Organization's Business Continuity in Cyberspace

[1]Natalia Miloslavskaya and [2]Svetlana Tolstaya
[1]*National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Russia*
[2]*Bank of Russia, Moscow, Russia*
NGMiloslavskaya@mephi.ru

Abstract
At present the reliable and efficient infrastructure of any organization plays an important role, contributes to the preservation and strengthening of its financial stability and economic development, and at the same time concentrates various risks. New risks are associated with the formation of a modern life environment called cyberspace. In the last decade, the risks of cybersecurity violation have acquired the status systemic risks due to a significant increase in possible consequences from their implementation. To conduct business in cyberspace, it is extremely important to develop solutions that eliminate a contradiction between the inability to avoid modern cyberattacks and strong requirement to quickly restore organization's business processes. The measures implemented to date to minimize the recovery time of the activities of organizations after cybersecurity attacks may not be sufficient. The brief description of a business continuity concept application to cyberspace is given.

Keywords: business continuity, cyberspace, cybersecurity violation risks

1 Introduction

Cyberspace does not exist in any physical form. It emerges from the interaction of people, software, Internet services through technological devices and network connections. It is not geographical in the generally accepted sense of this word, but fully international. In the process of global cyberspace formation, the convergence of military and civil computer technologies is taking place, and new methods and means of active destructive influence on the information infrastructure of potential adversaries are being developed. Their own official cyber armies already exist in the USA, China, Britain, France, Germany, Israel and some other countries (Borodakiy, 2013).

In the last decade, the risks of cybersecurity violation (RCSVs) have acquired the status systemic risks due to a significant increase in possible consequences from their implementation. The main reasons for this trend can be identified as follows: the increasing interconnection and interdependence among participants in cyberspace; the complexity of information infrastructures and the heterogeneity of organizations in terms of functions, structure, organizational and legal forms, as well as the growing role of various technologies in the provision of services and the increasing dependence of the latter on these technologies; the origination of new categories of intruders and the goals they pursue, as a factor

in the emergence of new threats from previously unreviewed sources and vulnerabilities, as well as the increase of complexity, broad focus and diversity of cyberattacks.

In some cases, security controls that are used to ensure physical security are ineffective against cybersecurity threats (CSTs). The measures implemented to date to minimize the recovery time (duration of response) of the activities of organizations may not be sufficient. The extent and duration of the spread of the cyberattacks consequences start to overlap the organization's ability to react and restore, as a result of which it loses its vitality and operational resilience. Thus, to conduct business in cyberspace, it is extremely important to develop solutions that eliminate the currently obvious contradiction between

on the one hand, the inability to avoid the actual cyberattacks carried out by sophisticated attackers with the latest technologies in hands, taking into account the tendency to increase the scale and complexity of these attacks, and

on the other hand, using obsolete strategies and information protection tools (IPTs) based on the response principle rather than anticipating the problem for countering cyberattacks and ensuring the resilience of systems and the ability to quickly restore all their assets (including business processes) at an equally high level.

Thus, the goal of the paper is to provide a framework for discussion of very up-to-date issues of organizations' business continuity in cyberspace that will help the community to converge on terminology and to start this international discussion on how to ensure it in modern conditions.

2 Business Processes

A business processes (BP) refers to a set of one or more time-ordered, logically related and completed types of activities that together support the organization's activities and implement its policies aimed at achieving the set goals (Miloslavskaya, 2014). The organization's activities and the functioning of its systems can be considered as a set of BPs or their parts (components). Each BP performs predefined functions and is aimed at achieving a specific expected result. The actual result of a BP can coincide with the expected, be worse or better than it. All organization's BPs can be divided into four groups. Their content, objectives and results are shown in Table. 1.

Table 1. The groups of organization's BPs

Process name	***Process objectives***	***Process results***	***Process content***
Basic (life cycle processes)	Creation of the main organization's products	The main product and/or semi-finished product for its manufacture for intermediate BPs	Ensuring the business objectives of the organization
Supporting	Ensuring the implementation of basic BPs	Resources and services for the basic BPs	Provision of basic (equipment maintenance, provision of energy resources and production environment, information support, financial support, environmental management, PR activities and public relations, etc.) and other BPs for normal operation
Management processes	Organization's activities management	Activities of the whole organization	Strategic planning, setting goals and establishing policies, providing communication, etc.
Processes of measurement, analysis and improvement	Generation of input data for activities improvement processes	Improvement of all organization' activities	Measurement, analysis and improvement of all activities of the organization

The efficiency (productivity) of a process reflects the ability to achieve the desired results. The effectiveness of a process as an economic category is determined by the results achieved in comparison with the resources used and can be assessed through internal and external control (verification). The possibility of obtaining various results during the BP implementation is influenced by various risks arising from the external and internal organization's environment (Figure 1).

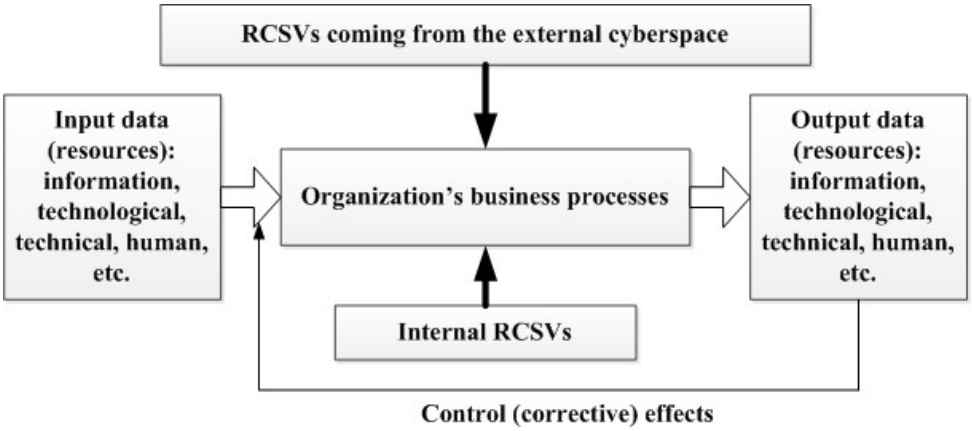

Figure 1: Organization's BPs implemented under RCSVs

3 Business Continuity Concept

The business continuity refers to the strategic and tactical ability of the organization to plan its work in the event of incidents and disruptions of its activities, aimed at ensuring its business operation continuity at an established acceptable level (GOST, 2009). Activity is understood as a process or system of processes performed by an organization with the purpose of producing one or more types of products, providing services or supporting them, while the business operation combines actions (procedures) that constitute the content of one activity operation. These operations are related to the organization's business processes. The term "business continuity" is better suited to organizations, while the term "continuity of functioning" seems more correct for individual systems.

Then the system's functioning continuity (SFC) in cyberspace is the strategic and tactical ability of the planned operation of this system in the event of cybersecurity incidents and the disruption of its functioning in cyberspace, aimed at ensuring the continuity of its processes at an established acceptable level. Logically continuing this definition, we can say that ensuring SFC in cyberspace will be the provision of such a strategic and tactical capability of this system, assuming the long-term its existence in cyberspace. The process of restoring the system's functioning after a cybersecurity incident can be visualized by Fig. 2. One important observation is that an abrupt termination of the implementation of all its processes (as shown in the figure) does not always occur immediately after the incident, since it can cause not only direct but also indirect consequences.

One of the main components of the modern organizations' activities is the information component. In the process of carrying out its activities, the organization is largely susceptible to the impact of various external and internal destructive factors. Therefore, a significant part of the organization's risks, including the risk of business interruption, is associated with information, and the level and conditions for manifesting these risks are largely determined by the quality of IT services (for preparation, processing, transmission, storage and visualization of information) that can be provided using information and communication technology (ICT) readiness.

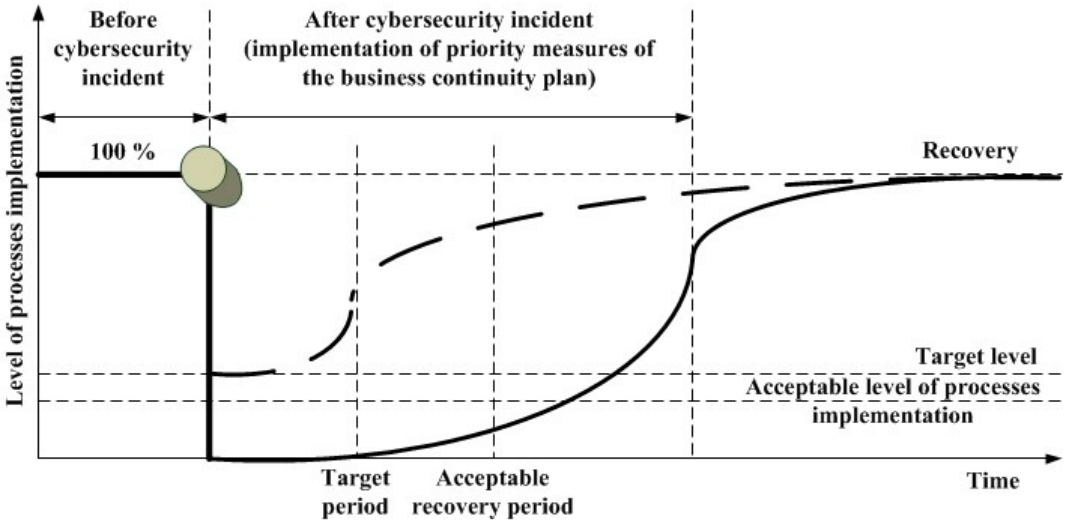

Figure 2: The process of restoring the system's functioning after a cybersecurity incident

In this regard, it is very important to note, repeating the idea of the international standard ISO/IEC 27031:2011 that the effectiveness of ensuring business continuity at the present stage of society development depends heavily on the ICT readiness for achieving the organization's business objectives during various violations and interruptions (ISO/IEC27031, 2011). ICT readiness for SFC manifests itself in the ability to solve five basic tasks:

1) Incident prevention, implying pre-established protection of the required level of availability of ICT services against various threats (for example, hardware failures, operational errors, malicious attacks and natural disasters);
2) Detection of incidents in the early stages, minimizing their impact on ICT services, reducing the effort and resources required for recovery and allowing to maintain the quality of services;
3) Adequate response to the incident, designed to more efficiently recovery and reducing downtime (otherwise the incident could lead to much more serious consequences);
4) Recovery in accordance with the most appropriate in each particular case strategy, which ensures the timely resumption of the operation of systems and services and the integrity of the data; understanding the priorities of recovery allows to first restore the most critical processes and services;
5) Improvement and the ability to avoid incidents in the future by learning lessons from all the events that happened and affected the SFC.

The SFC due to ICT readiness is manifested in its ability to support processes through the prevention, timely detection and response to incidents and restoration of services implemented on the basis of ICT. The ICT SFC as a high availability system is its ability to maintain the reliability of IT resources that ensure the continuity of BPs and the availability of IT services (information) to users, even in the conditions of infrastructure and functional processes degradation, including under the influence of various destabilizing factors. Accessibility means the ability of the ICT system to withstand failures. The level of accessibility is usually measured by "9s", where "five 9s" corresponds to the maximum level. The high availability system, whose availability is 99.999 %, allows only 5 minutes of idle time per year and is designed for the practically uninterrupted delivery of IT services (Figure 3) (as in cancelled PAS 77:2006 IT Service Continuity Management -- Code of Practice).

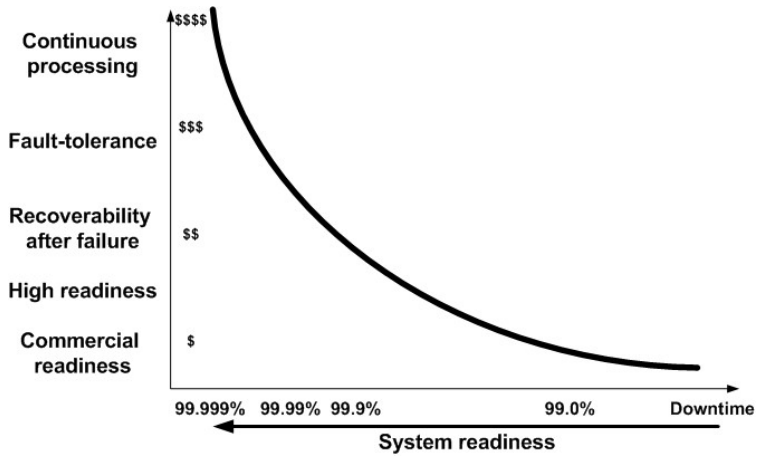

Figure 3: Dependencies of possible downtime on investments in the readiness of ICT systems

4 Business Continuity Management in Cyberspace

ISO/IEC 27031:2011 introduces the concept of business continuity management (BCM) as a holistic management process that identifies potential threats to an organization and the impacts to business operations whose threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities (ISO/IEC27031, 2011). BCM is an integral part of all organizations' activities, enabling them to ensure an almost uninterrupted operation in the event of small and medium-sized emergencies and restore their activities with minimal, pre-calculated losses in the case of large-scale disasters.

In its turn, the SFC management (SFCM) in cyberspace is a holistic system management process that provides identification of potential cybersecurity incidents (cyberattacks) and their impact on the functioning of the system for making informed decisions on the preservation of the system processes. It creates a basis for increasing the system's resilience to the CSTs and is aimed at implementing effective responses against them, that protects the functioning of the system and adds value to its assets (including the provided IT services). In general, the SFCM process implementation in cyberspace can be divided into two main directions (by analogy with (ISO/IEC27002, 2013)): ensuring the functioning resilience of the system and its processes to cybersecurity incidents, as a result of which the likelihood of occurrence of a risk event (RCSV) is reduced, based on the development and implementation of preventive anti-crisis measures, and recovery (continuation) of the functioning of the system, including its processes, individual operations and resources, after cybersecurity incidents, followed by minimization and correction of the negative impact of an incident that has been already occurred.

Thus, the SFCM process in cyberspace as a holistic management process includes, but is not limited to, the following main activities:

- Creation within the organization of a centralized SFCM system (with appropriate strategy), which is coordinated with a top-level BCM system for the entire organization;
- Identification, assessment and ranking according to the various criteria of the RCSVs that the systems can encounter in terms of their likelihood and scale, as well as likelihood of consequences occurrence in the short and long term, including the identification and prioritization of critical BPs;

- Identification of all assets involved in the critical BPs and their values for ensuring SFC;
- Selection of the most reliable ICT, methods and means of information processing, corresponding to the business objectives of the systems;
- Identification and investigation of the possibility of implementing additional (to already existing) controls to prevent and reduce the consequences of cybersecurity incidents;
- Identification of sufficient financial, organizational, technical, human and other resources, taking into account the requirements for ensuring SFC;
- Development of the SFC ensuring plans, as well as the regular updating and testing of these plans and processes implemented/planned for implementation;
- Ensuring the inclusion of the consideration and resolution of SFCM issues in all processes and structure of the systems;
- Compliance with the requirements of legislation, regulations and legal acts, departmental and other documents governing the issues of ensuring SFC in cyberspace;
- Establishing responsibility for the SFCM process within the framework of the systems;
- Development of procedures and formats for the exchange of information concerning the interruption of the systems' functioning.

5 Conclusion

Every organization needs SFCM for all its systems in cyberspace. With effective implementation of SFCM, it contributes to the continuous organization's BCM improvement and ensuring stability in achieving its main business objectives, providing a proven method for restoring the ability of the systems to provide IT services in cyberspace at a specified level within the agreed time after the disruption of activities, and ultimately it protects organization's BPs and reputation. We proposed how to apply a BCM concept to cyberspace, using which we are developing a cyber resilience concept.

6 Acknowledgement

This work was supported by the MEPhI Academic Excellence Project (agreement with the Ministry of Education and Science of the Russian Federation of August 27, 2013, project no. 02.a03.21.0005).

References

Borodakiy, Yu., Dobrodeev, A., Butusov I. (2013). Cybersecurity as the main factor of national and international security of the XXI century (Part 1). Cybersecurity issues. Vol. 1. (In Russian)

GOST R 53647.1-2009 "Business Continuity Management. Practical guidance" (2009). Moscow. Standartinform. (In Russian)

ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity.

ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security management.

Miloslavskaya, N.G., Senatorov, M.Y., Tolstoy, A.I. (2014). "Information Security Management Issues" Series. In 5 volumes. Volume 3: Information Security Incident and Business Continuity Management. Moscow: Goriachaja linia-Telecom. 2014. 2nd edition. 170 p. (In Russian)