NEW BULGARIAN UNIVERSITY

DEPARTMENT OF NATIONAL AND INTERNATIONAL SECURITY

DOCTORAL DEGREE PROGRAM “SECURITY STRATEGIES AND POLITICS”

INCREASING THE EFFECTIVENESS OF THE MEASUREMENT AND EVALUATION PROCESS OF THE ORGANIZATION’S CYBERSECURITY CAPABILITIES

EXTENDED ABSTRACT

of the dissertation for acquiring a “Doctor of Philosophy” degree in:
higher education field: 9. Security and defense,
professional field: 9.1. National security

Author: Dimitar Krasimirov Dimitrov

Scientific supervisor: prof. Venelin Georgiev, PhD

Sofia, 2023

The dissertation was discussed and accepted for defense at a meeting of the Department of National and International Security, held on ……………. 2024.

The dissertation consists of 146 pages, 15 figures, 22 tables, 2 appendices and a bibliography including 63 sources.

The defense of the dissertation will take place at an open meeting on 27.06.2024 at 11:20, building 1, room 407, NBU.

All materials are available to those interested in Building 2, room 202, NBU, 21 Montevideo Str., Sofia, 1618

Author: Dimitar Krasimirov Dimitrov

Title: Increasing the Effectiveness of the Measurement and Evaluation Process of the Organization's Cybersecurity Capabilities

TABLE OF CONTENTS

GENERAL CHARACTERISTICS OF THE DISSERTATION

Relevance, Object and Subject of the Research

With the advent of information technology, mobile devices, computer networks and the Internet, as well as the constant influx of new users of services and information, cyberspace is increasingly becoming a reflection of the real world. Never before has humanity been so connected as in the 21st century. A significant proportion of people are constantly online, and a large variety of programs, applications, web pages and social networks offer their users virtual experiences close to those of the real world - analogues of activities that connect them with relatives and friends, entertain them or assist them in their work.

Digital products for increasing the efficiency of the work process have long been widely used in business environments. Products such as Microsoft Word, Excel, PowerPoint, Visio, SPSS, AutoCAD, etc. provide an opportunity for productivity increase, minimizing errors, faster calculations, automatic word processing and presentations of data in text, tables. graphs and figures.

With the popularization of the Internet, e-mails, IM[1] and VoIP[2] calls are replacing conventional letters and telephony as a more efficient, more convenient and lower-cost way of communication. Alongside this, the boom of social networks such as Facebook, Twitter and Instagram, makes the communication with consumers even more personal - the business can present itself with a human face to the customer.

At the same time, it should not be forgotten that cyberspace can be a source of danger. Fast and limitless connection brings risks. The connectivity inside of the cyberspace and the accessibility of its infrastructure bring threats both to the

[1] Instant Messaging

[2] Voice over IP

confidentiality and the integrity of the information transmitted electronically, and to the availability of the services offered by the business.

The billions of dollars in losses and the constant change in cybercriminals' attack patterns and approaches make cybersecurity issues particularly relevant for businesses. Business organizations are forced to take a proactive approach in developing security capabilities that cover not only their informational and technological assets, but also their entire organizational structure.

To acquire adequate cybersecurity capabilities, organizations need an effective process for selecting, building, and managing them. And in order for this process to be effective - from an effective process for measuring and evaluating these capabilities. This provides an opportunity for both the selection of security activities and practices, and for measuring and evaluating their implementation within the organization. This dissertation examines this interconnected system.

The object of research in the dissertation is the process of measuring and evaluating the organization's cybersecurity capabilities, and **the subject of research is the effectiveness of this process**.

Hypotheses, Goal, and Research Problems

The thesis of the dissertation is built from two interrelated hypotheses:

- the stated strategic tools for measuring and assessing the cybersecurity capabilities do not fulfill all the requirements to ensure process effectiveness and present the possibility of gaps in the planning and creating cybersecurity within the organization;
- combining them into a new model would lead to an increase in the effectiveness of the process of measuring and assessing the cybersecurity

capabilities of the organization, as well as supporting the process of planning and building these capabilities.

The goal of the research is to conduct a study on the effectiveness of the process for measuring and evaluating the organization's cybersecurity capabilities and to propose opportunities for its increase.

To achieve this goal, the following **research problems** have been solved in the dissertation:

1. Exploring the theoretical aspect of organizational cybersecurity capability delevomepent, focusing on its process nature.
2. Establishing a conceptual framework for measuring the effectiveness of the cybersecurity evaluation and measurement process.
3. Conducting a comparative analysis of the effectiveness of the process managed with the selected strategic tools based on certain criteria and creating the framework of a problem analysis in order to eliminate the identified weaknesses.
4. Conduct a problem analysis to determine the problematic areas for process effectiveness of the selected strategic tools.
5. Conceptualizing, building, and implementing a model to increase the effectiveness of the measurement and evaluation process of the cybersecurity capabilities and based on this, formulate recommendations for improving the process.

Methodology and Limitations

The following **research approaches** are used for the implementation of the research part: systematic, systemic, process, historical and modeling.

The *systematic and systemic approaches* are used to analyze the elements and characteristics of the tools for measuring and evaluating the cybersecurity in organizations in the context of their implementation environment.

The process of measuring and evaluating cybersecurity itself requires the use of the *process approach* for its study.

The *historical approach* is used to trace the development of both the cyber threats for the organization and the development of the toolkit for planning, building and measuring cybersecurity capabilities.

Through the *model approach*, conditions are created for researching the process of measuring and evaluating the cybersecurity capabilities under the conditions of a predetermined scenario.

The study of the effectiveness of cybersecurity measurement and evaluation tools is done using the following **research methods**: theoretical analysis, comparative analysis, synthesis, scientific abstraction, problem analysis, modeling.

The following ***limitations and assumptions*** are made within the framework of this dissertation:

- Matters related to cybersecurity inside the organizations are a classified information.
- Each organization's cybersecurity target profile is strictly individual.
- The focus of the study is on the process of measuring and assessing the cybersecurity capabilities within the framework of business organizations, rather than on specific cybersecurity measures and capabilities. It considers the process as it is managed by the strategic management tools that provide the possibility of evaluation and control within the entire organizational structure and its units. Entirely technological tools, measures and practices are beyond the focus of this study.

Structure of the Dissertation

The content of the dissertation includes: introduction, three chapters, general conclusions and recommendations, conclusion, appendices, list of tables, list of figures.

The introduction presents the reader with the following characteristics of the research: relevance of the topic, the object, the subject, goal and problems of the research, hypotheses, methodology, limitations and assumptions, applicability of the results of the development.

Chapter One presents the theoretical setting of the study**.**

A brief historical overview of the development of the need for developing cybersecurity in organizations and its research is presented. The process for planning and building cybersecurity capabilities within the organization is detailed.

A definition of an *effective process for measuring and evaluating cybersecurity capabilities* is proposed, and the definition is complemented by a target matrix of process effectiveness factors. The requirements for the process management tools are defined so that the availability of process effectiveness factors can be ensured.

The chapter examines the essence of strategic tools for managing the process, in particular the Balanced Scorecard for Cybersecurity Measurement and the C2M2 Cybersecurity Capability Level Measurement Model.

In **Chapter Two**, the criteria and requirements for performing the comparative analyzes of the effectiveness of the cybersecurity measurement and evaluation process, managed by the cybersecurity measurement and evaluation tools selected in the first chapter, are presented. Research and analysis of the selected process management tools for measuring and evaluating cybersecurity using the defined criteria are described. The results of these studies are systematically presented.

Chapter Three explores the possibility of increasing the effectiveness of the cybersecurity capability measurement and evaluation process by proposing a combined model for planning, measuring, and building capabilities. The chapter describes the conceptual basis, the prerequisites for synthesis, as well as the construction of the model itself. The newly proposed model is subjected to allanogical analysis, following the example of the those carried out in Chapter Two.

A description is proposed for implementing the proposed combined model in the organizational framework to manage the process of planning and building cybersecurity capabilities in the organization and increasing its effectiveness.

CONTENTS OF THE DISSERTATION

Chapter One. Theoretical Aspects of the Process of Measuring and Evaluating the Organization's Cybersecurity Capabilities

Chapter One is composed of five main parts and sets the theoretical basis of the study.

A historical background on the development of the need to build up cybersecurity in organizations and its research is presented. The process for planning and building cybersecurity capabilities within the organization is detailed.

A definition of an *effective process for measuring and assessing cybersecurity capabilities* is proposed and the definition is supplemented by requirements for the managing tools to ensure the effectiveness of the process.

The chapter elaborates on the essence of strategic process management tools, in particular the cybersecurity measurement balanced scorecard and the C2M2 cybersecurity capability measurement model.

The first part presents the historical overview of the development of both the threats and the cybersecurity capabilities of the organizations. The data and findings of the annual survey of Ponemon Institute/Keeper Security [3, 4, 5, 6] for the period 2016-2020 are presented and reviewed with the aim of a detailed analysis of the main problems that the organizations are facing.

[3] Keeper Security, Ponemon Institute (2017). The 2016 State of SMB Cybersecurity. Ponemon Institute SMB Cybersecurity Annual Report

4 Keeper Security, Ponemon Institute (2019). The 2018 State of SMB Cybersecurity. Ponemon Institute SMB Cybersecurity Annual Report.

5 Keeper Security, Ponemon Institute (2020). The 2019 SMB Cybersecurity Study. Ponemon Institute SMB Cybersecurity Annual Report.

6 Keeper Security, Ponemon Institute (2021). Cybersecurity in the Remote Work Era: A Global Risk Report. Ponemon Institute SMB Cybersecurity Annual Report.

The survey in question demonstrates the following trends:

- the majority of cybersecurity decisions are made by the top management of organizations;
- for only a minor part of the respondents, the organization's activity determines the priorities for cybersecurity;
- the percentage of responses "No one function determines IT security priorities" is high.

These trends identify employee negligence, lack of clear responsibilities and priorities for building cybersecurity, and tying cybersecurity to the organization's core business as the *main issues for organizations to effectively defend against cyber threats*.

In the second part of Chapter One, the development of cybersecurity capabilities in the organization is examined in detail - the planning components and the phases of the process itself.

The main components of planning are: process, strategy and infrastructure[7]. The full assessment of these components involves an in-depth analysis of the steps of the cybersecurity capability planning process, which are summarized as follows:

- Determining the current state of cybersecurity capabilities described with their appropriate characteristics;
- Analysis of the organization's development goals and strategy to determine future cybersecurity capability requirements;
- Identifying the missing cybersecurity capabilities and determining the necessary activities for eliminating the gaps;

[7] Georgiev, V. (2015). "Cybersecurity Capability Planning." Scenario Planning for Cyber Security Capabilities. NBU

- Develop a plan to execute the activities in steps, the implementation of which would lead to the development of the necessary cybersecurity capabilities;

Based on the above steps, the methodology for planning the company's cybersecurity capabilities is created and the process itself is summarized in the following phases:

- Determination of strategic directions - an analysis of the organization's strategic plan is carried out and the goals are identified. Cybersecurity target capabilities are defined;
- Analysis of current state of capabilities and identification of missing cybersecurity capabilities;
- Develop a plan to build the missing capabilities. Metrics are selected for the implementation of the plan and achievement of the organization's goals;
- Implementation of the action plan and evaluation of the results obtained using the selected metrics;
- Monitoring, review and evaluation of the results of the implementation of the plan;

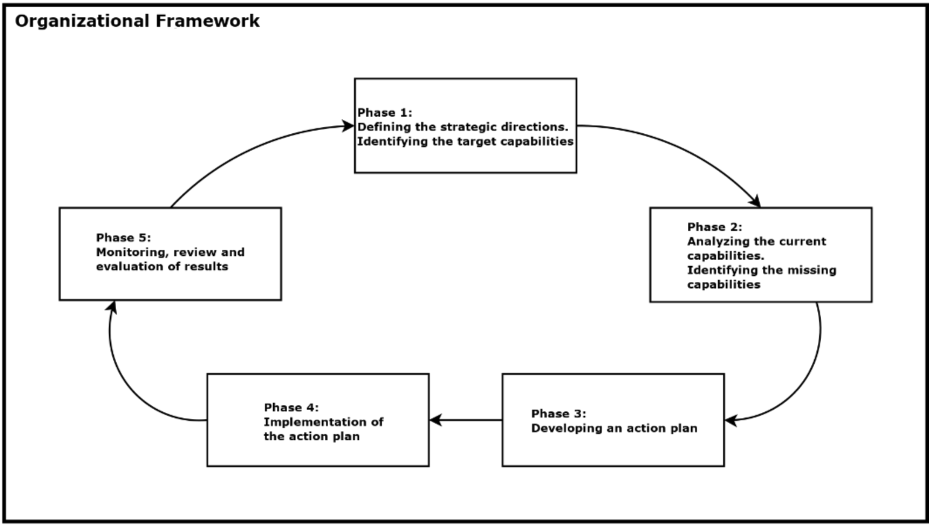
Organizational Framework
Phase 1:
Defining the strategic directions.
Identifying the target capabilities
Phase 2:
Analyzing the current capabilities.
Identifying the missing capabilities
Phase 3:
Developing an action plan
Phase 4:
Implementation of the action plan
Phase 5:
Monitoring, review and evaluation of results

Figure 1. Process phases for planning and building cybersecurity capabilities

The third part of Chapter One defines the conditions for the effectiveness of the process for measuring and evaluating cybersecurity capabilities.

Analytics and decision-making are key factors in every phase of the process. The individual process planning components as well as their elements point to cybersecurity as an organization-wide phenomenon. In parallel, cybersecurity also depends on external factors and the specifics of cyberspace itself.

The effectiveness of the process depends on:

- the ability to properly plan the capabilities to be built/improved;
- the ability to monitor the progress of the process. This requires the ability to extract relevant data at every stage of the process;
- an opportunity to present the extracted data and information to the relevant groups who need to analyze, evaluate and make a decision;

Therefore, the effectiveness of the process is directly dependent on the tools used for measurement and evaluation.

Based on the above conditions, the directions in which to analyze those tools are determined in order to study the effectiveness they provide for the process within the organization:

- To ensure an effective process, the tools must cover the entire organization - both its internal structure and functions, and the external factors that define the context of its activity. This condition predetermines the choice of management tools in order to ensure the effectiveness of the process.
- It is necessary to examine the chosen tool as an intermediary between the entity using it to measure (the organization and its interested levels) and the object being measured (the process of planning and building cybersecurity capabilities). In this case, for the effective intermediary (the evaluation tool) there must be beneficial two-way interactions with both systems it connects. In this way, two main perspectives on the effectiveness of the tool can be derived and conclusions can be drawn about each of them: *adaptability to the frame* and *process management*.

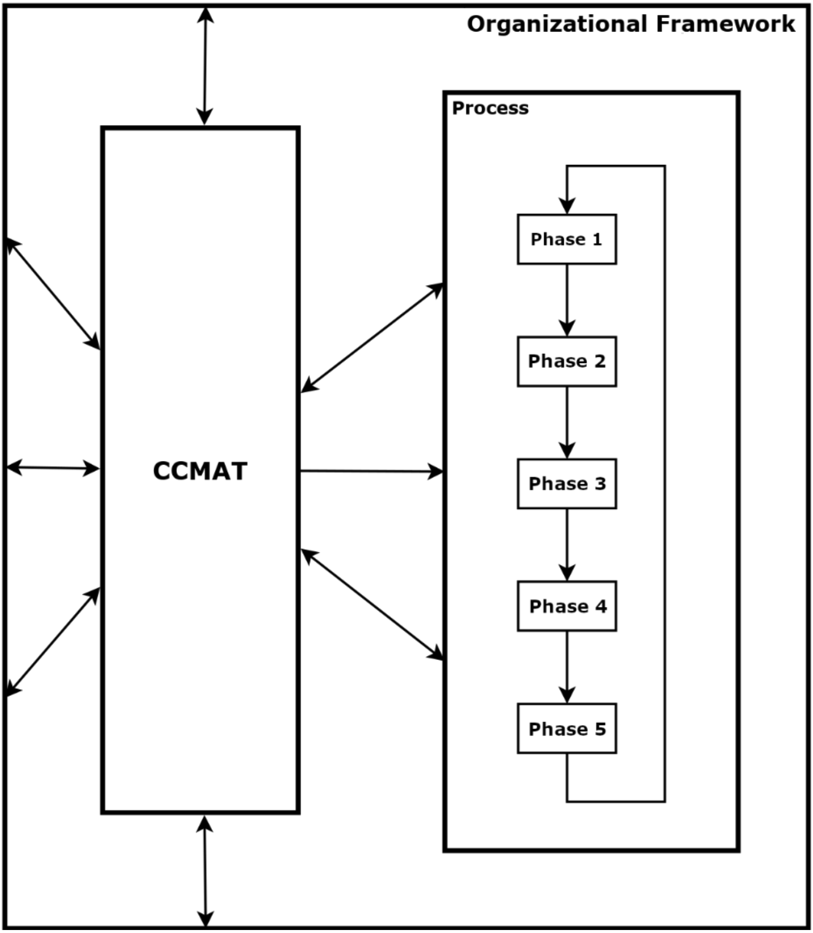

Figure 2. The Cybersecurity Capability Measurement and Evaluation Tool (CCMAT) as a medium between the organizational framework and the organization's cybersecurity capability planning and building process

The fourth part of Chapter One is a detailed overview of the structure and application of the Balanced Scorecard for Cybersecurity Assessment.

The purpose of the metrics laid out in the balanced scorecard is to provide information on aspects of the organization’s activity that are related to the internal structure, the level of personnel abilities and relations with entities external to the organization.

To balance the indicators in the map, Kaplan and Norton [8,9] propose a distribution into four groups known as aspects, thereby creating a sufficiently accurate and complete picture of the functions within the organization. The four aspects in question are:

- *financial* - this group includes traditional economic indicators;
- *customers* - this is where performance metrics for working with customers are included;
- *internal* - the group contains internal organization performance metrics;
- *learning and growth* - metrics for measuring knowledge and innovation.

For completeness, each of the indicators in the balanced scorecard should be described with the following characteristics:

- target - closely related to the framework of the organization.
- an indicator/metric with which the level of achievement of the goal is measured.
- target value;
- measured activity;

In this way, a framework is created, assisting organizations in distributing in a convenient and balanced way the indicators for measuring the effectiveness of their activity. Within this framework, they are free to choose the specific metrics that best

[8] Kaplan, Robert S; Norton, D. P. (1996). "The Balanced Scorecard – Measures That Drive Performance". Harvard Business Review (January–February): 71–79.

[9] Kaplan, Robert S; Norton, D. P. (1996). The Balanced Scorecard: Translating Strategy into Action. Boston, MA.: Harvard Business School Press. ISBN 978-0-87584-651-4

describe their activity. Also, if necessary, an additional aspect can be added or one of the proposed ones can be omitted. A critical part of choosing metrics is that the metrics and perspectives are in the context of the company's vision, mission, values, and strategy.

The essence and application of the C2M2 model are described in the fifth part of the First Chapter.

The model is organized into ten domains. They represent logically related groups of cybersecurity practices. In turn, practices are grouped by targets that the company is trying to achieve. Within the content of each area, the practices are arranged by maturity level[10].

For each of the domain, the model defines four levels of maturity, which are applied independently of the other domains. The levels define a dual aspects of progression to maturity – an approach progression and an institutionalization progression.

The *approach progression* is described by the cybersecurity goals and practices described in the relevant area of the model.

Institutionalization describes the extent to which a practice or activity is integrated into organizational operations.

The ability to measure changes between levels allows the organization to use the scale to:

- determine its current level of maturity;
- mark a future, higher level of maturity as a target;
- determine the abilities it needs to acquire/develop (targeted and missing) to reach the desired level of maturity.

[10] U.S. Department of Energy и U.S. Departament of Homeland Security (2014). “Cybersecurity Capability Maturity Model Version 1.1”

C2M2 was developed based on cybersecurity standards, guidelines, programs and initiatives. Each domain of the model contains a structured toolkit of practices, activities and capabilities that the organization must perform/acquire/develop in order to reach the next level of maturity.

The historical and documentary analysis provides the theoretical setting for the study and solves the ***first research problem*** pointed in the Introduction.

Chapter Two. Benchmarking the Effectiveness of the Organization's Cybersecurity Measurement and Evaluation Process

Chapter Two is divided into three main parts.

It presents the criteria and requirements for performing comparative analyzes of the effectiveness of the cybersecurity measurement and evaluation process, managed by the cybersecurity measurement and evaluation tools selected in Chapter One.

Research and analysis of selected process management tools for measuring and evaluating cybersecurity using the defined criteria are described. The results of these studies are also systematized and presented.

In the first part of Chapter Two, the criteria for the subsequent comparative analyzes were selected based on the factors of effectiveness derived in Chapter One. Maps have been compiled with criteria for evaluating the effectiveness of the tools under consideration for both perspectives.

Category	Adaptability to:
Organizational framework	vision
	mission
	values
	strategy
Internal structure	goals
	organizational structure
	internal policies
Holistic model	internal processes
	personnel
	technologies
External framework	external policies
	external processes
	external environment impact

Table 1. Criteria Map for Framework Adaptability

Process phases	Manages
Phase 1	the selection of the target level of cybersecurity
Phase 2	the measurement of the current level of cybersecurity
	the identification of missing cybersecurity capabilities
Phase 3	the selection of standards, procedures, and practices for building cybersecurity
Phase 4	the effective monitoring of the implementation of the plan
	the integration of the selected standards, practices and procedures into the general organizational structure and activity
Phase 5	evaluating the results of the implementation of the plan
	data visualization and analysis
	making informed decisions
	the process iteration

Table 2. Criteria Map for Planning and Building Cybersecurity Capabilities Process Management

In order to facilitate the presentation of the research results, a *process efficiency assurance coefficient* is proposed, which is calculated according to the following formula:

$$E = \frac{\sum_{i=1}^{n} pr_i}{\sum_{i=1}^{n} pt_i} \qquad (1)$$

където:

- **E** is an efficiency assurance coefficient;
- **n** is the total number of criteria;
- **pr** is a real point score for criterion coverage;
- **pt** is a target score for criterion coverage.

For this purpose, a 5-point scale is used for the coverage of each of the criteria in the maps.

The conceptualization of process effectiveness measurement presented in this part solves the *second research problem*.

In the second part of the Chapter Two, the results of the comparative analyzes between the target maps (those with the maximum score for all criteria) and the coverage of the selected criteria by the two tools are presented.

Category	Adaptability to:	Target	BS	C2M2
Organizational framework	vision	++	++	-
	mission	++	++	-
	values	++	++	-
	strategy	++	++	-
Internal structure	goals	++	++	-
	organizational structure	++	+	+
	internal policies	++	+	-
Holistic model	internal processes	++	+	-
	personnel	++	+	-
	technologies	++	+	+
External framework	external policies	++	+	-
	external processes	++	+	-
	external environment impact	++	+	-

Table 3. A summary of the comparative analysis of the framework adaptability criteria coverage of the Balance Scorecard (BS) and C2M2

Process Phases	Manages	Target	BS	C2M2
Phase 1	the selection of the target level of cybersecurity	++	-	+
Phase 2	the measurement of the current level of cybersecurity	++	-	+
	the identification of missing cybersecurity capabilities	++	-	+
Phase 3	the selection of standards, procedures, and practices for building cybersecurity	++	-	+
Phase 4	the effective monitoring of the implementation of the plan	++	?	++
	the integration of the selected standards, practices and procedures into the general organizational structure and activity	++	-	++
Phase 5	evaluating the results of the implementation of the plan	++	?	++
	data visualization and analysis	++	+	++
	making informed decisions	++	+	++
	the process iteration	++	+	++

Table 4. A summary of the comparative analysis of process management criteria coverage of the Balance Scorecard (BS) and C2M2

The coefficients for ensuring efficiency have been calculated:

- $E(FA^{11})_{BS} \approx 0.88$ и $E(PM^{12})_{BS} = 0.56$
- $E(EA)_{C2M2} \approx 0.46$ и $E(PM)_{C2M2} = 0.92$

The results of these analyzes and the large difference between the calculated values of the coefficient and the target value of the coefficient ($E_T = 1$) demonstrate weaknesses in the tools and the possibility of ineffectiveness of the process. These weaknesses can be further explored through a problem analysis.

The comparative analyzes made solve the *third research problem*.

The third part of Chapter Two presents the results of the aforementioned problem analysis. It defines the problem areas of the tools:

- for the Balance Scorecard - formulating, planning and facilitating the process;
- for C2M2 - the adaptation of the tool to the framework of the organization.

Conducting the problem analysis solves the *fourth research problem* and confirms the *first hypothesis of the dissertation*.

Chapter Three. Modeling the Process for Measuring and Evaluating the Cybersecurity Capabilities of the Organization in Order to Increase its Effectiveness

Chapter Three is composed of three main parts.

The chapter describes the conceptual basis, the prerequisites for building, as well as the actual synthesis of a combined model for planning, measuring and evaluating cybersecurity capabilities. The implementation of the model is described and the efficiency assurance for the process is analyzed.

[11] FA = Framework adaptability

[12] PM = Process management

In the first part of Chapter Three the conceptual foundation of the combined model is laid out.

Based on the problem analysis conducted in Chapter Two it can be concluded that the balanced scorecard and the C2M2 model suggest the possibility of gaps in the proper management and evaluation of cybersecurity. When analyzing the results, there is an opportunity to overlap the areas of one tool with those of the other in order to minimize their weaknesses and increase the effectiveness of the process. The desired result is shown on Figure 3.

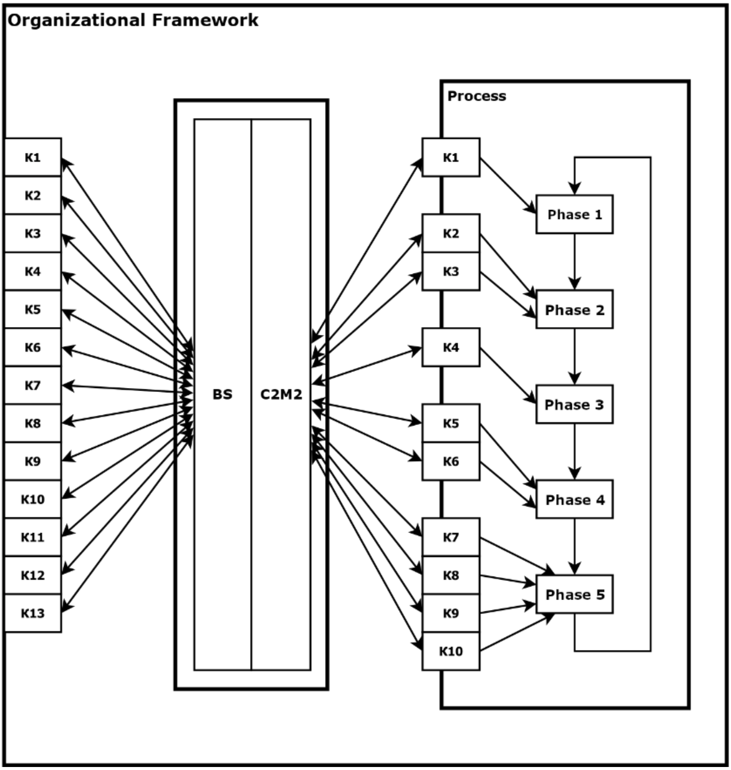

Figure 3. Schematic representation of the concept of the Combined Cybersecurity Capability Measurement and Evaluation Model

At the heart of the conceptual model is to preserve the strengths of both tools and minimize their weaknesses by using:

- the elements from the Balanced Scorecard to ensure a good adaptability to the framework and a balanced distribution of the planned capabilities;
- the elements from the C2M2 model to provide the toolkit for planning, building, evaluating and institutionalizing them.

The second part of Chapter Three describes the decomposition of the two tools into their constituent elements and the synthesis of the combined model.

The "Internal" and "Customers" aspects (from the Balance Scorecard) build the “Operational” domain of the combined model. It is aimed at measuring and evaluating cybersecurity capabilities related to the organization's core activity and functions.

The “Tactical Management” domain contains capabilities that serve the tactical management of cybersecurity. These capabilities are aimed at cybersecurity professionals.

The presented metrics in the domain of "Strategic management" are aimed at the strategic management of the organization. It is built from the "Financial" and "Learning and Growth" aspects and it does not present specific capabilities, but describes the overall development/improvement of the organization's cybersecurity program and its budgeting.

The presented concept solves the *fifth research problem*.

The third part of the Chapter Three presents the results of the comparative analyzes and the calculations of the values of E to investigate the effectiveness of the proposed tool.

Category	Adaptability to:	Target	CM
Organizational framework	vision	++	++
	mission	++	++
	values	++	++
	strategy	++	++
Internal structure	goals	++	++
	organizational structure	++	+
	internal policies	++	+
Holistic model	internal processes	++	+
	personnel	++	+
	technologies	++	+
External framework	external policies	++	+
	external processes	++	+
	external environment impact	++	+

Table 5. A summary of the comparative analysis of the framework adaptability criteria coverage of the combined model (CM)

Process Phases	Manages	Target	CM
Phase 1	the selection of the target level of cybersecurity	++	+
Phase 2	the measurement of the current level of cybersecurity	++	+
	the identification of missing cybersecurity capabilities	++	+
Phase 3	the selection of standards, procedures, and practices for building cybersecurity	++	+
Phase 4	the effective monitoring of the implementation of the plan	++	++
	the integration of the selected standards, practices and procedures into the general organizational structure and activity	++	++
Phase 5	evaluating the results of the implementation of the plan	++	++
	data visualization and analysis	++	++
	making informed decisions	++	++
	the process iteration	++	++

Table 6. A summary of the comparative analysis of process management criteria coverage of the combined model (CM)

	Target Value	BS	C2M2	CM
E(FA)	1	0.88	0.46	0.88
E(PM)	1	0.56	0.92	0.92
E	1	0.74	0.66	0.9

Table 7. Values of the efficiency ensuring coefficients of the BS, C2M2 and CM

In summary, the results demonstrate an increased overall effectiveness of the cybersecurity capability measurement and evaluation process when using the Combined Model to manage it, both in adapting to the organization's framework and in managing the cybersecurity planning and construction process. This statement confirms the *second hypothesis* of the dissertation.

CONCLUSION AND OVERALL FINDINGS

The object of research in this dissertation is **the process of measuring and evaluating the cybersecurity capabilities of the organization**, and the work focuses on its **effectiveness**. In the course of the review of the documents and the results of the already conducted studies, the presence of weaknesses in ensuring adequate cybersecurity in the organizations and the importance of the human factor for this are established. These conclusions, together with the novelty of this specific field of security, prove the **relevance of the thesis topic**.

The results of the historical review of the development of cybersecurity in organizations proves the need for an **effective process for its planning and development** and the need for a supporting **effective process for its measurement and evaluation**. This process is governed by the so-called measurement and evaluation tools, and the subsequent examination of survey data and documents suggests that these tools should be strategic in scale, i.e. to include in the management of the process the entire structure of the organization.

Examining the theoretical aspect and considering the processual nature of building cybersecurity within the organization provides the necessary theoretical framing of the study and solves the first research problem posed in the Introduction.

On the basis of this theoretical formulation, the conditions "**an effective process for measuring and evaluating the cybersecurity capabilities of the organization**" are defined and the basis for its measurement is conceptualized. Target maps with criteria that must be met to ensure effectiveness are created. An effectiveness ensuring coefficient is also defined. In this way, the second research problem is solved. Also, the theoretical formulation justifies the choice of the research tools – the Balanced Scorecard for Cybersecurity Assessment and the model C2M2.

Using the method of comparative analysis, possible weaknesses of thees tools are identified, which could be a prerequisite for low effectiveness of the process. This is also demonstrated through the calculation of the efficiency assurance coefficient for each tool. This step solves the third research problem and confirms the first hypothesis.

The inferred prerequisites for low effectiveness are further surveyed through problem analysis and the specific problem areas for the tools are defined. Through this, the fourth research problem is solved.

By solving these problems, the first part of the dissertation goal is achieved - the study of the effectiveness of the process for measuring and evaluating the organization's cybersecurity capabilities.

The fifth research problem is solved by proposing a solution for the increase of the effectiveness of the process of measuring and evaluating the cybersecurity capabilities in the organization in the form of a concept of a combined model for planning, measuring and evaluating cybersecurity. Through analysis and subsequent synthesis of the elements of the Balanced Scorecard and the C2M2 model, a way to minimize their weaknesses is proposed. The implementation of the new management model at each phase of the cybersecurity planning and development process is described. The subsequent benchmarking and calculation of the efficiency assurance coefficient demonstrate increased effectiveness of the process managed by the new model.

With the solution of the fifth research problem, the second hypothesis is confirmed and the goal of the research is finally achieved.

Through the proposed model, organizations of all sizes, especially those from small and medium-sized scale are given the opportunity to build an effective and adequate cyberdefense, based on good practices and procedures and tailored to their framework, structure and activity.

CONTRIBUTIONS

The scientific contributions contribute to the development of knowledge in the field of the subject of the dissertation and are formulated as follows:

- defining the necessary conditions for "an effective process for measuring and evaluating cyber security in the organization";
- creating a conceptual framework for measuring the effectiveness of the cybersecurity capability measurement and evaluation process;
- modeling a combined tool for planning, measuring and evaluating organizational cybersecurity capabilities.

The applied contributions are directly related to the implementation of the developed model in practice and are formulated as follows:

- developing a system of criteria to ensure the effectiveness of the process for measuring and evaluating cybersecurity, aimed at the tools for managing this process;
- synthesizing the combined model for planning, measuring and evaluating cyber security capabilities in the organization;
- description of the implementation of the combined model for managing the process of measurement and evaluation of cybersecurity in the organization.

PUBLICATIONS

1. Dimitrov, D. (2020). Dystopia in Utopia. Cyberthreats to the smart city. National Security and the European Union: Youth Security Discussion Forum "Current Urban Security Issues in EU Member States", 29 November 2019, Student Security Webinar "National Security and the European Union", 12 June 2020: Proceedings reports, Avangard Prima, Sofia, pp. 7-12, ISBN 978-619-239-520-9

2. Dimitrov, D. (2020). Social engineering - a major threat to business. Recommended protection measures, Proceedings of the International Scientific Conference "Broad Security", Volume 2, National and International Security Department, NBU, Sofia, 2020, pp. 570-572, ISBN 978-619-7383-19-5

3. Dimitrov, D. (2020). Cybersecurity in business: the human factor, Proceedings of the International Scientific Conference "Broad Security", Volume 2, Department of "National and International Security", NBU, Sofia, 2020, pp. 392-398, ISBN 978-619-7383-19- 5