

STRATEGIC CYBERSECURITY MANAGEMENT

Ionuț-Claudiu POPA ^{*a}, *Marian NĂSTASE* ^b, *Raluca-Giorgiana (CHIVU) POPA* ^c

^{a, b, c} *Bucharest University of Economic Studies*

ABSTRACT

Cybersecurity, as well as its management, is a broad issue facing organizations today. The latter must undertake the necessary measures to deal with these threats through complex management processes. Emphasis is placed on placing cyber security management in a strategic context so that the decision-making process on cyber security management enables vital individuals, such as the cyber security manager, in unison with other senior managers, to identify and solve cyber security issues. Problems by designing and implementing appropriate countermeasures that prevent cyber attacks. By accepting that cyber security is a shared responsibility, the cyber security manager can work with managers from various organizations and ensure that a unified approach is taken to counter the different cyber attacks.

Through this article, we emphasize the importance of strategic management at the organizational level, especially in the current context, when the valences of cyber security are extremely important at the organizational level. In this article, we have carried out quantitative research in the form of a questionnaire, and among the objectives can be listed: analyzing the opinions of some Romanian specialists on how strategic management evolves in the implementation of new technologies, highlighting the best tools that are used in this process and what are the perspectives regarding the implementation of new technologies

KEYWORDS: *cybersecurity, development, security tools, strategic management.*

DOI: 10.24818/IMC/2022/03.15

1. INTRODUCTION

Strategic Cyber Security Management is distinct in that it contains references to policies, systems and procedures that will enable students, researchers and practitioners to understand the complexity of cybersecurity management and how the subject is evolving. The main objective of cyber security management, and indeed the job of the cyber security manager, is to put in place organizational structures that make an organization more resilient and enable managers to better deal with different forms of cyber attack.

How much knowledge an individual has about cyber attacks and how and why they are launched in an organization should bode well for the ability to anticipate events and work with people with a similar mindset to develop long-term solutions to a recurring problem. Identifying and dealing with a range of cyber threats, with varying levels of risk intensity, means adopting a proactive cyber security management approach that benefits the organization and the organizations it does business with. Recognizing that a cyber security manager fulfils a vital and high-level role within an organization should ensure that the focus is on making the organization more resilient in terms of its business operations and connectivity and is less vulnerable to attack through a supply chain partner.

* Corresponding author: *claudiu.popa@mk.ase.ro*

Government officials, managers and people in society realize that the threat from cyber attacks is increasing, and criminals are becoming more sophisticated in defrauding people for financial gain. Individuals and all types of organizations are at risk, whether in the public or private sector and charities, in particular, have been targeted in recent years. With this in mind, an argument can be made for members of society to be more aware of the threats posed by cybercriminals and to be more fully involved in cybercrime prevention. Therefore, a stakeholder approach to the issue that views cybersecurity as a shared, collectivist responsibility can be advocated. The advantage of a collectivist approach is that it will provide a central focus that mobilizes the expertise of cybersecurity personnel under the guidance of a cybersecurity manager so that government and industry resources can be leveraged and bring people together. to counter the different types of cyber-attacks that are launched. As the actions of cybercriminals are thwarted, successful cybersecurity initiatives should be highlighted to provide insights into how a cybersecurity policy and strategic framework can be improved through the actions of the general public. To justify this, stakeholder theory is referred to, and a collectivist view is presented with practical, every day and policy implications. Various real examples of cyber attacks are referred to convince people that a collectivist approach to the problem is needed.

The Internet and social media are impacting how people interact with each other and the information they share as they go about their daily activities. Indeed, the Internet is seen as a relationship-building facilitator that helps managers modify business processes and revise the company's business model, improve the use of customer information, and streamline supply chain activities (Lichtenthal & Eliaz, 2003; Makkonen & Vuori, 2014). Through improved connectivity, rapid interaction occurs between personalized individuals, enabling information acquisition and enhanced distribution and storage (Walters, 2008). Future developments in the use of communication technology are likely to influence how individuals in society respond to events, engage with and share information, respond to the news, whether genuine or fake and become influential in writing reviews. This is because, e.g. Key influencers in organizations, professional bodies, and institutions are likely to increase their engagement with the government and demand that government departments take a proactive approach to addressing cybersecurity threats as they materialize.

2. CYBERSECURITY MANAGEMENT

The cybersecurity policy and strategic framework presented in this chapter are derived from an analysis of attacks on a computer system and network and two critical peer groups involving highly experienced intelligence personnel, security personnel, and academics. The findings suggest that cyber security should be placed in the context of an organization's corporate social responsibility program. By imbuing a collectivist spirit, stakeholders can be identified and grouped accordingly so that specific trust-based relationships are formed that ensure that all the world in the community remains. They are focused on countering the actions of cybercriminals. There is no doubt that cyber security is a complex topic that will continue to be a high priority in testing management judgment and will remain on top management's agenda. Recognizing that cybercrime affects everyone, it should be possible to foster increased engagement to strengthen government-to-government relationships. Business takes the lead in designing and implementing a broad set of cybersecurity initiatives. Accepting that organizations can be at the heart of a cyber security awareness program bodes well because it allows for uniformity in what needs to be done and by whom. By embracing the spirit of collectivism, stakeholders can be identified and grouped accordingly. Relationships based on trust can be developed to ensure that everyone remains focused on one central goal, which is counter cybercriminals' actions.

A cybersecurity strategy is a high-level plan for securing your company's assets over the next three to five years. Because technology and cyber dangers are constantly evolving, you will almost probably

need to revise your approach sooner than three years from now. A cybersecurity plan is not intended to be perfect; rather, it is a well-informed judgment as to what you should do. Your strategy should grow in tandem with your organization and the environment around you.

The goal of establishing and implementing a cybersecurity plan is to make your assets more secure. This often entails shifting from a reactive to a proactive strategy to security, with an emphasis on preventing cyber assaults and incidents rather than responding to them after the fact. Solid cybersecurity strategy, on the other hand, will better prepare firms to respond to crises that do occur. Furthermore, by averting minor events, businesses may protect their brand and minimize harm to employees, customers, stakeholders, partners, and others.

How do you create a cybersecurity plan for your company?

Developing a cybersecurity strategy for your company requires time and work, but it might mean the difference between outperforming your competitors and going out of business. Here are the fundamental steps to developing an effective security strategy.

Step 1: Analyze your cyber threat landscape.

Before you can grasp your cyber threat landscape, you must first investigate the cyber-attacks that your firm is now facing. What types of cyber threats are now wreaking the most havoc on your organization: malware, phishing, insider threats, or something else? Have your competitors recently experienced big incidents, and if so, what threats did they pose?

Then, be abreast of projected cyber threat trends that may affect your firm. Many security researchers, for example, predict ransomware will become a big issue if ransomware businesses thrive. Furthermore, there is rising worry about supply chain vulnerabilities generated, for example, by purchasing tainted components and either employing them within your firm or incorporating them into the products you sell to consumers. Understanding future cybersecurity threats and their potential severity is critical to developing a successful cybersecurity plan.

Step 2: Determine your cybersecurity maturity.

Once you understand what you're up against, you must assess your organization's cybersecurity maturity honestly. Choose a cybersecurity framework, such as the NIST Cybersecurity Framework, first. First, use it to evaluate your organization's maturity in hundreds of categories and subcategories, ranging from policies and governance to security technology and incident recovery skills. This evaluation should cover all of your technologies, including traditional IT, operational technology, IoT, and cyber-physical systems.

Then, using the same cybersecurity framework, determine where your firm should be in terms of maturity for each category and subcategory in the next three to five years. If distributed denial-of-service assaults, for example, are going to be a big danger, your network security skills should be extremely advanced. If ransomware is the most serious security issue, making sure your backup and recovery mechanisms are mature is vital. If COVID-19-driven remote work practices become permanent at your firm, the temporary tools put in place during the pandemic must be strengthened. Your new strategic goals are the maturity levels you are aiming towards.

Step 3: Identify ways to strengthen your cybersecurity program.

You need to find out what cybersecurity tools and capabilities will help you get there now that you've set a baseline and identified where you want to go. Determine ways to strengthen your cybersecurity program to fulfill the strategic goals you've set. Each upgrade will require resources such as money and staff effort. You will need to explore many possibilities for accomplishing your goals, as well as the benefits and drawbacks of each option. You may, for example, elect to outsource some or all of your security tasks.

Step 4: Write down your cybersecurity strategy.

Once your cybersecurity strategy has been approved by management, you must ensure that it is fully documented. This includes creating or revising risk assessments, cybersecurity strategies, rules, guidelines, and processes, as well as anything else required to describe what is required or suggested to achieve strategic goals. Again, it is essential to be clear about each person's responsibilities.

A practical organizational strategic governance framework must incorporate a set of procedures, plans and systems that enable the cyber security manager to identify where a cyber attack has been launched, initiate an appropriate response and liaise with internal staff and properly externally to ensure that the attack gets as much media coverage as possible. As cyber-attacks are launched from different parts of the world and can affect an organization at any time, a cyber attack must be recorded so that various government bodies and agencies can be informed about the trend. Through sharing information about cyber threats, the cyber security manager and senior management can establish appropriate management and organizational and structural responses and ensure that the damage is limited if a cyber attack affects the organization. Furthermore, the fact that cyber attacks are becoming increasingly sophisticated emphasizes the cyber security manager to record the full details in the organization's memory so that the cyber attack countermeasures in place within the partnership agreement can be proactively managed and analyzed by external experts/auditors. This again focuses on the fact that to have adequate countermeasures; employees must be aware of the different types of cyber attacks launched against an organization and have the appropriate knowledge and skills (Baker, 2010) to respond in active mode. The attack. The cyber security knowledge and skills required to repel an attack can be defined in terms of system forensics knowledge; network forensics; deep pocket facilities; Windows; UNIX; PDA defence configurations; log analysis; script development; exploitation and penetration testing; service coding; reverse engineering and counterintelligence (Paller, 2010).

Business continuity management is often seen as something managers have to do without a clear overview of what is involved and who is assigned to do it. This means that business continuity management is seen as necessary but often designated as an administrative role instead of an operational one because most of the impacts they have on an organization are superficial. Both the business continuity management process and the business continuity manager are receiving increased attention, however, because a successful cyber attack will result in an impact that affects the functioning of an organization and could lead to reputational damage. Therefore, for the business continuity management planning framework in place to be considered adequate for the type and severity of a cyber attack, the cyber security manager must ensure that senior management is aware of several factors, including organizational. and structural issues related to business model vulnerability; resource availability implications related to data and information exchange; factors specific to the operation within the partnership agreement; and legal and ethical considerations relating to the countries in which the partnership agreement operates. The appropriate business continuity management planning framework requires the cybersecurity manager to cooperate with managers based on industry partners and various external stakeholders. As a result, all of them subscribe to the concept of business continuity management planning. To be effective, the necessary contingency plans must be in place, and the contingency planning process must ensure that business recovery is at the heart of the process. To facilitate this approach, managers with a low-probability, the high-impact mindset must establish and support a security culture.

Rid and McBurney (2012) are firm in their view of what constitutes a cyber threat and what a cyber weapon is. Cyber weapons can be grouped according to their potential to cause damage, which can be viewed from a psychological and a physical perspective. Looking to the future of cyberweapons, Rid and McBurney (2012: 10) state: "It would be surprising if a coded smart weapon capable of learning had not yet been developed. A learning weapon could autonomously observe and assess the specifics of an isolated environment, analyze available courses of action, and take action." This is appealing because artificial intelligence and machine learning are critical aspects of cyber security management, which must increasingly encompass a geo-political and technological dimension. With this in mind, the cybersecurity manager must answer the following question: How can the organization's leadership model be aligned with the nation's political leadership model in cybersecurity defence? Longstaff et al. (2010: 7) have provided insight into this and are correct to suggest that leadership can be seen as a 'vital community resource' and used to produce innovation and learning. Longstaff et al. (2010: 9)

suggest that: "When a community has a high level of all three features - institutional memory, inventive learning, and connectivity - it has a great capacity to adapt to environmental changes". The reason an organization needs a robust resilience policy is because of the "complex consideration of threatening events, interdependencies with other infrastructures, and the impact of human behaviour on systems performance" (Steinberg et al., 2011, p. 28). In addition, top management must ensure that they adapt the organization's security policies according to received threat intelligence and can mitigate threats in real time (Anand et al., 2012).

Corporate social responsibility in cybersecurity

Perspective on Social Cybersecurity-Social cybersecurity is an emerging scientific field that focuses on characterizing, understanding, and forecasting cyber-mediated changes in human behavior and social, cultural, and political outcomes, as well as developing the cyberinfrastructure required for society to retain its essential character. Current or potential social cyber risks arise in a cyber-mediated information ecosystem under changing conditions. An example is a technology and theory needed to assess, predict, and mitigate community influence and manipulation through changes or control of the cyber-mediated information environment through cogs, cyborgs (bot-human combination), and humans. The viewpoint that we must maintain and protect a free and open information environment in which ideas may be freely exchanged, the source of information is known, disinformation and false data are identified and reduced, and technology is not used to distort is central to this discipline. This is based on the idea that the flow of information should not compromise infrastructure and that actors should not be able to compromise the cyber environment in such a way as to influence or manipulate individuals, groups and communities unduly. The events that need to be prevented include the viral retweeting of messages containing images that, if downloaded, launch malware or bots to manipulate groups into accepting fake news as accurate. In cybersecurity, much of the focus has been on attacks on and through cyberinfrastructure designed to disrupt technology, steal or destroy information, and steal money or identities. Instead, in cyber social security, the focus is on influencing or manipulating individuals, groups or communities and thus affecting their behaviours, emphasizing socio-political-cultural consequences.

Questionnaire

Through this questionnaire, we aim to identify the opinion of Romanian specialists regarding the implementation process of the new processes related to strategic management, especially in the current context of the valence of information security. It is also important to emphasize that this research is a primary part of a much more extensive analysis.

In this article, the research was based on a sample of 50 people and had as a research instrument a questionnaire consisting of 21 questions, five of which were classified and identified. In Romania, this was done between June and September 2022 by sending the questionnaire to public and private company specialists. This questionnaire was applied through Google Forms.

1. Is the use of strategic management critical in Romanian entities?

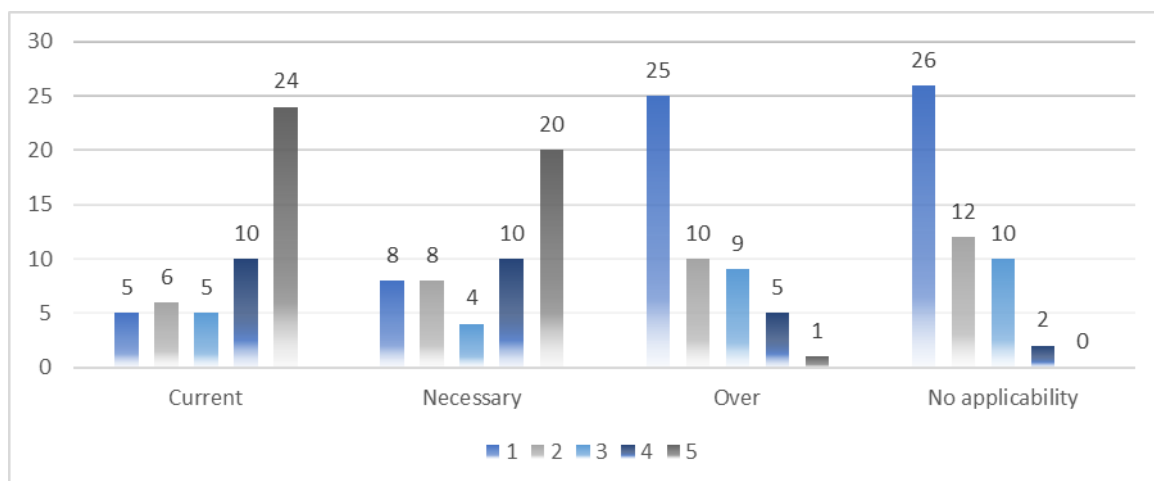


Figure 1. The use of strategic management in Romania

Source: The authors

- 1.Current : $1 \times 5 + 2 \times 6 + 3 \times 5 + 4 \times 10 + 5 \times 24 = 3.84$
- 2.Required: $1 \times 8 + 2 \times 8 + 3 \times 4 + 4 \times 10 + 5 \times 20 = 3.52$
- 3.Over: $1 \times 25 + 2 \times 10 + 3 \times 9 + 4 \times 5 + 5 \times 1 = 1.94$
- 4.No applicability: $1 \times 26 + 2 \times 12 + 3 \times 10 + 4 \times 2 + 5 \times 0 = 1.76$

In the opinion of specialists from our country, it is essential to use strategic management in Romanian entities. As can be seen from the results, the "current " answer obtained the best score - 3.84, and the "necessary" answer was ranked second. Also, this question highlighted that it is no longer effective that a strategic management system is no longer implemented in companies.

2. Given the current cybersecurity context, how do you perceive the implementation processes of strategic management in public/private entities?

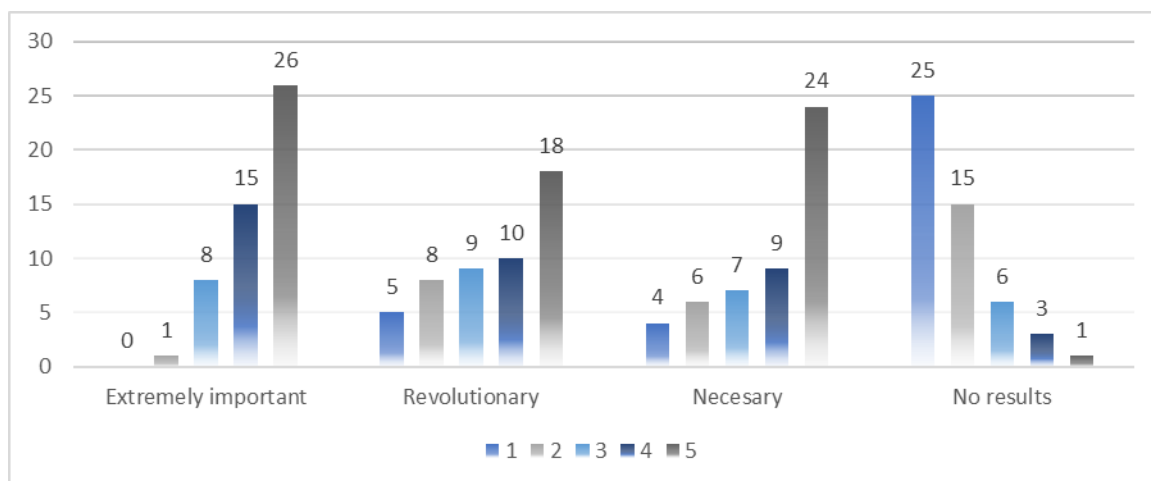


Figure 2. The implementation of cybersecurity in Romania

Source: The authors

- 1.Extremely important : $1 \times 0 + 2 \times 1 + 3 \times 8 + 4 \times 15 + 5 \times 26 = 4.32$
- 2.Revolutionary: $1 \times 5 + 2 \times 8 + 3 \times 9 + 4 \times 10 + 5 \times 18 = 3.56$
- 3.Required: $1 \times 4 + 2 \times 6 + 3 \times 7 + 4 \times 9 + 4 \times 24 = 3.86$
- 4.No result: $1 \times 25 + 2 \times 15 + 3 \times 6 + 4 \times 3 + 5 \times 1 = 1.8$

The diversity of actions taken globally in 2022 is increasing, and the cyber security segment is no exception. It can be seen that the management processes in this activity segment are primarily critical (4.32), necessary (3.86) and revolutionary (3.56). Perceptions such as that they would have no results do not represent a valid option for Romanian specialists, the result for this variable being very low compared to the others – 1.8.

3. What methods are used to implement sustainable solutions related to cybersecurity in terms of strategic management?

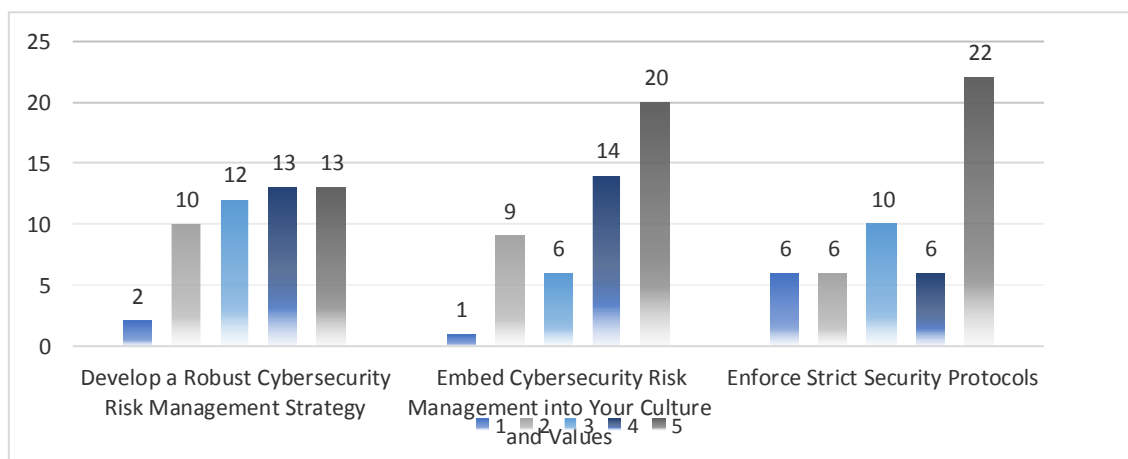


Figure 3. Methods are used to implement sustainable solutions

Source: The authors

- 1) 1.Develop a robust cybersecurity risk management strategy : $1 \times 2 + 2 \times 10 + 3 \times 12 + 4 \times 13 + 5 \times 13 = 3.50$
- 2) 2.Embed cybersecurity risk management into your culture and values: $1 \times 0 + 2 \times 9 + 3 \times 6 + 4 \times 16 + 5 \times 20 = 3.86$
- 3) 3.Enforce strict security protocols: $1 \times 6 + 2 \times 6 + 3 \times 10 + 4 \times 6 + 5 \times 22 = 3.64$

As seen in the previous graph, the specialists' position is vast and diverse when the methods of improving strategic management from the cyber perspective are analyzed. However, most believe that the best perspective lies in developing the organizational culture and implementing their risk management system - a score of 3.86. Also, the score obtained by the other two questions reinforces the previously mentioned idea, namely the improvement of security procedures – 3.64 and the development of one's cyber strategy – 3.50.

3. CONCLUSIONS

Strategic management is essential in the implementation and development process for organizations in Romania and all over the world. However, considering the premises of all actions in the online environment in the last period, a need for developing strategic management in cybersecurity is clearly emphasized.

The values under which strategic management is developed at the organizational level differ wherever it is implemented. Therefore, the last decade emphasized that its implementation processes were interwoven with all kinds of technological elements, which in the general sense, contribute decisively to the improvement of all processes at the organizational level.

Finally, it is essential that at the level of each entity, its analysis and control tools related to strategic management are developed to observe the direction towards which the company is heading. Also, through the new technical solutions available in Romania and worldwide, processes have been extensively developed, creating new opportunities and perspectives for organizational evolution. At the same time, the processes developed at this moment in the area of cybersecurity are only at the beginning, and the following years will consecrate an exponential evolution of this field. (12 pt)

REFERENCES

- Baker, J. (2010). *Talk at the Cyber Security Challenge UK*, University College London (26th July).
- Lichtenthal, J. D., and Eliaz, S. (2003). *Internet integration in business marketing tactics*. *Industrial Marketing Management*, 32(1): 3–13. PII: S0019–8501(01)00198-5.
- Longstaff, P. H., Armstrong, N. J., Perrin, K., Parker, W. M., and Hidek, M. A (2010). Building resilient communities: A preliminary framework for assessment. *Homeland Security Affairs*, 6 (September): pp. 1–23.
- Makkonen, H., and Vuori, V. (2014). *The role of information technology in a strategic buyer-supplier relationship*. *Industrial Marketing Management*, 43(6): 1053–1062. <https://doi.org/10.1016/j.indmarman.2014.05.018>.
- Paller, A. (2010). *Talk at the Cyber Security Challenge UK*, University College London (26th July).
- Rid, T., & McBurney, P. (2012). Cyber-weapons. *RUSSI Journal*, 157(1): 6–13.
- Steinberg, L. J., Santella, N., and Zoli, C. B. (2011). Baton Rouge post-Katrina: The role of critical infrastructure modelling in promoting resilience. *Homeland Security Affairs*, 7 (February): Indirect citation.