Enterprise Continuity Program*

Alexsandr A. Petrenko [1], Sergei A. Petrenko [2] [0000-0003-0644-1731],
Krystina A. Makoveichuk [3] [0000-0003-1258-0463], Alexander A. Olifirov [3] [0000-0002-5288-2725]

[1] Russian Technological University (MIREA), Moscow, Russia
[2] Innopolis University, Kazan, Russia
[3] V.I. Vernadsky Crimean Federal University, Simferopol, Russia
s.petrenko@rambler.ru,
christin2003@yandex.ru

Abstract. Today Business Continuity Management affects almost every one of us. We are just beginning to fight the global coronavirus pandemic (lat. Coronaviridae) COVID-19 infection, which has already claimed tens of thousands of lives, we are experiencing another global economic crisis equal to which has never been before, and we are only starting to understand new global threats such as climate change, energy security, cyberterror, and cybercrime. Major technogeneous accidents and other emergencies in recent years have become the starting point for revising existing Enterprise Continuity Programs and the emergence of a new practice of Cyber Resilience Management for digital economics. However, in the professional literature, the issues of Business Continuity and Cyber Resilience have not been fully considered.

Keywords: ISO, Security, Resilience, Business Continuity Management, Enterprise Continuity Program, COVID-19, Pandemic.

1 Introduction

The beginning of 2020 was marked by an outbreak of extremely dangerous and previously unknown coronavirus (lat. Coronaviridae) COVID-19 infection, which was first reported on 31 December 2019 in Wuhan, Hubei Province, China. In 2019, France and Spain experienced a traffic collapse due to strikes at gas stations and on public transport. In winter 2020, Bulgaria had seriously aggravated transport problems due to heavy snowfall in the north of the Balkan Peninsula. These and other events have once again demonstrated to us how vulnerable we are to such threats and how interconnected today's world is.

It should be noted that company management often mistakenly believes that business continuity management (BCM) processes are too complex for the scale of their businesses. This is a serious misconception — threats to which any organization is exposed are similar, regardless of the scale and type of its activity, differences are manifested only in the available powers, means, and resources that can be allocated to ensure business continuity and, accordingly, to respond quickly to security incidents. It is clear that at small enterprises they are much lower. It should be borne in mind that many assumptions on which traditional risk management (assessment, reduction, transfer, acceptance) are based have certain disadvantages. The fact is that the identification of risks and the assessment of the likelihood of their occurrence are not so important. What matters is the business impact of a security incident, not the likelihood of a security incident. In practice, it is recommended to highlight the following areas of the possible impact of security incidents on business: people, facilities and indoor space, technology, supply chains, customers, liquidity, and reputation [10, 11]. Focusing on the possible consequences of losses in these areas as opposed to a detailed study of each specific risk, allows you to increase the sustainability of the organization, which in its turn leads to improved business efficiency as a whole.

Business Continuity Management, BCM is the only management trend that ensures a high level of protection and sustainability of the enterprise, which is inextricably linked to the issues of security, and management, and communications in emergencies and crises. Many aspects of BCM have always been present in organizations under different names. And now it is important to bring them together in a single structure of the continuity management process to clarify and form a common course on this issue. For example, we follow the recommendations of the well-known international standard ISO 22301:2019 “Security and resilience — Business continuity management systems — Requirements”, as well as recommendations of other known standards ISO 9001 “Quality management systems”, ISO 14001 “Environmental management systems”, ISO 31000 “Risk management”, ISO/IEC 20000-1: Information technology — Service management”, ISO/IEC 27001:2013 “Information security management systems”, ISO 28000 “Specification for security management systems for the supply chain”, recommendations of some national standards ASIS ORM.1-2017, NIST SP800-34, NFPA 1600:2019, and best practices COBIT ®2019, RESILIA 2015, ITIL V4 and MOF 4.0 in part BCM, etc. [1-7, 9].

2 Business Continuity Management

The term Business Continuity Management (BCM) appeared recently and today attracts constant interest from top managers of international companies. Since approximately 1988, several high-tech countries around the world, mainly in the United Kingdom, the United States, Canada, the European Union, Russia, Australia, China, Singapore, and Japan, have held annual hearings and meetings of specially created committees and commissions on Business Continuity Management. Over a dozen different international and national standards and specifications on Business Continuity Management were prepared, including the most famous: ISO 22301:2019 (replaced part 2 of the standard BS 25999 (PAS 56)), ISO/IEC 27001:2013(A. 17), and ISO/IEC 27031:2011, ASIS ORM.1-2017, NIST SP800-34, NFPA 1600:2019, CSA Z1600, AS/NZS 5050 (HB 292), SS540:2009 (TR19:2004), SI 24001:2007, High-Level Principles for Business Continuity (2006), COBIT ®2019, RESILIA 2015, V4 ITIL and MOF 4.0 in the BCM part, etc. For example, the ISO 22301:2019 standard "Security and resilience - Business continuity management systems — Requirements" is intended for certification of BCMS—Business Continuity Management Systems of organizations operating internationally. ISO 22301:2019 is coordinated with other well-known international standards ISO 9001 "Quality management systems", ISO 14001 "Environmental management systems", ISO 31000 "Risk management", ISO/IEC 20000-1 "Information technology-Service management", ISO / IEC 27001:2013 "Information security management systems", ISO 28000 "Specification for security management systems for the supply chain", etc.

Currently, Business Continuity Management is one of the most relevant and dynamically developing areas of strategic and operational management of modern enterprises. The relevance of this trend for each company is explained by the need to ensure the survival and preservation of their business in emergencies. The term Business Continuity Management usually refers to the systematic process of assessing the consequences of emergencies and making appropriate decisions to preserve the company's business. Therefore, the main goal of the relevant Enterprise Continuity Program (ECP) is to minimize the risk of business loss in case of its interruption and to continue the company's activities in emergencies [12, 13].

In some countries, including Russia, the practice of developing and implementing corporate ECP programs is just beginning. One of the best initiatives of the Bank of Russia prepared the corresponding section 8.11 of the STO BR IBBS-1.0-2008, on the grounds of recommendations of ISO/IEC 27001:2005 (A. 14), and then based on the document of the Basel Committee on the Banking supervision (High-Level Principles for Business Continuity) developed Paragraph 3.7 Of the Bank of Russia regulations dated December 16, 2003. N 242-P "On the organization of internal control in credit organizations and banking groups" (updated following the Instruction dated March 5, 2009, No. 2194-U “On amendments to the Regulations of the Bank of Russia dated December 16, 2003, N 242-P“).

At the same time, in Europe and the United States, the implementation and support of these corporate programs are fast-forward, and in some government and commercial structures, Business Continuity Management issues are given the closest attention. For example, US Federal departments carry out business continuity planning following approved Continuity of Operations (COOP) directives. In the financial field, business continuity issues for American companies are regulated by the recommendations of the Gramm-Leach-Bliley and the Expedited Funds Availability laws, as well as the recommendations of the SAS 78/94 standard. In the field of health, the guiding document in the BCM part is HIPAA. Also, for most companies that provide essential services (electricity, water, gas, communications, etc.), certain benefits are provided by the state when using business continuity procedures. The fact is that the continuity of these companies plays an important role in ensuring the continuity of various Federal organizations and structures (hospitals, police, fire departments, schools, and government agencies), as well as large commercial structures (banks, financial organizations, insurance companies, Internet service providers, and so on). In the USA, Canada, and the EU, the most active users of Business Continuity Plans (BCP) are various financial institutions and organizations, enterprises of the raw materials and oil refining industry, airlines, telecommunications companies, etc.

The recent tragic events, such as the terrorist attacks in September 2001 in New York at the World Trade Center, the blackout in North-Eastern USA and South-Eastern Canada in 2003-2009, volcanoes in Guatemala, New Zealand, Indonesia, and Iceland in 2010-2018, natural disasters in India, Philippines and China in 2018, traffic collapses in the European Union in 2019, and finally the pandemic threat of the virus COVID-19 in early 2020 that we have only begun to fight and that has already claimed hundreds of thousands of lives, clearly showed that only those companies that took timely advantage of the recommendations for business continuity were able to avoid major financial losses and maintain their business. The rest of the companies suffered significant financial losses and some even lost their business. Therefore, companies are constantly improving their Business Continuity Plan and its various derivatives: the Business Crash Plan, the Business Disaster Plan, the Anti-terrorist plan, the Anti-bomb plan, the Business Continuity Plan, the Business Recovery Plan, the Anti-crisis plan, and so on [8].

Emergencies occur almost every day, therefore every company probably raises the following questions:

1. What are the legal guidelines and requirements for ensuring business continuity? How should we organize work within this scope?
2. How to create and implement a cost-effective corporate business continuity management program?
3. What kind of BCM solutions or services best meet our company's needs?
4. Should our company itself create and maintain Business Continuity and Recovery Plans, or is it sufficient to enter into an appropriate contract with a consulting company?
5. What tools exist for automating Business Continuity Planning and Management?
6. How to control Business Continuity Management?
7. How to evaluate and manage the costs of support and maintaining an Enterprise Continuity Program?

The answers to these and many other questions will create and implement a truly effective and cost-effective Enterprise Continuity Program (Table 1) and at the same time, make the aforementioned program "transparent" and understandable both for the management and ordinary employees, as well as for business partners and clients of the company.

3 Conclusions

However, the first experience of developing and implementing corporate ECP programs revealed the following problems:

- Many organizations do not have any kind of policies, strategies, plans, or procedures for business continuity and recovery in emergency’s situations;

- Insufficient system development of the subject area, and as a result, the focus on disaster recovery of its services and poor coverage of critical business processes, including services provided to customers and partners;
- The lack of a formal description of business processes with the names of responsible persons and, as a result, difficulties in determining the acceptable recovery time and optimal recovery point;
- Irregular and/or incomplete analysis of external and internal impacts on critically important business processes of the company, which leads to the fact that business continuity plans do not always meet the goals and objectives of the business, not to mention inadequate expenses for business continuity;
- Outdated methods and approaches to business continuity planning and management that are poorly adapted to the requirements of international legislation and relevant regulatory documents of state bodies and regulators;
- Insufficient training of employees of organizations in business continuity management, lack of knowledge, and practical skills in emergencies.

Table 1. Stages of the Enterprise Continuity Program lifecycle.

Stages of the Enterprise Continuity Program lifecycle	Possible outcome
Stage 1: Analysis of business continuity requirements	
Necessary: Analyze the company's critical business processes and supporting infrastructure; Identify and verify current threats and vulnerabilities of business processes; Assess the main risks (RA) of business processes; Assess potential financial losses in the event of an emergency; Conduct a full business impact analysis (BIA) for the company's business units	The results: Methods of assessment and ranking of company critical business processes; Methods of verifying threats and vulnerabilities of company business processes; Methods of risk assessment; RA report with the analysis of risks and priorities, and priority tasks to ensure business continuity; The methodology of damage assessment in case of emergency's situations; BIA report with estimates of company assets and possible damage as a result of the emergency's situations
Stage 2: Business Continuity Planning	
Necessary: Form and approve the BCPM business continuity planning and management group; Develop strategies and continuity plans for each business unit of the company; Identify priority measures to ensure business continuity; Develop alternative solutions	The results: Membership of the Business Continuity Planning and Management Group; Business Continuity Strategies; Business continuity plans for each business unit of the company; List of priority measures to ensure business continuity; List of alternatives and criteria for choosing the optimal solution;

Choose the best solution from the available alternatives; Determine the necessary resources for business continuity planning and management; Form and approve the BCPM business continuity planning and management group.	Official instructions of the company's employees on business continuity provision with the definition of the role, responsibilities, and degree of responsibility of each employee; Formalized requirements for business continuity planning and management; Estimates of the cost of possible solutions for Business Continuity Management; Criteria for selecting BCP solution providers; Extracts from the company budget for business continuity planning and management.
Stage 3: Support and maintenance of the corporate ECP program	
Necessary: Train company employees on business continuity and management issues; Develop regulations for maintaining and supporting business continuity plans, BCP; Purchase the necessary BCP support tools; Install and configure BCP support tools; Develop a notification system for adjustments and changes to the BCP; Develop control tests of the effectiveness of Business Continuity Plans and a schedule of control checks; Develop formal criteria for evaluating BCP audits; Develop a procedure for making changes to the BCP.	Results: Employee certificates in the field of BCM; Methods and guidelines for installing, configuring, and servicing BCP tools; Specifications of BCP support regulations; Annunciation scheme introducing the changes that are being made. BCP testing and verification methods; Formal BCP evaluation criteria for presenting test results; Reports on testing BCP plans; Instructions on how to make changes to the BCP. Guidelines for maintaining and supporting business continuity.

4 Acknowledgment

The author would like to thank Professor Alexander Tormasov (Innopolis University).

The author sincerely thanks Prof. Alexander Lomako and Prof. Igor Sheremet (Russian Foundation for Basic Research, RFBR) for valuable advice and their comments on the manuscript, the elimination of which contributed to improving its quality.

The author would like to thank Prof. Alexander Lomako and Dr. Alexey Markov (Bauman Moscow State Technical University) for the positive review and semantic editing of the monograph.

This work was financially supported by the Russian Foundation for Basic Research Grant (RFBR) and the Government of the Republic of Tatarstan in frames of the scientific research No. 18-47-160011 p_a “Development of an early warning system for

cyber-attacks on the critical infrastructure of enterprises of the Republic of Tatarstan based on the creation and development of new NBIC cybersecurity technologies".

References

1. ISO 22301:2012. Societal security -- Business continuity management systems – Requirements, [Online]. Available: https://www.iso.org/standard/50038.html
2. ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements, ISO 22313:2020 - Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301, [Online]. Available: https://www.iso.org/committee/5259148.html
3. ISO 22313:2012. Societal security -- Business continuity management systems – Guidance, [Online]. Available: https://www.iso.org/standard/50050.html
4. ISO/TS 22317:2015. Societal security -- Business continuity management systems -- Guidelines for business impact analysis (BIA), [Online]. Available: https://www.iso.org/standard/50054.html
5. ISO/TS 22318:2015, Societal security -- Business continuity management systems -- Guidelines for supply chain continuity, [Online]. Available: https://www.iso.org/standard/65336.html
6. ISO/TS 22330:2018, Security and resilience -- Business continuity management systems -- Guidelines for people aspects of business continuity, [Online]. Available: https://www.iso.org/standard/50067.html
7. ISO/TS 22331:2018, Security and resilience -- Business continuity management systems -- Guidelines for business continuity strategy, [Online]. Available: https://www.iso.org/standard/50068.html
8. NIST SP800-34 – Contingency planning guide for information technology, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
9. Olifirov, A.V., Makoveichuk, K.A., Zhytnyy, P.Y., Filimonenkova, T.N., Petrenko, S.A. Models of Processes for Governance of Enterprise IT and Personnel Training for Digital Economy / 2019 Proceedings of 2018 17th Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region, PTES 2018 c. 216-219 DOI: 10.1109/PTES.2018.8604166
10. Petrenko, S., Makoveichuk, K.: (2020) Development of BI-Platforms for Cybersecurity Predictive Analytics. In: Sukhomlin V., Zubareva E. (eds) Convergent Cognitive Information Technologies. Convergent 2018. Communications in Computer and Information Science, vol 1140. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-37436-5_25
11. Petrenko, S., Makoveichuk, K., Olifirov, A.: (2020) New Methods of the Cybersecurity Knowledge Management Analytics. In: Sukhomlin V., Zubareva E. (eds) Convergent Cognitive Information Technologies. Convergent 2018. Communications in Computer and Information Science, vol 1140. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-37436-5_27
12. The Good Practice Guidelines (GPG) 2018 Edition, Business Continuity Institute (BCI), [Online]. Available: www.thebci.org
13. The Professional Practices for Business Continuity Management 2017 Edition, Disaster Recovery Institute International (DRI), [Online]. Available: www.drii.org