komunikácie COMMUNICATIONS

Roman Jašek *

THE INFORMATION SECURITY OF ENTERPRISES AND CITIZENS' SECURITY CONTEXT

The aim of the article to show the analogical procedures encountered while dealing with the security of a company or personal security. Security of Information Systems relates closely to modern-day life and the solution of crisis situations is but one part. It does not matter whether the reason of the crisis is the human factor (purposely or unpremeditated) or even a technical failure. All systems must be able to switch to reserves within real time in order to ensure process continuity. While this article is about systems in the economic (financial) field, the same rules apply in government crisis management at any level. Consequently, the rule of Crisis Management in contemporary society is essential.

Introduction

When resolving questions regarding information security, we encounter many approaches which we, with all sense of gravity, perceive as parallels in the domain of Crisis Management and the citizens' security. In every case, the aim is always a question of protecting something – anything that makes sense to protect and which can be considered to be threatened in some way (e.g. unauthorised access to a database, manipulations of data, assumed identities, misuse of communications possibilities of networks for illegal activities, etc., ... and ending with terrorism).

From the view above, it is therefore possible to say that information security is a specific case of citizens' security oriented on the protection of tangible and intangible commodities. The resolution of such a conception of the problems and issues involved in information is, therefore, highly important and beneficial for society at large.

Security management activities under unusual circumstances

One of the first tasks of security management is to establish how the security situation will be classified as a security incident as well as how it should be resolved. Simply put, it is necessary to establish the borders defining when the problem will be the concern of the security specialist in conjunction with the Managing Director and which situations should be resolved at the consultant and specialist levels.

The resolution of grave security incidents classified as catastrophes and accidents are usually resolved in specially-prepared documents (i.e. crisis plans or contingency measures based on the same) [4] [5].

In Security Policies, the category of security incident and the duties of each employee must be clearly set out, as follows:

- Proactively circumventing the security incident.
- To act in a decisive manner and in compliance with the instructions of the security management personnel in the discovery and liquidation of consequences of security incidents at all three levels of the security system[2)].
- To directly inform each and every breach of the security policy to the appropriate security management system employee.
- The security policies or regulations based upon them shall be openly publicised by the person in charge of third-level security management issues in each workplace (department, office, organisational structure unit, etc).

In case of an incident arising, the security management team should proceed in line with the following schema:

- The employee who discovers the security incident must immediately inform the employees of the second and third security management levels.
- This should be in writing (or verbally while ensuring a written record) in one's own special log and the immediate securing of the place (or technical equipment), where the security incident occurred. This announcement is classified as a *Confidential* Document.
- If a third-level security management employee has been informed – the facts regarding the discovery must be passed on as quickly as possible to a second-level security management employee – into whose competence this security incident falls.
- This second-level security management employee must ensure a complete security analysis of the incident and establish the

* **Roman Jašek**
Deptartment of Informatics and Statistics, Faculty of Management and Economics, Mostní 5139, 76001 Zlín, Czech Republic,
E-mail: jasek@fame.utb.cz, Tel : +420 576 037 436

[2)] The first level is represented by the position of Head of Security, who is directly subordinate to the Managing Director himself. The second level represents the position of security specialists for: administration, personnel issues, technical and plant and machinery issues, information (data) and cryptographic security. The third-level (down) represents the relevant position of the security consultants (their role resides in the collection of information and consultations in normal operational activities).

direct measures undertaken to resolve the issue. If the measure(s) exceed their powers and competencies, they must inform the first-level security management employee (the Head of Security) about this event as soon as possible, who will ensure the taking of adequate measures.
- Second-level security management employees should pass on a summary of information about security incidents to the chief security managers at proscribed intervals (e.g. once every three months) for their operational and strategic importance.
- Each and every employee should have the right to contact and confide in a security management team employee at the level of their choice if they suspect that there is a threat to the security of the information they deal with.

Crisis situation management plans

Security, like a coin, has two sides – the protection of information and its accessibility; and the mastery of exceptional situations – this is precisely to be found in the preservation of its accessibility – therefore, not only "fences" and passwords but also back-ups onto storage disks; planning; etc. The mastery of *Exceptional Circumstances (EC)* therefore may only be successful where it respects to the letter the important elements of crisis management, i.e. overall security policies, and especially – *Systemic Systems Security Policies*[3] (SSSP). Without the below-mentioned documents, it is only possible to master an EC in the sense of generally-applicable principles and bearing in mind the specific procedures prevailing in differing organisations [1] [6].

The resolution of exceptional circumstances (events) is usually reflected in three basic key documents, which are hierarchically linked together. In the first instance, we must interest ourselves in how to manage the security aspects of business life. Then, we must plan ways in which we can remain under our specific conditions as long and as effectively as possible. And finally, we must know how to survive even the most unfavourable of circumstances that we could possibly meet. Sometimes, the following terminology is used:

- *Business Continuity Management* (*BCM* – Management of the unbroken continuity of a business' commercial activities).
- *Business Continuity Plan* (*BCP* – Planning for uninterrupted continuity in business operations).
- *Disaster Recovery Plan* (*DRP* – Planning for remedial activities for situations occurring under exceptional circumstances).

The above-mentioned documents provide a starting-point at the level of the organisation as a whole, and define the critical production domains, determine procedures and ensure their compliance in the event of occurrences of exceptional circumstances; and set out in detail the resolution of critical and exceptional circumstances in the form of concrete approaches and procedures. When designing a manual for the mastery of EC, it is necessary to take the following basic stages in the resolution of exceptional circumstances into account:

Normal operations prior to the occurrence of an exceptional circumstance:
1. *Reactions to an exceptional circumstance.*
2. *The renewal of basic functions after an exceptional circumstance.*
3. *Interim operations.*
4. *Restoring full services and operations.*
5. *Normal operations after renewal of full services and operations functions.*
6. *Normal operations prior to the occurrence of an exceptional circumstance.*

During normal operations, we must gradually create and fulfil conditions that enable execution of crisis plans – whether in "normal" (main) or reserve facilities with Main Spaces and Resources (MSRF) or of Reserve Spaces and Resources and Equipment (RSREF).

These mainly are:
- Data and programme back-up and storage.
- Contracted Guaranteed (Technical) Support.
- Reserve and back-up space and their repairs and maintenance.
- Archive documents and media.

Obviously, in such a sense the RSREF must provide not only for the fulfilment of the third point above (i.e. reserve and back-up space and repairs and maintenance), but also the following point, i.e. the unbroken continuity of the archiving of documents and media [2] [3] [8].

Reactions to an exceptional circumstance

Exceptional circumstances do not only cover fires or local flooding, but also destructions caused by explosions, industrial influences, sabotage, premeditated or unpremeditated damages, etc. In reality however, the site is not usually guarded by sentries and only the ingress points from public domain external sources are subjected to scrutiny – otherwise, the compound is only guarded when patrol cars pass by or personnel within the compound patrol on foot[4], and a time-delayed sabotage act for instance could create wide ranging damage at a time when the attacker is long gone. It is perfectly possible to carry some form of destructive materials into the building and to place them precisely where they can do the greatest degree of harm and destruction, and this can be carried off without attracting any special attention whatsoever.

Immediate activities undertaken by individuals and technical equipment in response to the occurrence of an exceptional circumstance are, for instance, the reactions of:
- A person directly impacted by the situation.

[3] Sometimes also called the Information Systems Security Policy (ISSP).
[4] Here, we are thinking of normal (floor) space, i.e. not fitted with any form of industrial tracking technical equipment.

- A top-echelon employee (Management).
- An IT employee.
- Technical equipment.

From the RSREF point of view, the reaction of the IT employees is important in connection with the reaction of users directly affected by the event and especially in reaction to events of a technical character. Activities undertaken immediately after the occurrence of an EC directly influence further approaches to the resolution of the crisis state. For example, after the intervention of the Fire Brigade, it is unlikely that production machinery and equipment or production media operations will recommence within a period of less than 12 hours, and it is necessary to take this fact into consideration when planning alternative activities.

A component of the transformation process is the transport and installation of larger quantities of materials, which not only require the construction of external access roads with sufficient load-bearing capacities, but additionally, sufficiently suitably-dimensioned passageways and corridors. This issue is inseparably interconnected with the implementation of the DRP itself to an emergency stand-by state, i.e. equipping oneself with appropriate technological equipment, furniture, etc.

Renewal of basic functions after an Exceptional Circumstance

Renewal of basic functions must include:
- Transition to back-up approaches and procedures (e.g. the manual processing of information), before the basic functions and services in the RSREF are brought on-line.
- Bringing on-line the RSREF (communication-links, activation of alternate power resources and media, etc.).
- Renewal of the basic IS functions of the RSREF.
- Working in the back-up regime.

When mastering an EC, it is important that the transition to the back-up operating regime should reflect as fully as possible the fulfilment of the basic functions and, especially, that their renewal in the back-up sites must be supported by the initiation of the basic state (i.e. at the moment of occurrence of an EC on the BCP) from reserve backup media, etc. Communications must be renewed as soon as possible between the productive departments (i.e. users, production, etc.) and the team which will renew and manage the basic functioning of DRP (Crisis Management Team).

In the first phase, the Crisis Management team must, therefore, be capable of activating not only technical equipment and technical communications paths (e.g. networks, the Internet, etc), but also master Head Office activities on the front lines, acquiring back-up media, their installation and bringing on-line, and especially, those activities that enable a transition back to normal full operational activities in the original locality of the DRP. From this it must be clear that the operations of the RSREF must also be managed as regards the continuous creation of operational back-ups and reserves and their safe storage [11][12].

Interim operations

Interim operations must enable the execution or accessibility of functions that are specified in the BCP and DRP. These are the minimum number of functions that need to be preserved to cover basic activities, i.e. to be able to, at least in part, continue to manufacture and sell.

Frome the above, it is clear that mastery of the EC from this point of view is, lacking the requisite documents (the BCP, DRP, CBP, and SBP), only a generalised concept and is further burdened by a certain degree of subjectivity.

Restoring full services and operations

The restoration of full services and operations is usually the least-considered part of the whole chain. What this means is that, in accord with the BCP and DRP, plans are elaborated and later implemented for the return to the original HPP and the renewal or restoration of full operations after the transition from the RSRPF. This requires above all:
- The execution of previously established technical and organisational measures in line with the BCP and DRP.
- The gradual handover and transfer of tasks (activities).
- Replacement of the materials consumed or destroyed in the course of the RSRPF, and others.

The RSREFP must finish its functions by the renewal or restoration of conditions for the full operation of the HPP and the preparations for the new handover of operations activities subsequent to the EC.

As a function of the RSRPF as a back-up reserve centre, it follows that upon liquidation of the EC, it is not only necessary to support the renewal and restoration of full operations through the handover of documentation and media, but also to assess all of the activities undertaken by the RSRPF. This should be followed by the updating of the CBP, SBP, BCP and DRP action plans, as required [7] [9].

This area is both theoretically and practically demanding and complicated, and one-hundred percent effectiveness of the measures designed for mastery of crisis situations can never be guaranteed. We can only test the plans repeatedly to verify their applicability in practice. The possibility of using the services of specialised companies is an issue – not only will they elaborate the requisite documentation (or eventually, help in their creation), but they will prepare for the conditions in their own environments in order to be able to take-over operations without a hitch using their own technical equipment and thus to reduce any damages incurred as a consequence of the non-functioning of one's own production system [10].

All of this however, requires the construction of a functionally equivalent environment, which is – for the majority of operators of information systems, absolutely uneconomical – and for this

very reason, impossible to put into practice. For these reasons, these specialised companies usually have corresponding environments pre-prepared for a variety of users and thanks to the low probability of a crisis actually occurring, two such systems exist concurrently on the market today. In the case of crisis situations and the crash of these two systems at the same time, there also currently exist contracts between other providers of similar such services, where these assume a portion of the burden of obligation. For the global network, this is not a technical problem. It does however require increased protection of information since data from more than one user can co-exist on one system at the same time, and also, a greater variety of processes will most probably operate on the data with varying degrees of sensitivity. For each and every such "backed-up" system a specific security project is required, to be approved prior to the conclusion of contracts for reserve /back-up operational capacity.

Conclusion – Summary

The security of information systems is closely linked to contemporary life and the resolution of crisis situations forms an integral part of it. It is absolutely all one whether or not the crisis occurs as the consequence or influence of failures of the human factor, premeditated or not, or due to a technical failure. All of the systems must be capable in real-time of immediately switching over to back-up systems and thus to ensure the continuity of operational processes. In this article, we have talked and written about systems with an orientation on economic (financial) areas; nevertheless, the same rules also apply to the elements of state's crisis management teams at whatever level.

The role of crisis management as outlined above is therefore absolutely indispensable in contemporary society for the abovementioned reasons.

References

[1] BENDA, R., BRÁZDILOVÁ, M.: *The Role of Knowledge Management in Increasing the Competitive Abilities of Enterprises (in Czech),* Internet a konkurenceschopnost podniku VI. ročník konference, Zlín, Univerzita Tomáše Bati ve Zlíně, 2004
[2] BRÁZDILOVÁ, M.: *Information Resources for the Needs of Competitive Espionage (in Czech),* In: Internet a konkurenceschopnost podniku, VI. ročník konference, Zlín, Univerzita Tomáše Bati ve Zlíně, 2004
[3] BLAŽEK, V.: *The Continuity of Transformation Processes and the Role of Universities and the Long-term Development Goals of the Police Academy in Bratislava (in Slovak),* In: Policajná teória a prax, Bratislava, 2003.
[4] ČANDÍK, M.: *Site Security II. (in Czech),* Zlín, 2004
[5] HOFREITER, L.: *Security, Security Risks and Threats (in Slovak),* Žilinská univerzita, EDIS-Publishing ŽU, Žilina, 2004
[6] KORZENIOWSKI, L.: *Security Management (in Polish),* Study Programme taught at: Szkola Wyzsza, Przedmioty Specjalizacyjne, European Association for Security, Krakow, 2004
[7] KOZÁK, V., ROSMAN, P. JAŠEK, R.: *Facts about Firms Security in Central of Moravia (in Czech),* Využitie databáz v marketingu, Ekonomická univerzita v Bratislavě, 2004
[8] KOZAK, V., JASEK, R., MELICHAREK, Z., CHERNEL, A.: *Economic Inteligence and Espionage,* In: Edukacja ekologiczna oraz determinanty rozwoju regialnego i bezpieczenstwa biznesu w jednoczacej Europie, Wysza Skola Zarzadzania w Slupsku, Slupsk, 2004
[9] KLÍMEK, P.: *Econometrics (in Czech),* Fakulta managementu a ekonomiky, TBU in Zlín, 2004
[10] ŠIMÁK, L.: *Crisis Management in Public sector Administration (in Slovak),* Žilinská University in Žilině, Fakulta špeciálneho inžinierstva, Žilina, 1998
[11] TOMASZEWSKI, J.: *Economic and Legal Problems in Electronic Trade and Company Competitiveness,* In: Internet a konkurenceschopnost podniku, VI. ročník konference, Zlín, 2005
[12] VOLNÁ, E.: *Neural Networks and Cryptography,* In Book of Abstracts of the Central-European Conference on Cryptology, Tatracrypt '01, Liptovský Ján, Slovakia 2001.