommendations connecting to mainly information security and information system operation, furthermore it is focusing on the base aims of them and how are they worked relevant in operation continuity questions, and how are they used and applicable in the defense sphere.

The analysis – first of all because of size limits – does not sum up all complex components of information security, it concentrates mainly the marked recommendations.

The third chapter negotiates the protection of operation continuity and its main components including situation report, contingencies (disasters), risk management, assigment of defense processes, preparation for operation continuity, testing, actualization and topics of controlling in disaster situations furthermore it investigates that protection of operation continuity can cause same problems in the defense and civil sphere, the normal „every-day" life, and in operation-oriented working processes.

However it does not contain – first of all because of size limits – detailed discussion of defense actions (concretes technological solutions) used against different threathens.

The fourth chapter reviews that an index number system relative to actual condition of operation continuity should contain different requirements.

Consequently it makes a proposal to establish a qualification system which is suitable to describe the actual level of operation continuity inside an organization, furthermore it allows of different organizations, corps to compare their levels of operation continuity and follow up of temporal change of operation continuity, and to formulate objective aims.

New science results

1. Establishment of base conception of operation continuity, definition of its approach, systematization of its feautres.

   The system allows of discuss and demonstrate the operation continuity in easy way, including the base fundamentals of it (controlling information sources, organizational and controlling questions, and handling disaster situations) and with an apropriate alignment the particular contingencies.

   An important function of the system is that it can be useful in the defense and civil sphere alike, consequently on critical infrastructure protection sphere and in the normal continous or operation-oriented activities.

2. Verification of reccomendations relative to information security and information systems operation in the defense sphere.

   During the systematization and analization of recommendations connecting to operation continuity problems it has been recorded that such recommendation - which focuses just on operation continuity – does not exist, however there are some of them which contain at least such normatives which can be relevant in operation continuity questions.

   In the thesis it has been turned out that relevant recommendations can be used in the defense and civil sphere alike, and on the critical infrastructure sphere furthermore can not be established differencies for their applicability in practice.

3. Summary and establishment of main components of protection of the operation continuity

   The main components allow of the protection of operation continuity and mark out practical steps for the plan relative to protection of operation continuity.

   Furthermore it has been proven – except for small diferrencies – that the protection of operation continuity causes same problems int he defense and civil sphere, consequently on the critical infrastrucutre defense sphere too.

4. Establishment of concept of index number system which describes the level of

operation continuity.

This index number system can be graphically represented and it is suitable that by the help of it we can describe the actual level of operation continuity in an organization independently that the action (work) is being operating on the defense, civil or critical infrastructure spheres.

The index number system contains all criteria of several levels, it has been worked out for normal everyday continous operation, and for operation-oriented action too.

Recommendations, practical use

1. The thesis contains the base concept and the systematization of main features of operation continuity, it systematizes and standardizes the base ideas and principles connecting to operation continuity which can be found in the relevant literature, consequently it can be utilized for educational themes as a main document.
2. The thesis reviews and evaluates the recommendations relative to information security and information systems operation and this way it supports that the different regulations which determine the operation of several organizations can be suitable for relevant recommendations so indirectly it can help for the different organizations to operate more effective.
3. The thesis records that steps, which are important, and the different organizations have to do and accept these towards the establishment of operation continuity, and it can be served as a base document for them to work out concrete operation continuity plans.
4. And finaly the thesis contains an index number system, which is applied for to describe and typify the established level of operation continuity. With this it supports comparisons of level of operation continuity in different organizations furthermore the follow up of temporal change of operation continuity, and to formulate and record objective aims relative to operation continuity.

Publications releated to research area

1. Beinschróth József: A működésfolytonosság modelljei, kutatói szemináriumi tanulmány, ZMNE, 2005.
2. Beinschróth József: A működésfolytonosság kérdése az informatikai biztonságra vonatkozó ajánlásokban, Kard és Toll, 2005/1.
3. Beinschróth József: A működésfolytonosság kérdése az informatikai rendszerek üzemeltetésére vonatkozó ajánlásokban, Nemzetvédelmi Egyetemi Közlemények, 2005. IX évf. 2. sz.
4. Munk Sándor – Beinschróth József: Informatikai rendszerek működésfolytonossági kérdéseinek sajátosságai művelet-orientált környezetben, Bolyai Szemle, 2006. IV. sz.
5. Beinschróth – Lukács: Informatikai biztonság menedzselése egy magyar középvállalatnál, Kandó Konferencia 2006.
6. Beinschróth József: A működésfolytonosságot fenyegető veszélyforrások, Nemzetvédelmi Egyetemi Közlemények 2006. X évf. 1. sz.
7. Jozsef Beinschroth: Physical and Environmental Security, KANDO CONFERENCE 2006, XXIIIth SCIENTIFIC SESSION, 2006. ISBN 963 7154 42 6
8. Beinschróth József: Informatikai rendszerekkel támogatott folyamatok működésfolytonosságának modellezése és mérése, Hadmérnök, 2006. IV. szám
9. Beinschróth József: Működésfolytonossági és katasztrófa tervek koncepcionális kérdései, Vészhelyzeti kommunikáció - tudományos konferencia, Budapesti Műszaki Főiskola, Kandó Kálmán Villamosmérnöki Kar, 2007. ISBN 978-963-7154-57-7

Budapest, 31. 10. 2007.

Dr. József Beinschróth