Cybersecurity management: a knowledge-based perspective

Jan Voracek *

Department of Technical Studies
College of Polytechnics
Tolsteho 16, 586 01 Jihlava, Czech
E-mail: jan.voracek@vspj.cz

Antonin Pribyl

Department of Technical Studies
College of Polytechnics
Tolsteho 16, 586 01 Jihlava, Czech
E-mail: antonin.pribyl@vspj.cz

Johanna Schroeder

Faculty of Applied Natural Sciences and Cultural Studies
Ostbayerische Technische Hochschule Regensburg
Seybothstraße 2, 93053 Regensburg, Germany
E-mail: johanna.schroeder@oth-regensburg.de

* *Corresponding author*

Abstract

The continuously growing importance of cybersecurity is an unavoidable consequence of the rapid development of innovative technological solutions, including, e.g., ubiquitous networking, mobile computing, Internet of things, or various forms of cloud services. Every new solution, however, gradually threatens electronic data, accessible practically from anywhere. Such vulnerability is critical, particularly in the industrial domain, where single firms and institutions must remain competitive and cannot ignore business advantages if of modern platforms. Although strategic managers are generally aware of cybersecurity risks, they frequently have problems with the efficient implementation of efficient managerial solutions. Thorough characterisation and minimisation of this bottleneck, based on qualitative dynamic modelling, is the primary goal of this research. We see the main reason for this discrepancy in a mainly technical nature of cybersecurity and related tools and policies in comparison with qualitatively oriented frameworks and techniques of strategic management. The existence of such vertical inconsistence naturally reflects knowledge asymmetry between business, architectural and logical views of enterprise architecture on one side and explicit ways of network communication, configuration of related components and other physical aspects on the other.

Consequently, the cybersecurity planning power of strategic managers tends to be limited and unfocused. Such a lack of specific technical knowledge can result in the adoption of risky and possibly limiting strategies of cyber under- or overprotection. Beyond the internal vertical gap, there is also a horizontal gap, influencing company interoperability in external networks, like supply chains, critical infrastructures, keiretsu groups, or international partnerships.
We believe that both kinds of problems could be minimised with transparent and holistic integration and continuous bidirectional understanding and sharing of related business and technical knowledge. That is why we conducted a literature review, reflecting typical structural and behavioural aspects, related to all investigated levels and directions of cybersecurity management in a business context. Collected results were visualised and analysed using the mind map and system diagram. Based on these findings, we formulated a set of typical dynamic hypotheses and validated it quantitatively through the corresponding causal loop diagram. Because of the adopted knowledge-based approach, we propose a generally transparent, but still reasonably comprehensive solution, addressing both strategic decision-makers and technicians.

Keywords – Cybersecurity, Business alignment, Qualitative modelling

Paper type – Academic Research Paper

1 Introduction

Cybersecurity is a pervasive phenomenon, attracting the increasing interest of authorities, industry, researches and end-users (Lezzi et al., 2018), (Pala & Zhuang, 2019), (Sánchez et al., 2019), (Fitzgerald, 2020) as a side effect of progressively escalating development of information and communication technologies (Leszczyna, 2018), (Habibzadeh et al., 2019), (Corallo et al., 2020). Importance of cybersecurity on all levels is widely reflected by international and national legislation, e.g., (Directive (EU) 2016/1148, 2016), (Commission Implementing Regulation (EU) 2018/151, 2018), (Council Regulation (EU) 2019/881, 2019) and industrial standards (International Organization for Standardization ISO/IEC 13335-1:2004, 2004), (ISO/IEC 27002:2005, 2005), (ISO/IEC 27002:2013, 2013), (ISO/IEC 30111:2019, 2019), supported by specialised institutions (ENISA, The European Union Agency for Cybersecurity, ECSO, The European Cyber Security Organisation) and implemented through wide range of different frameworks and up-to-date tools (Li et al., 2019), (Bland et al., 2020), (Williams et al., 2020).

Despite this effort, the number, intensity and impact of cyberattacks growth as a natural consequence of the increasing number of interconnected devices (Arumugam &

Subramanian, 2019). Thus the contemporary orientation on smart spaces and people-centric approaches (Elmaghraby & Losavio, 2014), (Rawat & Ghafoor, 2019) considers the systematic embedding of security principles to any kind of interaction with information and communication (ICT) resources as an unavoidable must. The inherent complexity of this task, however, lies in its two-folded nature. Disregarding whether we deal with the private, industrial or public traffic, there is an evident gap between the technical and user level of computer applications, which our research strived to fill. To narrow the spectrum of the addressed target audience, we concentrated only on security aspects of enterprise information systems and on the qualitative level answer the following question:

Is it possible to present cybersecurity matters also to the non-technical strategic manager makers in a transparent, applicable and profitable form?

Such formulation anticipates the following assumptions:

- Transparency means that the structural and functional formalisation of the analysed phenomenon must be generally understandable, easy to interpret and discuss, as well as precise and concise. All these criteria can be met on the knowledge level of representation, which integrates and creatively summarises available data and information resources (Lai, 2007), (Brusoni et al., 2009), (Malhotra & Nair, 2015). If done correctly, significant characteristics remain preserved and selected specific details are omitted.
- Applicability and profitability are based on a seamless inclusion of proposed model into standardised performance management frameworks. These arrangements expect realistic definition and quantification of all involved variables.

To fulfil these goals, we adopted the balanced scorecard framework (BSC) and extended it with knowledge-based aspects of cybersecurity, including the threat intelligence, measures of cyber risks and security-supporting architectures, orchestrated in the following context:

- Value engineering as a transparent way of company value-creating processes requires systemic utilisation of standardised performance architectures (Kiran, 2017), (Egbuhuzor & Port, 2019), (Yihong et al., 2019). They must reflect its two-folded structure, incorporating effectiveness, i.e. measure of success in doing the right things and efficiency, quantifying the level of embedded quality. Because of cyclic, i.e. dynamic nature of management, related frameworks must use temporal indicators from all internal domains of business, because single time slice can

hardly explain complex relations among its key leading (predictive, drivers-related) and lagging (output-oriented) indicators (KPIs) (Badawy et al., 2016), (Domínguez et al., 2019). This research used mainly strategic mapping and dynamic balanced scorecards techniques (Kaplan & Norton, 2005), extend with selected features of next generations of BSC (Sofiyabadi & Nasabb, 2012), (Nielsen & Nielsen, 2013) and inclusion of cybersecurity performance features into this framework.

- Cyber threat intelligence (Abu et al., 2018), (Wagner et al., 2019), (Shin & Lowry, 2020) can be considered as a complementary initiative to the researched topic. Generally, the threat intelligence is evidence-based, must deliver expected value and allow to formulate efficient counteractions. Its main goal to collect and distribute information about passed threats and their actors to strengthen the current level of cyber resilience. Its outputs can be in the form of technical recommendations, traditional and advanced data analyses or comprehensive knowledge-based representations, depending on the level of discovered behaviour. Final recommendations are composed of internally collected data and knowledge and extended with experience form external partners and security-related communities of practice. They include strategic suggestions for board members and C-type of managers, tactical hints for security architects, operational information, characterising defenders' behaviour and finally also technical data, quantifying incident parameters.
- Cybersecurity/cyber risk indexes transform diverse and interlinked cybersecurity aspects into a single number, which is convenient for governance and strategic planning (Lewis et al., 2012), (Bunker, 2020), (Hoffmann et al., 2020). There are several recognised approaches, combining internal cybersecurity capabilities with the country and industrial sector-specific characteristics (Sammut-Bonnici & Galea, 2015). Typical final formulas consider data from the following areas:
    - Level of preparation, including cybersecurity-related business alignment, strategic context, governance and leadership, investments or resilience and response readiness,
    - Characteristics of historical security incidents,
    - Exposition of cybersecurity risks, given by actual ICT infrastructure, impacts of cyber threats, or portfolio of core businesses.

- Enterprise architecture: structural implementation of strategic management tools and techniques, gradually transforming business processes and organisational structures into particular services, provided by specific IT applications, and running on appropriate technical infrastructure (Moeller, 2013), (Mowbray & Shimonski, 2014), (Dhingra, 2017), (Bhattacharya, 2018). There are numerous applicable frameworks, addressing specific types of management. Because this research dealt mainly with the inclusion of cybersecurity into the governance, strategic planning and change management levels, the following frameworks were of our specific interest:
    - Control Objectives for Information and Related Technology (COBIT) is a direction-level framework, proposed by The Information Systems Audit and Control Association (ISACA) for ICT governance and management (Bartens et al., 2015), (Arief & Wahab, 2016), (Almeida et al., 2018), proposing tools and processes, minimising the gap between technical issues, business risk and process requirements and, consequently, reflecting and supporting business processes. Its mission is to get optimal value from enterprise ICT infrastructure by balancing related benefits, risks and resources. These goals are achieved through the following principles: (i) meeting stakeholder needs, (ii) covering the enterprise end to end, (iii) applying a single integrated framework, enabling a holistic approach and (iv) separating governance from management. Moreover, COBIT scalable structure supports straightforward inclusion of new business processes, including the cybersecurity. Although the main strength of COBIT insists in the direction level, it covers also change management (enterprise architecture) and partially touches also design and management of operations. Because for the business alignment of last two levels is frequently used Information Technology Infrastructure Library (ITIL), companies usually combine both platforms to cover the whole range of business activities equally (Sauve et al., 2006), (Huang et al., 2009), (Hermanto et al., 2019).
    - The Open Group Architecture Framework (TOGAF) is a framework and a set of supporting tools for developing enterprise ICT architecture and aligning it with business objectives (Winter & Fischer, 2006), (Hermawan & Sumitra, 2019), (*The TOGAF® Standard, Version 9.2*, 2020).

It is based on the Architecture Development Method (ADM), which can also accommodate cybersecurity requirements. As an intermediate layer, TOGAF takes requirements from governance and strategic planning and transforms them into the design and implementation matters, convenient for operational, e.g. ITIL-based level.

- From the security architecture point of view, particularly interesting is also Sherwood Applied Business Security Architecture (SABSA) framework, suggesting an optimal methodology for the development of risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives (Coetzee, 2012), (Pleinevaux, 2016).

2 Methods

Although the routine utilisation of knowledge-driven solutions belongs among the most perspective performance drivers, there are still some open questions, related mainly to appropriate ways of their implementation. Beyond the already mentioned representational clarity, practical solutions must be holistic, user-friendly, scalable, intuitive or easily shareable in teams. Logically, also the set of applied tools and techniques must reflect these non-functional requirements. Based on such assumptions, we conducted initial qualitative research, discovering state of the art in knowledge-based inclusion of cybersecurity aspects into standardised strategic planning and management frameworks. Thus, we followed the general principles of system thinking and design, including holism, purposefulness, openness, multidimensionality, hierarchy, interdependence, equilibrium, counterintuitiveness, ambiguity or entropy, introduced and refined, e.g., by (Bertalanffy et al., 2015), (Forrester, 1961), (Sterman, 2014) or (Meadows & Wright, 2015). These aspects were employed in both main phases of the presented research, including knowledge elicitation (Diaper, 1989) and modelling (Firlej & Hellens, 1991). Resultant findings were considered in the context of organisational learning, divided in (Senge, 2006) into the following five disciplines: personal mastery, mental models, shared vision and team learning, integrated through the principles of systems thinking. Organisations with properly implemented learning principles can also profit from knowledge management (Massingham, 2019). As a result, related findings were summarised in the mind map (Buzan, 2018), providing a loosely structured graphical representation of analysed

phenomenon. Due to its visual straightforwardness and clarity, this technique represents an efficient way of representation, communication and sharing of comprehensive outputs of literature review. In parallel, the collected conceptual artefacts are further structured with the system diagram. In contrast to the linearly structured mind map, system diagram already uses feedback loops and more sharply distinguishes between parameters (connections) and state variables (boxes). I

Invented assumptions concerning internal dynamics were incorporated into dynamic hypotheses and modelled with the causal loop diagram. The behaviour of the resultant model was discussed for selected scenarios, the feasibility of which also proves model validity. Thus, the achieved qualitative results and recognised limitations can facilitate managerial decisions and modifying the existing reality. Although the presented outputs were simplified because of their readability in this document, full versions of all modelling diagrams are more comprehensive and serve as resources for currently developed computation model.

3 Results and discussion

3.1 Mind map

The mind map in figure 1 characterises the main pillars of our understanding of the business alignment of cybersecurity. In its left part, the risk related factors are structured into selected types of threats, which can spoil both company data and ICT infrastructure and affect its business processes in different ways with explicitly quantifiable impacts. To minimise their occurrence, duration and consequences, selected aspects of cybersecurity risks must be appropriately included into the existing system of company governance and management, summarised in the right part of the map. It covers the particular levels of governance, extended with related cybersecurity policy and high-level structure for strategic planning and management. Achieved cybersecurity performance, in our case integrated into BSC framework, can be evaluated with a selected metric from the left part.

Then the detailed CS strategy can be composed as a weighted mixture of listed components, to maximise the goals, listed in the underlying branch. It also shows the specific cycle of CS management, which differs from the generic plan, organise, staff, lead and control quintuplet. Finally, structural foundations of EU governance are shown as unavoidable external factors.

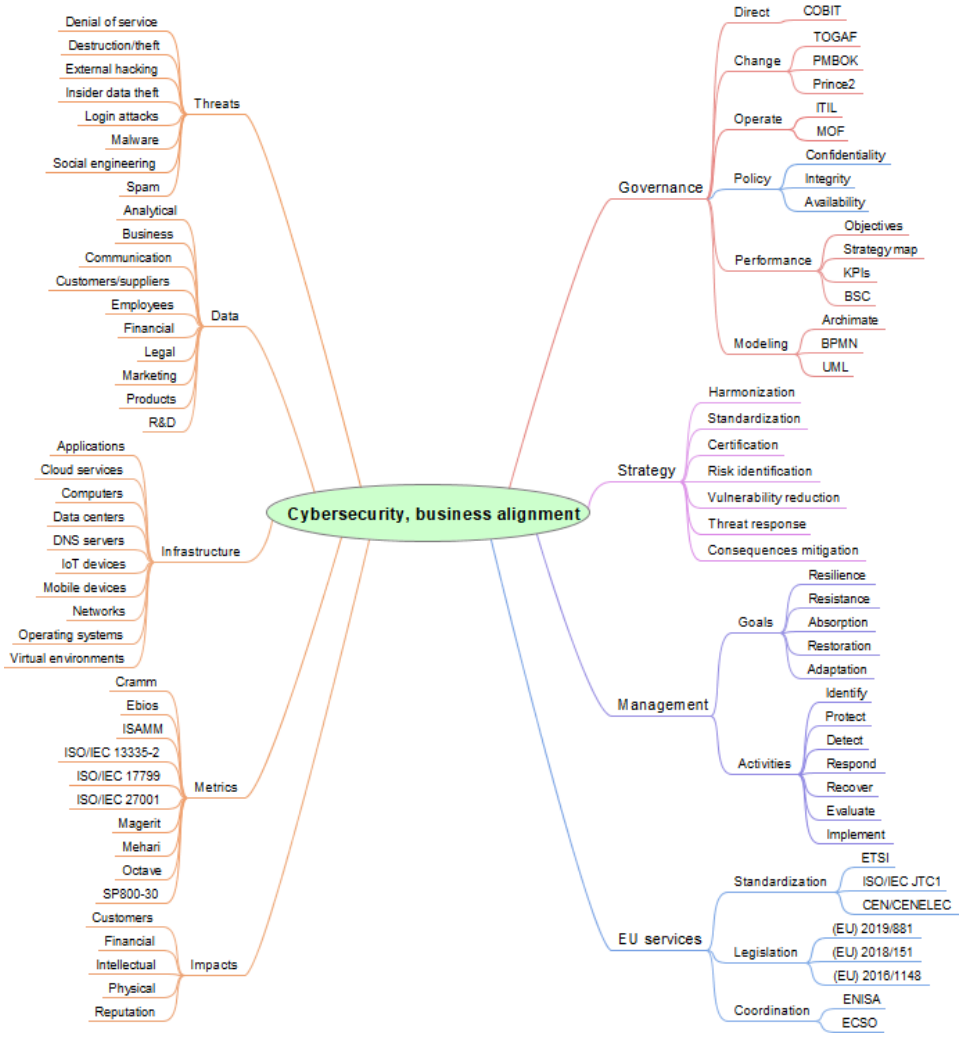

Figure 1 Mind map of analysed domain

3.2 System diagram

Following the adopted way of implementation, figure 2 presents the related system diagram is the system dynamics notation. We extended four BSC sectors with the cybersecurity one because it simultaneously and nontrivially influences segments of customers, operations and learning & growth, and indirectly also finances. The diagram is composed of the following elements:

- Rectangles, stocks or capacities are time-varying state variables, expressed with nouns. Mutually coordinated development of their levels is crucial for the final performance.

- Clouds are dummy external resources, which do not belong to the system.
- Annotated hourglasses are valves, filling or draining the stocks through the oriented double arrows (pipes). Because their turning represents an activity, are expressed with verbs.
- Regular variables without borders are stationary parameters, generally represented with linear or nonlinear functions (risk, utility, subjectivity).
- Oriented single arrows constitute a parametric setting of the system. Double-crossed ones denote considerably slower transfers from start to end.
- Phantom variables in angle brackets only increase the visual clarity of the diagram by removal of possibly intersected graphical elements.

System-level interpretation of BSC considers the main system variables of single sectors as stocks, filled or drained with parametrically controlled valves. Interconnection of subsystems is demonstrated with binding stock levels. Strategic decisions are realised through *Finances*, primarily collected from sold products or services, i.e. *Operations*.

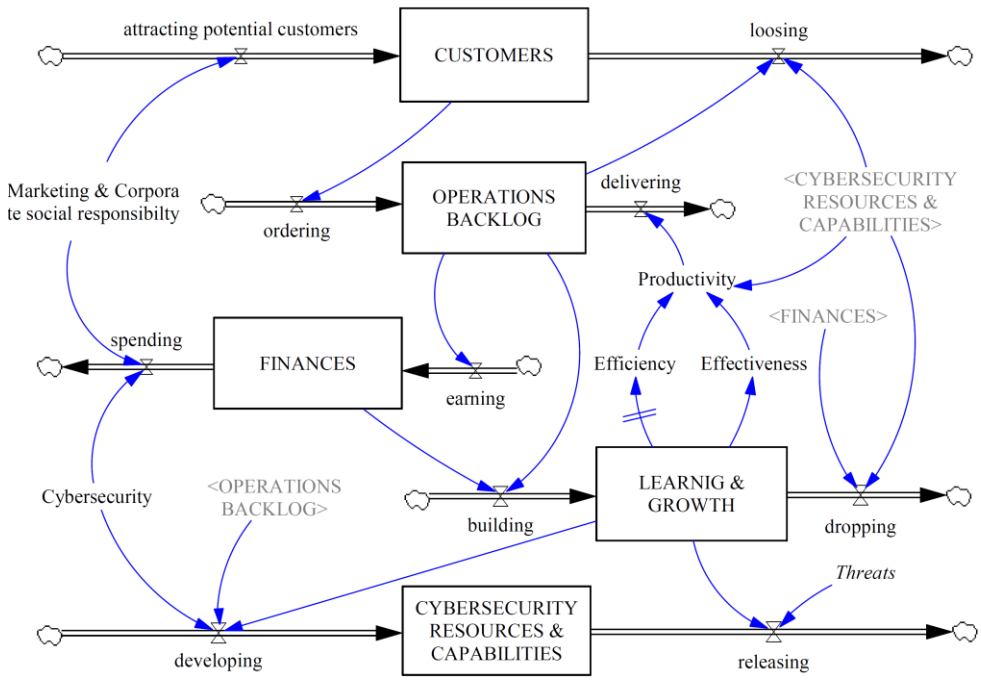

Figure 2 System diagram of cybersecurity in BSC-like performance framework

Thus, the constant level of *Operations* backlog is one of the desirable planning targets. Available level of *Finances* directly determines the most expensive *Learning and growth* subsystem, including both performance drivers (mostly human resources) and infrastructural performance enablers. This sector generates both components of productivity, efficiency and effectiveness, which, altogether with market-related activities, maintain the level of *Customers* and generate backlog. *Cybersecurity* was separated from *Learning and growth* sector, because of its broader impact, which is, moreover, oriented mainly in the opposite direction from the performance. Beyond productivity, cybersecurity incidents can discourage both customers and employees, as well as damage infrastructure or business data.

3.3 Dynamic hypotheses

For simplicity, let us expect that the performance is expressed with a normalised function of quantitative and qualitative indicators from all fours BSC sectors, i.e.,

Performance (Customers, Operations, Learning and growth, Finances) [%],

and its target value should be 100% at the end of the planning period. This situation represents the basal dynamics hypothesis H1 in figure 3. Let us also introduce an overall normalised index of company cybersecurity level (CSI), structured in accordance with the left side of figure 1. This relative indicator can be used in the following ways:

- Independently from performance to provide decision-makers compound information concerning this matter.
- As a part of more or less independent risk management, where the risk is normalised function of threat probability or likelihood, level of vulnerability and impact of consequences, i.e.:

  Risk(exposed CSI).
- Fully integrated into existing performance management framework, which is approach, presented in this paper. In such case, CSI must be distributed into particular BSC sectors.

To illustrate this last option, we considered a scenario, when single cyberattack appeared at the end of the fourth month. With this situation, we interlinked the remaining four dynamic hypotheses, H2 – H5 as follows:

- H2: If company does not systematically invest into own cybersecurity, an average security incident can negatively and irreversibly affect its performance. Although an immediate recovery is possible, the slope of performance graph remains negative until the further managerial event or threat occurrence.
- H3: Even a low level of systematic inclusion of cybersecurity into a performance framework can eliminate performance decrease and preserve its steady level.
- H4: Optimal level of systematic inclusion of cybersecurity into a performance framework can eliminate performance decrease and originate its next growth.
- H5: Extensive level of systematic inclusion of cybersecurity into a performance framework can quickly eliminate performance decrease and originate its next growth. However, this level of security and fast adaptability is expensive, which, it turns, negatively influence the performance. That is why it is generally difficult to overcome a smaller growth slope, caused by extensive investments to cybersecurity.

Exact implementation strategy of particular hypotheses can be derived from the corresponding causal loop diagram, serving as a qualitative dynamic model of integration of cybersecurity into the business.

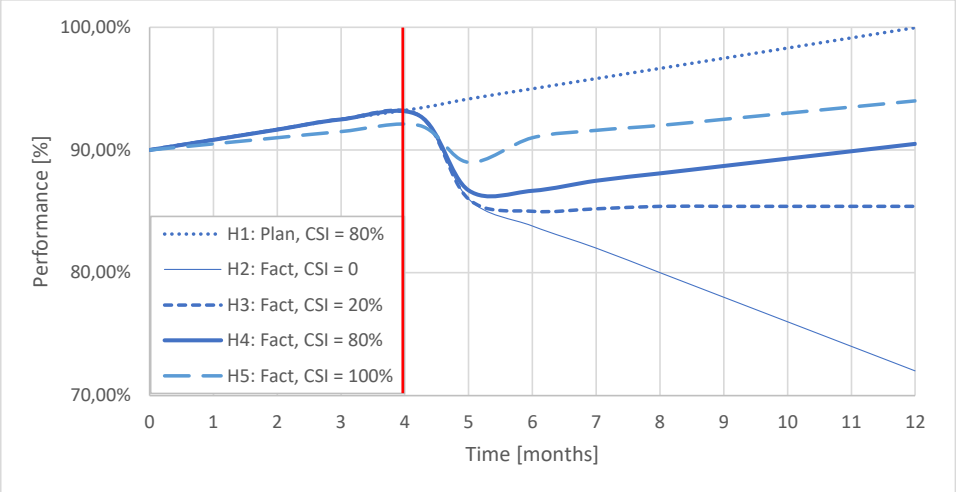

Figure 3 Dynamic hypotheses for sample scenarios and strategies

3.4 Causal loop diagram

The diagram of qualitative dynamics in figure 4 approximately refines the system diagram and suggests conditions, satisfying the above-outlined dynamic hypotheses. Sample resources for strategic decisions are shown in its lower part in the form of several stabilising loops with for clarity omitted settings of desired levels. The exact values of single parameters depend on adopted strategy and are limited mainly with available finances, generated by operations backlog, maintained with an appropriate combination of orders, technology and productivity. Productivity, i.e. input to output conversion ratio, is composed of the quantitative part, including staff and infrastructural changes and the qualitative one, achieving efficiency through organisational learning and development of teamwork and individual capabilities.

The upper right quadrant illustrates sample structure of the cybersecurity sector. It includes own quantitative and qualitative loops, establishing the desired level of resilience and decreasing vulnerability. Marketing focuses purely on the attraction of potential customers. Corporate social responsibility has, however, a broader scope and introduces external Political, Economic, Social, Technological, Environmental and Legal factors (PESTEL) to the model. They can be interpreted, e.g., as a competitive advantage, reputation, customers' satisfaction, interoperability or public awareness. From the dynamic point of view, cybersecurity is included in seven loops, chronologically ordered as follows:

Single balancing loop of strategic planning:

- L1: CS → Resources for strategic decisions → CS

Four reinforcing loops for building and using CS capabilities:

- L2: CS → General CS training → Resilience → Vulnerability → CS
- L3: CS → Specific CS training → Resilience → Vulnerability → CS
- L4: CS → CS staff → Resilience → Vulnerability → CS
- L5: CS → CS architecture, compliance, infrastructure → Resilience → Vulnerability → CS

Two balancing controlling loops:

- L6: CS → Effectiveness → Productivity → Operations backlog → Resources for strategic decisions → CS
- L7: CS → Quality of services Efficiency → Productivity → Operations backlog → Resources for strategic decisions→ CS

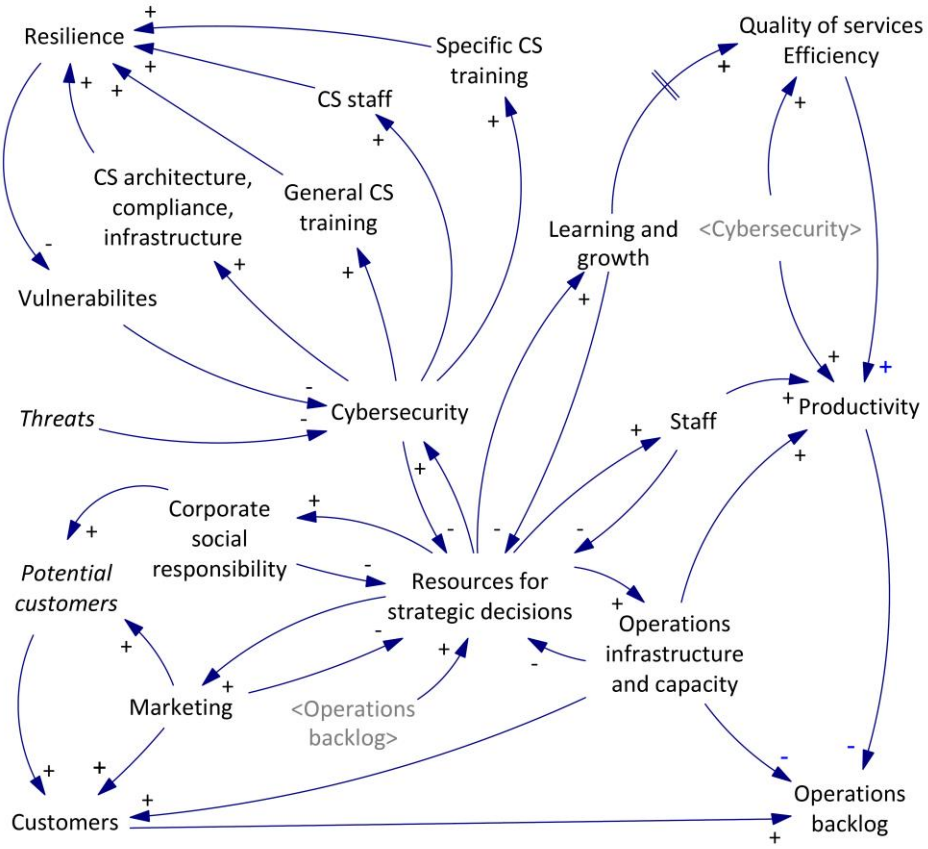

Figure 4 Causal loop diagram summarising dynamics of cybersecurity integration

These loops constitute behaviour, assumed by the specicic dynamic hypotheses:

- H1 represents a sample output from the planning phase, and functionally corresponds with H4. Without external or internal threats, there is no need for any reactive actions, and the performace develops steadily during the whole period.
- H2 does not expect any explicit cybersecurity infrastructure, which means, that loops L1 - L7 are missing. Such solution is cheaper and in a safe environment influences performance positively. However, when an accident happens, a vulnerable system is not prepared for a prompt recovery and loses performance gradually.
- H3 assumes only development of mandatory cybersecurity quantities, represented with the loops L1, L2 and L6. These resources are enough for incident recovery, but cannot guarantee the recurring performance growth.

- H4 benefits from the existence of all cybersecurity loops L1 – L7 and their optimal adjustment. Well-developed qualitative aspects of cybersecurity through loops L3 - L5 and L7 result at least in a renewal of original growth. Additional managerial decisions can this situation even improve.
- H5 is the opposite extreme to H2. Excessive level of cybersecurity is a costly alternative, restricting performance growth because of budget limitations. On the other hand, minimisation of impacts and fast recovery are its evident advantages.

4 Conclusions

This research provides a qualitative dynamic analysis of an enterprise cybersecurity inclusion into a standardised performance framework. Its main goal was to propose a knowledge-based interconnection of technical and business aspects of the studied phenomenon. Practically it means that traffic data, outputs of network analysing tools as well as cybersecurity-related technical knowledge and threat intelligence are integrated into particular key performance indicators. In parallel, employees are educated in cybersecurity matters and trained to identify and mitigate cybersecurity risks early. Such a joint approach can result in a generally understood, systemically governed and safe growth of the business, capable to minimise consequences of incidents and efficiently reflect a continuous expansion of external and internal threats.

To establish such framework, we adopted the dynamic system approach and reviewed the latest related resources. Collected conceptual information was modelled and gradually structured using the mind map and system diagram. Then we proposed five dynamic hypotheses and justified them through the related causal loop diagram. The main findings were:

- Because of the fast dynamics of cybersecurity, caused by technological development, increasing diversity and frequency of cyberattacks, companies must be able to adopt systemic, scalable, transparent and well-justified, preferably knowledge-based solutions.
- From the governance point of view, cybersecurity represents a specific area of interest, directly or indirectly addressing all standard sectors of performance. That is why it cannot be merged with existing processes and requires specific structural arrangements.

- Strategic management of cybersecurity requires should be based on compound metrics, summarising its quantitative and qualitative aspects.
- Adequately unsecured organisations can face significant problems even after a single attack. On the other hand, massive cybersecurity investments slow down core business development. Optimal system of cybersecurity management has well-balanced its effectiveness and efficiency components.

Finally, the main advantage of knowledge-based modelling insists in its ability to find key behavioural features in the context of the whole system, identify counterintuitive patterns or simplify and visualise multidimensional nonlinear and delayed relations. Realistic transformation of real-world problems into a software form also establishes an intuitive platform for acquisition and sharing of knowledge among distributed research teams and supports professional education and training. Thus, the obtained qualitative model currently serves as a group decision-support tool, based entirely on domain knowledge and primarily validated with expert opinions. Its is intuitive and scalable architecture supports its continuous development. Our future research will concentrate mainly on the quantitative system dynamics implementation of the presented qualitative concept.

Acknowledgments

This research was supported by the Ministry of Education, Youth and Sports of the Czech Republic within the INTER-EXCELLENCE program under the project LTAB 19021 *Czech-German Cross-Border Situational Awareness for Critical Infrastructures* .

References

Abu, M., Rahayu, S., Ariffin (DrAA), D. A., & Robiah, Y. (2018). Cyber threat intelligence – Issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10, 371–379. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Almeida, R., Lourinho, R., Silva, M. M. da, & Pereira, R. (2018). A Model for Assessing COBIT 5 and ISO 27001 Simultaneously. 2018 IEEE 20th Conference on Business Informatics (CBI), 01, 60–69. https://doi.org/10.1109/CBI.2018.00016

Arief, A., & Wahab, I. H. A. (2016). Information technology audit for management evaluation using COBIT and IT security (Case study on Dishubkominfo of North Maluku Provincial Government, Indonesia). 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), 388–392. https://doi.org/10.1109/ICITACEE.2016.7892477

Arumugam, S., & Subramanian, S. (2019). A Review on Cyber Security and the Fifth Generation Cyberattacks. Oriental journal of computer science and technology, 12, 50–56. https://doi.org/10.13005/ojcst12.02.04

Badawy, M., El-Aziz, A. A. A., Idress, A. M., Hefny, H., & Hossam, S. (2016). A survey on exploring key performance indicators. Future Computing and Informatics Journal, 1(1), 47–52. https://doi.org/10.1016/j.fcij.2016.04.001

Bartens, Y., Haes, S. d, Lamoen, Y., Schulte, F., & Voss, S. (2015). On the Way to a Minimum Baseline in IT Governance: Using Expert Views for Selective Implementation of COBIT 5. 2015 48th Hawaii International Conference on System Sciences, 4554–4563. https://doi.org/10.1109/HICSS.2015.543

Bertalanffy, L. von, Hofkirchner, W., & Rousseau, D. (2015). General System Theory: Foundations, Development, Applications (1 edition). George Braziller Inc.

Bhattacharya, P. (2018). Aligning Enterprise Systems Capabilities with Business Strategy: An extension of the Strategic Alignment Model (SAM) using Enterprise Architecture. Procedia Computer Science, 138, 655–662. https://doi.org/10.1016/j.procs.2018.10.087

Bland, J. A., Petty, M. D., Whitaker, T. S., Maxwell, K. P., & Cantrell, W. A. (2020). Machine Learning Cyberattack and Defense Strategies. Computers & Security, 92, 101738. https://doi.org/10.1016/j.cose.2020.101738

Brusoni, S., Vaccaro, A., & Veloso, F. (2009). The impact of virtual technologies on knowledge-based processes: An empirical study. Research Policy, 38, 1278–1287. https://doi.org/10.1016/j.respol.2009.06.012

Bunker, G. (2020). Targeted cyber attacks: How to mitigate the increasing risk. Network Security, 2020(1), 17–19. https://doi.org/10.1016/S1353-4858(20)30010-6

Buzan, T. (2018). Mind Map Mastery: The Complete Guide to Learning and Using the Most Powerful Thinking Tool in the Universe. Watkins Publishing.

Coetzee, M. (2012). Towards a Holistic Information Security Governance Framework for SOA. 2012 Seventh International Conference on Availability, Reliability and Security, 155–160. https://doi.org/10.1109/ARES.2012.62

Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, Pub. L. No. 32018R0151, 026 OJ L (2018). http://data.europa.eu/eli/reg_impl/2018/151/oj/eng

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in Industry, 114, 103165. https://doi.org/10.1016/j.compind.2019.103165

Dhingra, M. (2017). Enterprise Security Architecture. IJSER.

Diaper, Dan. (1989). Knowledge elicitation: Principles, techniques and applications. Ellis Horwood [etc.]; /z-wcorg/.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 32016L1148, EP, CONSIL, OJ L 194 (2016). http://data.europa.eu/eli/dir/2016/1148/oj/eng

Domínguez, E., Pérez, B., Rubio, Á. L., & Zapata, M. A. (2019). A taxonomy for key performance indicators management. Computer Standards & Interfaces, 64, 24–40. https://doi.org/10.1016/j.csi.2018.12.001

Egbuhuzor, C., & Port, R. (2019, srpen 17). Target costing and value engineering. https://doi.org/10.13140/RG.2.2.16410.39363

Elmaghraby, A., & Losavio, M. (2014). Cyber Security Challenges in Smart Cities: Safety, security and privacy. Journal of Advanced Research, 5. https://doi.org/10.1016/j.jare.2014.02.006

Firlej, Maureen., & Hellens, Dave. (1991). Knowledge elicitation: A practical handbook. Prentice-Hall; /z-wcorg/.

Fitzgerald, T. (2020). CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers (1 edition). Auerbach Publications.

Forrester, J. W. (1961). Industrial dynamics. M.I.T. Press; /z-wcorg/.

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50, 101660. https://doi.org/10.1016/j.scs.2019.101660

Hermanto, A., Kusnanto, G., & Supangat. (2019). Developing Sociopreneurship Business Incubator Using ITIL to Improve Competitiveness Advantage. 2019 Fourth International Conference on Informatics and Computing (ICIC), 1–6. https://doi.org/10.1109/ICIC47613.2019.8985793

Hermawan, R., & Sumitra, I. (2019). Designing Enterprise Architecture Using TOGAF Architecture Development Method. IOP Conference Series: Materials Science and Engineering, 662, 042021. https://doi.org/10.1088/1757-899X/662/4/042021

Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. Procedia Manufacturing, 44, 655–662. https://doi.org/10.1016/j.promfg.2020.02.243

Huang, Z., Zavarsky, P., & Ruhl, R. (2009). An Efficient Framework for IT Controls of Bill 198 (Canada Sarbanes-Oxley) Compliance by Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002. 2009 International Conference on Computational Science and Engineering, 3, 386–391. https://doi.org/10.1109/CSE.2009.336

International Organization for Standardization ISO/IEC 13335-1:2004. (2004). International Organization for Standardization ISO/IEC 13335-1:2004. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/90/39066.html

ISO/IEC 27002:2005. (2005). ISO/IEC 27002:2005. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/02/50297.html

ISO/IEC 27002:2013. (2013). ISO/IEC 27002:2013. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54533.html

ISO/IEC 30111:2019. (2019). ISO/IEC 30111:2019. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/97/69725.html

Kaplan, R. S., & Norton, D. (2005). The Balanced Scorecard: Measures that drive performance. Harvard business review, 83, 172-+.

Kiran, D. R. (2017). Chapter 33—Value Engineering. In D. R. Kiran (Ed.), Total Quality Management (s. 455–470). Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-811035-5.00033-7

Lai, L. F. (2007). A knowledge engineering approach to knowledge management. Information Sciences, 177(19), 4072–4094. https://doi.org/10.1016/j.ins.2007.02.028

Leszczyna, R. (2018). A review of standards with cybersecurity requirements for smart grid. Computers & Security, 77, 262–276. https://doi.org/10.1016/j.cose.2018.03.011

Lewis, T. G., Darken, R. P., Mackin, T., & Dudenhoeffer, D. (2012). Model-based risk analysis for critical infrastructures. In F. Flammini (Ed.), WIT Transactions on State of the Art in Science and Engineering (Verze 1, 1. vyd., Roč. 1, s. 3–19). WIT Press. https://doi.org/10.2495/978-1-84564-562-5/01

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

Li, G., Shen, Y., Zhao, P., Lu, X., Liu, J., Liu, Y., & Hoi, S. C. H. (2019). Detecting cyberattacks in industrial control systems using online learning algorithms. Neurocomputing, 364, 338–348. https://doi.org/10.1016/j.neucom.2019.07.031

Malhotra, M., & Nair, T. R. (2015). Evolution of Knowledge Representation and Retrieval Techniques. International Journal of Intelligent Systems and Applications, 7, 18–28. https://doi.org/10.5815/ijisa.2015.07.03

Massingham, P. (2019). Knowledge Management. SAGE Publications Ltd. https://uk.sagepub.com/en-gb/eur/knowledge-management/book249007

Meadows, D. H., & Wright, D. (2015). Thinking in systems: A primer. /z-wcorg/.

Moeller, R. R. (2013). Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL (1 edition). Wiley.

Mowbray, T. J., & Shimonski, Robert. (2014). Cybersecurity: Managing systems, conducting testing, and investigating intrusions. John Wiley & Sons; /z-wcorg/. http://www.books24x7.com/marc.asp?bookid=58142

Nielsen, S., & Nielsen, E. (2013). Transcribing the balanced scorecard into system dynamics: From idea to design. Int. J. of Business and Systems Research, 7, 25–50. https://doi.org/10.1504/IJBSR.2013.050618

Pala, A., & Zhuang, J. (2019). Information Sharing in Cybersecurity: A Review. Decision Analysis, 16(3), 172–196. https://doi.org/10.1287/deca.2018.0387

Pleinevaux, P. (2016, září 1). Towards a metamodel for SABSA Conceptual Architecture Descriptions.

Rawat, D., B., & Ghafoor, K., Z. (2019). Smart Cities Cybersecurity and Privacy. Elsevier. https://doi.org/10.1016/C2017-0-02545-4

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), Pub. L. No. 32019R0881, 151 OJ L (2019). http://data.europa.eu/eli/reg/2019/881/oj/eng

Sammut-Bonnici, T., & Galea, D. (2015). PEST analysis. https://doi.org/10.1002/9781118785317.weom120113

Sánchez, H. S., Rotondo, D., Escobet, T., Puig, V., & Quevedo, J. (2019). Bibliographical review on cyber attacks from a control oriented perspective. Annual Reviews in Control, 48, 103–128. https://doi.org/10.1016/j.arcontrol.2019.08.002

Sauve, J., Moura, A., Sampaio, M., Jornada, J., & Radziuk, E. (2006). An Introductory Overview and Survey of Business-Driven IT Management. 2006 IEEE/IFIP Business Driven IT Management, 1–10. https://doi.org/10.1109/BDIM.2006.1649205

Senge, P. M. (2006). The fifth discipline: The art and practice of the learning organization. Doubleday/Currency; /z-wcorg/.

Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. Computers & Security, 92, 101761. https://doi.org/10.1016/j.cose.2020.101761

Sofiyabadi, J., & Nasabb, S. (2012). A dynamic balanced scorecard for identification internal process factor. Management Science Letters, 2, 1721–1730. https://doi.org/10.5267/j.msl.2012.04.015

Sterman, J. D. (2014). Business dynamics: Systems thinking and modeling for a complex world. Irwin; /z-wcorg/.

The TOGAF® Standard, Version 9.2. (2020, červen 9). https://pubs.opengroup.org/architecture/togaf9-doc/arch/

Wagner, T., Mahbub, K., Palomar, E., & Abdallah, A. (2019). Cyber Threat Intelligence Sharing: Survey and Research Directions. Computers & Security, 87, 101589. https://doi.org/10.1016/j.cose.2019.101589

Williams, M. A., Barranco, R. C., Naim, S. M., Dey, S., Shahriar Hossain, M., & Akbar, M. (2020). A vulnerability analysis and prediction framework. Computers & Security, 92, 101751. https://doi.org/10.1016/j.cose.2020.101751

Winter, R., & Fischer, R. (2006). Essential Layers, Artifacts, and Dependencies of Enterprise Architecture. 2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06), 30–30. https://doi.org/10.1109/EDOCW.2006.33

Yihong, W., Pingye, T., & Binchao, D. (2019). Research on Value Engineering System of Modern Engineering Project. Proceedings of the 2019 2nd International Conference on Information Management and Management Sciences, 101–105. https://doi.org/10.1145/3357292.3357324