On the way to resilient information security management: Business Continuity Management (BCM) for public institutions

Christian SCHACHTNER,
Full Professorship for Business Informatics with focus on Digitalization in the Public Sector, RheinMain University of Applied Science Wiesbaden, Germany
christian.schachtner@hs-rm.de

Abstract
This article refers to Business Continuity Management (BCM) for public institutions in Germany. Objectives: The main objective is to raise awareness of the importance of robust business continuity planning (BCP) in public institutions. It emphasizes how a well-designed BCP can increase an institution's ability to anticipate potential business interruptions, minimize eventual impacts, resume operations, and ensure basic services during unforeseen events such as natural disasters or pandemics. Prior Work: Reference is made to previous studies and practices dealing with BCM in public institutions. Among these, most are limited to theory and do not deal with BCM from a practical point of view. Many institutions are working with conventional BCM practices, even though new technologies and frameworks are opening up new opportunities. Approach: The method presented here focuses on the practice of BCM application in public institutions. Through case studies and interviews with public officials, approaches are demonstrated that maximize the continuity of public service during unexpected events. The article also highlights the importance of new technologies and data-driven approaches for effective BCM. Results: The results show that effective application of BCM enables public institutions to respond quickly and efficiently to emergencies, minimize their impact, and provide recovery services. It is clear that a proactive, technology- and data-driven approach to BCM contributes significantly to its effectiveness. Value: The value of this article lies in emphasizing the practical application of BCM in public institutions and demonstrating how technology can be used to make BCM practices more effective. For public administrators and politicians, this article can serve as a guide for improving their BCPs and ensuring continued public service even in times of unavoidable disruption.

Keywords: business continuity management, data-driven scenarios, management of public innovation.

1. Introduction
Information security is a vital issue for companies of all sizes and industries. However, despite the high risks, executives still do not seem to give this area the importance and resources it deserves.

There are several reasons for this, which have been investigated in various studies.

First, the problem is often due to a misperception of risk. An international study by EY [1]showed that only 56% of executives surveyed consider information security to be a significant risk to their organization. It seems that many decision-makers still underestimate the dangers, even though cyberattacks and data breaches are repeatedly reported in the media.

Second, information security is often seen as a purely IT problem that does not fall within the scope of responsibility of the C-suite. A study by the Ponemon Institute [2] found that 68% of respondents see the responsibility for information security with the IT department and only 22% with the executives. This misunderstanding can lead to the area not being adequately funded and supported.

Another obstacle is the lack of understanding of the complexity of information security. A study by KPMG [3]showed that less than half of business leaders believe they have a sufficient understanding of information security to make effective decisions.

It is also striking that many companies consider the costs of information security to be too high or are not willing to invest in this area. According to the Cybersecurity Insiders Threat Report 2024 [4], 50% of respondents believe that the lack of budget is the biggest challenge to information security in their organization.

After all, the fast-paced evolution of cyber threats, technologies and regulations poses a challenge. Information security requires constant adaptation and training, which requires additional resources and is often considered too burdensome by executives [5].

It is therefore obvious that the awareness and understanding of the importance and complexity of information security at the management level is not sufficient. It is therefore crucial that executives are trained in this area and recognize the added value of effective information security – both to protect the business and to increase business value.

Business continuity management (BCM) is a comprehensive management approach to ensure the continuous operation of a company during and after emergencies or crises. A number of important terms and concepts play a decisive role here.

It is difficult to find an accurate statistical record of the prevalence of business continuity management (BCM) in state institutions and municipalities, as this data is usually not publicly available. However, it is widely believed that the prevalence of BCM in these areas is relatively low. At the same time, various surveys prove reasons for inadequate systemic dissemination of information security mechanisms:

- Lack of awareness and knowledge: According to a study by Rathmell et al. [6], there is a lack of awareness of the importance of information security in local governments. There is often a lack of sufficient knowledge about risks and prevention measures in the field of information systems.
- Scarcity of resources: A study by the Bertelsmann Stiftung [7] clearly showed that municipalities are often under considerable financial pressure. The limited resources often lead to the fact that investments in the field of information security are reduced to a minimum.
- Setting priorities: According to the findings of a study by Kuhlmann et al. [8], information security is often not perceived as a strategic management task in municipal administrations. It is seen more as a technical matter and is therefore usually pushed back in the setting of priorities.

2. International players in information security

The design of specifications in the field of information security is significantly influenced by various working groups and decision-making networks. Due to their expertise and technical knowledge, these institutions are crucial for the development and adaptation of safety standards and regulations.

- ISO/IEC JTC 1/SC 27 Working Group: The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have jointly established a working group called JTC 1/SC 27. This is specifically responsible for standardization in the areas of information security, cybersecurity and privacy protection. The work of this group has a significant influence on international standards such as ISO/IEC 27001 for information security management systems.
- Internet Engineering Task Force (IETF): The IETF is an open international community of network designers, operators, manufacturers, and researchers dedicated to the technical advancement of the Internet. Among other things, this also includes the development and promotion of standards around the security and stability of the Internet.
- European Institute for Standardization (CEN): This international organization develops standards for a wide range of areas, including information security. They play an important role in setting standards that must be met across Europe. It promotes effective measures to protect information systems and develops regulations and standards for information security. It works closely with representatives from business, science and administration to develop these guidelines.
- National Institute of Standards and Technology (NIST): NIST develops and promotes standards and technologies to improve information security. These include guidelines for cybersecurity and privacy protection.
- ENISA: Die European Union Agency for Cybersecurity unterstützt die EU und ihre Mitgliedstaaten beim Schutz ihrer Informationssysteme. Dazu zählen auch die Entwicklung von Richtlinien und Best Practices im Bereich der Informationssicherheit.
- The specifications and standards developed and promoted by these and similar working groups and networks have a significant influence on information security requirements at international, national and internal company level. They define the measures that companies and organizations must take to ensure adequate security of the information processed.

3. Comparative studies according to process models

The scientific survey methodology for the assessment of information security in organizations includes a variety of methods and models. The purpose of these methodologies is to empower organizations to assess and improve their security processes. Here are some of the leading methods used in cross-comparisons.

3.1. Interviews

These are face-to-face conversations with staff that are used to understand the security practices in the company. Interviews can be structured or unstructured and provide information about risk perception, safety culture, and the effectiveness of the security measures used.

3.2. Questionnaires
They are similar to interviews, but they are conducted in writing or electronically. They allow a large amount of data to be collected at once and can be cost-effective and efficient.

3.3. Case studies
Case studies allow for a detailed examination of security practices in a particular organization or context. They can include qualitative data, such as interviews, document analysis, and observations, as well as quantitative data, such as surveys or statistical analysis.

3.4. Document analysis
This involves reading through reports, policies, and other relevant documents to understand the organization's security practices and identify potential vulnerabilities.

3.5. Observations
Observations can be conducted both formally and informally. They can provide information about employees' work practices and behavior that may not be disclosed in interviews or surveys.

Some of the process models for information security are exemplary in relation to international requirements for large organizations:

- ISO/IEC 27001: ISO/IEC 27001 is an internationally recognized standard for information security management systems. It provides a systematic approach to implementing, monitoring, maintaining, and improving information security in organizations. ISO/IEC 27001 aims to ensure the confidentiality, integrity and availability of information through the application of a risk management process and provides stakeholders with the necessary assurance that risks are correctly assessed and appropriately managed. ISO/IEC 27001 also serves as a benchmark for managing information security practices, including risk management and compliance.
- National Institute of Standards and Technology (NIST) SP 800-53: This model provides a catalog of security and privacy controls intended for U.S. federal information systems.

However, it is also applicable to private organizations. SP 800-53 includes 18 control families covering all aspects of information security, including access control, awareness and training, audit and accountability, security assessment and approval, configuration management, contingency planning, identification and authentication services, maintenance, media protection, physical and environmental protection, planning, risk assessment, system and information integrity, system and service acquisition, System and communication protection and system and information protection. NIST SP 800-53 is typically used to assess risk and improve information security in organizations. It helps identify potential vulnerabilities and threats to information systems and implement appropriate security controls to mitigate these risks.

- Control Objectives for Information and Related Technologies (COBIT): COBIT is an IT governance framework developed by the IT Governance Institute (ISACA). It provides best practices for managing and controlling IT assets and also serves as a standard for information security. With regard to information security, COBIT offers various objectives and controls to ensure the confidentiality, integrity and availability of information.
- Confidentiality: COBIT helps to ensure that only authorized persons have access to confidential information. It includes controls to manage user permissions and monitor access to information systems.
- Integrity: COBIT includes control mechanisms to ensure that information is accurate, complete and has not been altered without authorization. It includes controls to process data, secure transactions, and manage changes in information systems.
- Availability: COBIT ensures that information and systems are available and accessible when needed. It includes controls to monitor system performance, manage capacity, and minimize downtime.

In addition to these goals, COBIT also helps organizations meet regulatory requirements by providing governance structures and processes to ensure compliance. It also supports risk assessment and risk management in relation to information systems. Overall, COBIT provides a comprehensive framework to help organizations achieve secure and effective IT management and control while meeting business and regulatory requirements.

A cross-comparison of these models can help organizations choose the most appropriate method to assess and improve their information security. Each model has its strengths and weaknesses, and the ideal choice depends on the specific needs and circumstances of the organization.

4. Dissemination and application

In a 2020 study by the Federal Office for Information Security (BSI), it was found that about 58 percent of the public bodies surveyed in Germany are striving for BCM planning or have already implemented it. In some countries, the implementation of BCM is required by law for certain public institutions (e.g. health services, emergency services), but in others it is not. Thus, the prevalence of BCM can vary greatly. However, there are some findings that suggest that awareness of the need for BCM in public institutions is increasing. For example, research shows that after major natural disasters or epidemics occur, interest in and demand for BCM plans in public institutions tends to increase.

Fig. 1. Key Elements of an Effective BCM Program.
Source: Own Diagram

4.1. Steps towards a holistic BCM system

Organizational resilience is one of these terms. It refers to an organization's ability to withstand disruption and respond quickly when needed. An organization with high organizational resilience has the ability to detect threats, minimize impact, and successfully recover from setbacks. Emergency management is a crucial part of BCM. It includes measures to prepare, respond and recover from an emergency. This can include anything from natural disasters to technical failures. Effective emergency management can help minimize damage and reduce recovery costs. The situation is similar with crisis management. While emergency management is more focused on immediate events, crisis management focuses on limiting the damage and steering the company through a longer-term crisis. This can include both internal and external crises.

The components of the BCMS are diverse and include business impact analysis (BIA) and risk management. The BIA is a process used to determine the potential impact of an interruption on business operations and to prioritize the restoration of operational capability. In this way, the BIA provides valuable information for the preparation of emergency plans and crisis management.

Risk management, on the other hand, is the process of identifying, assessing, and prioritizing risks, followed by applying resources to minimize, control, and monitor the likelihood or impact of adverse events. It is an important part of the BCMS as it helps identify potential threats and take appropriate action to mitigate risk. After all, processes are the orderly processes that make up daily business. In the context of the BCMS, this means designing and managing these processes in such a way that they are tolerant of disruption and can be quickly restored in the event of an emergency or crisis.

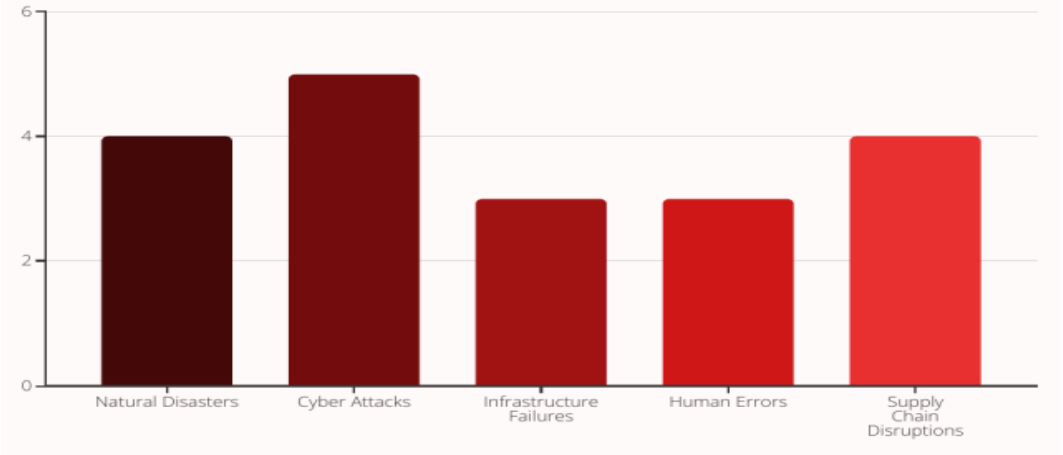

Fig. 2. Risk factors by an business impact analysis.
Source: Own Diagram

BCM is a complex and important task that can significantly affect the success or failure of a company during and after a crisis. However, with the right tools and approaches, a company can ensure that it is prepared for any situation.

4.2. Findings and Potentials

Business continuity management (BCM) is a central component for the maintenance and smooth functioning of business processes in institutions worldwide. This concept focuses on ensuring that critical business processes are restored and continued during and after a disaster. Despite its importance, however, there is often a lack of sufficient investment in BCM programs required for their comprehensive implementation and ongoing operation.

The reasons for the lack of investment in BCM are manifold. Some organizations don't see the need for such a program, while others find the potential cost and complexity involved in implementing it a deterrent. In addition, the lack of regulations and standards can discourage institutions from experimenting in a pilot to pursue BCM strategies.

Despite these challenges, the concept of BCM is gaining international importance. To reap the benefits of BCM and minimize the drawbacks, institutions should define clear goals, seek executive buyback, and assemble a cross-functional team. They should also invest in their employees by training them in BCM practices and teaching them the importance of BCM. Finally, they should regularly review and update their BCM programs to ensure they are effective in the event of an emergency.

From an international perspective, regulations and standards in the field of BCM are becoming increasingly important. Many countries and regional entities have begun to develop and implement specific BCM standards, which motivates companies to invest in BCM programs and practices.

Although the establishment of BCM in the global economy is still in its infancy, it is important that companies become aware of the importance of BCM and integrate it into their business strategies. As a consequence, a governance model for public institutions would also have to be developed.

5. Conclusions

Information security is an overarching topic that is of great importance in a networked world. It covers various areas from the establishment of security standards to data protection and defense against cyberattacks. Various working groups and decision-making networks at national and international level have a significant influence on the design of specifications in this area. It participates in the development of IT security standards at national and international level and makes recommendations for risk mitigation and prevention.

However, these networks often face challenges when it comes to implementing security mandates.

Leadership decisions that neglect investments in information security are a significant problem. We often lack understanding that information security is a strategic investment that can prevent potential losses from data breaches, intellectual property theft, and brand reputational damage.

Another critical point is the lack of employee training in the field of information security. Employees are often the weakest point in the security chain, as they can become the target of phishing attacks and other social engineering techniques.

In addition, the integration of the topic of information security into mission-critical processes is often insufficient. Information security should be seen as an integral part of all business processes and anchored in the corporate culture. This is the only way to ensure that all employees understand the importance of information security and take it into account in their daily work.

Overall, the above-mentioned working groups and decision-making networks should be supported in their work and their recommendations should be taken seriously. The transfer of risk identification in systematic considerations seems to be insufficient due to the reporting situation on the implementation status.

References

[1] EY, „Global Information Security Survey," 2018. [Online]. Available: https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf.

[2] Ponemon Institute, „The Cost of Cyber Crime Study," 2016. [Online]. Available: https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf.

[3] KPMG, „CIO Survey," 2017. [Online]. Available: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/07/harvey-nash-kpmg-cio-survey-2017.pdf.

[4] Cybersecurity Insiders, „2024 Insider Threat Report," 2024. [Online]. Available: https://go.crowdstrike.com/global-threat-report-2024.html?utm_campaign=cao&utm_content=crwd-cao-eur-dach-en-psp-x-wht-gtr-tct-x_x_x_x-x&utm_medium=sem&utm_source=goog&utm_term=threat%20report%20global&cq_cmp=12613083831&cq_plac=&gad_source=1&gclid=Cj0KCQ.

[5] Cisco, „Cybersecurity Series 2020: The Future of Secure Remote Work Report," 2020. [Online]. Available: https://www.cisco.com/c/dam/global/en_uk/products/security/pdf/cisco-emea-report-2020_fa_final.pdf.

[6] A. Rathmell, R. Jones und T. Ciza, „Understanding cyber risk: Lessons from the frontline," *International Journal of Information Security,* Bd. 17(3), pp. 283-297, 2018.

[7] B. Stiftung, „Kommunale Finanzen 2016: Eine Analyse der Jahresabschlüss," *Bertelsmann Publishing,* 2016.

[8] S. Kuhlmann, J. Bogumil und S. Grohs, „Kommunale Verwaltung in der digitalen Kommune," *Der digitale Wandel in Kommunen,* pp. 83-104, 2019.