Scientific Research Publishing

Journal of Software Engineering and Applications, 2025, 18(6), 159-174
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

Critical Information Infrastructure Protection and Cybersecurity in New York State: Governance Models, Practices, and Crisis Escalation Procedures—A Vital Discussion for the Future of New York's Security

Robb Shawe

Department of Critical Infrastructure, Capitol Technology University, Laurel, MD, USA
Email: rshawe@captechu.edu

How to cite this paper: Shawe, R. (2025) Critical Information Infrastructure Protection and Cybersecurity in New York State: Governance Models, Practices, and Crisis Escalation Procedures—A Vital Discussion for the Future of New York's Security. *Journal of Software Engineering and Applications*, **18**, 159-174.
https://doi.org/10.4236/jsea.2025.186011

Received: April 2, 2025
Accepted: June 17, 2025
Published: June 20, 2025

Copyright © 2025 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

Critical Information Infrastructure Protection (CIIP) and cybersecurity are significant topics for New York State. The safety of vital systems, such as power grids, water supplies, and hospitals, is crucial for maintaining the community's safety and well-being. CIIP involves protecting these essential services from threats such as cyberattacks. With the rise in technology use, the state must implement strong governance models. These models help organize how various agencies collaborate to secure information. New York can strengthen its defense against cyber threats by adhering to established rules and guidelines. In addition to governance, examining the practices employed to protect critical infrastructure is essential. These practices include regular security assessments, employee training, and incident response plans. Regular assessments help identify weak spots in the security systems, while training prepares employees to recognize and respond to potential threats. Incident response plans outline the steps to take in the event of a cyber incident. Solid practices build confidence among the public that their essential services are secure and reliable. Clear escalation procedures are essential for an effective response and recovery during a crisis. Escalation procedures outline the steps taken in a cyber incident. They help determine when to notify higher authorities and which resources to mobilize. New York State has developed protocols to ensure everyone responds appropriately during crises. These procedures include communication plans that inform the public about ongoing developments and activities. Combining good governance, firm practices, and clear escalation procedures is vital for protecting critical information infrastructure and enhancing cybersecurity in New York State.

Keywords

Critical Information Infrastructure Protection, Cyber Incidents, Cybersecurity, Crisis Escalation Procedures, Governance Models, Practices, Cybersecurity Capability Maturity Model (C2M2), The Smart Grid Interoperability Maturity Model (SGIMM)

1. Introduction

Due to the growing prevalence and sophistication of breaches, protecting New York State's critical information infrastructure and enhancing its cybersecurity governance have been developed as major priorities over recent years. The increasing sophistication and prevalence of cyber incursions necessitate the development of effective and adaptive governance models to influence security policy in protecting digital network perimeters from cyber threats. At the same time, specific procedures for crisis escalation would be important for a fast and effective response to cybersecurity cases when required. Such measures could significantly reduce the potential harm and emergence of cybersecurity incidents in varied spheres, protecting overarching critical functioning. For response systems, the know-how completion of defined actions for the real-time incident response also proves the need to form such protocols and train them beforehand.

As the digital landscape changes, recognizing the relationship between governance models and crisis management frameworks will allow New York State to understand better and respond to its implications. This paper explores the delicate balance required to roll out successful cybersecurity frameworks while demonstrating how a consistent governance model serves as a fundamental pillar in mitigating cyber risks to ensure that today's security is as preventative as it is reactive. This is a significant conversation to consider when building a firm, firm infrastructure is flexible enough to navigate the changing climate.

2. Challenges in Implementing Cybersecurity Frameworks in New York State

Cybersecurity framework implementation in New York State is faced with various regulatory and technological barriers, and it is important to highlight the challenges associated with each of them. With respect to regulatory aspects, one of the main concerns faced by the state authorities is their duty to synchronize cybersecurity policies with the constantly changing federal standards. Such synchronization is important to implement cyber policies coherently across multiple levels of governance. However, the changes in federal guidelines create discontinuous enforcement of policies within the state, which makes it challenging to retain coherent cybersecurity policy implementation [1].

The technological complexities are also multifaceted. Cybersecurity implementation requires integration of advanced and often unconnected systems. Imple-

mentation processes across various sectors (*i.e.*, finance, communication, health, and energy) can present interoperability challenges caused by technological misalignment. Furthermore, the emergence of new technologies renders cybersecurity implementation inefficient and ineffective due to increasing variations [2]. Furthermore, the dynamic nature of cyber threats and rapid technological innovations necessitate that cybersecurity policies remain flexible and forward-looking. Policy frameworks must anticipate and quickly adapt to new types of risks and technological advancements, a requirement that often stretches the current capabilities of state resources and systems. As a result, New York State must carefully maneuver these complex regulatory and technological landscapes to develop effective, robust cybersecurity frameworks capable of evolving in response to the ever-changing threat landscape.

2.1. Complexities in Governance Models

The governance models used for cybersecurity in New York State present complex challenges, particularly in balancing the dual demands of security and privacy. These models must provide strong protection against cyber threats while respecting the privacy rights of individuals and organizations. According to Pylant [3], a centralized and coordinated governance approach can streamline security measures, yet it may also pose risks of privacy infringement. Moreover, the governance framework must keep up with the ever-changing nature of cyber threats, necessitating rapid policy adjustments that can challenge existing legal and ethical norms [2]. Examining these complexities underscores the ongoing tension in managing effective cybersecurity without compromising individual freedoms, emphasizing the need for innovative and flexible governance models to navigate this delicate balance.

The coordination-related issues concerning New York State governance models' stakeholders are primarily associated with their vast diversity. Indeed, stakeholders include multiple government agencies and departments as well as a wide range of private sector stakeholders and civil society actors. Each of these stakeholders has a specific viewpoint on the issue of cybersecurity, and it is crucial to ensure their coordinated interaction within the overarching strategy. According to Pylant [3], this objective often requires balancing various competing priorities characteristic of diverse stakeholders. The latter may relate to their distinct approaches to resource allocation, compliance with their obligations, and an array of strategic interests. In addition, the evolving nature of cyber threats also emphasizes the need for a responsive and adaptive governance model that involves the contributions of all relevant stakeholders, further complicating collaboration [2]. As demonstrated by the interrelation of stakeholders' cooperation and cybersecurity success, an urgent demand exists for an inclusive governance model that simultaneously enables quick adaptation to emerging digital threats to conventional security strategies. Remarkably, implementing an inclusive model allows stakeholders to work collaboratively while managing uncertainties and the rapid evo-

lution of digital threats.

2.2. Evaluating Current Cybersecurity Procedures

The thorough analysis of the contemporary cybersecurity practices in New York State indicates an intricate situation when effective measures are implemented. Yet, there are unignorable aspects that need to be improved. The New York State's willingness to protect its cyberspace is based on a transposition of existing cybersecurity approaches to the local context, that is always difficult due to the rapidly changing environment of cybersecurity threats and technologies [1].

On the positive side, these procedures have played a pivotal role in raising awareness among public and private institutions about the importance of cybersecurity. They have fortified defenses against a variety of prevalent cyber threats, from phishing attacks to malware intrusions. However, this progress also underscores certain vulnerabilities, particularly the difficulty of keeping security measures updated in line with the rapid evolution of technology [3]. Rapid technological advancements mean that threats continually evolve, often outpacing current safeguarding measures and exposing specific systems. Additionally, there are notable gaps in how comprehensively these cybersecurity frameworks are integrated across the various sectors within the state. This lack of integration can significantly compromise overall state security, as inconsistencies in security measures across different sectors can create weak links in the collective defense system [2].

A committed and collaborative approach is needed to refine policy implementation processes to address these challenges effectively. Such refinement should ensure that policies are robust, able to resist increasingly sophisticated cyber threats, and flexible enough to adapt to future technological innovations. By pursuing these goals, New York State can enhance its capacity to protect its digital infrastructure against current and emerging cyber threats, ensuring a more secure environment for all its digital operations.

Moreover, recent cybersecurity breaches have posed serious threats to the approach adopted in New York State. One of the breaches that hit the digital infrastructure in the state was a complex cyber-attack that infiltrated the current defenses, hence exposing the system [1]. The attack revealed failures in the existing rapid response plans, prompting an overhaul in the escalation procedures and adopting a more flexible response. As stated by Bechara and Schuch [2], the breach revealed that more adaptive regulatory strategies and technical architecture are inevitable if the new threats are to be mitigated successfully. Consequently, the experience gained from the breach also provided critical insights and lessons, including the need for flexible and integrated cybersecurity strategies to prevent imminent risks from sliding into possible security loopholes.

3. Insights from Literature and Frameworks

The knowledge derived from the existing literature and frameworks also acts as a

supportive cornerstone in understanding and enhancing cybersecurity policies across New York State. Georgiev [4] analyzes cybersecurity maturity models comparatively and explains their importance in preparing organizations for dynamically evolving cyber threats at the state level. The importance of these maturity models in reflecting the state policy goals and the newest technologies in the dynamic cybersecurity landscape is evident in enabling them to take action for hazardous predicaments before they snowball into operating risks.

Moreover, Rabii *et al.* [5] focused on using maturity models in various domains in the state. The results showed that the applicability of maturity models varies considerably based on the industry, thereby requiring unique strategies for their implementation. This stratification, consequently, is important to ensure the most efficient effect of these models in each case study. Cumulatively, these findings show how essential sound structures are in support of state governance systems' ability to ensure high levels of cybersecurity and their capacity to deal with the complexities of technological change. The balance between organizational and structural support for securing an effective response to cyber threats and adapting to the evolving environment helps ensure New York State's capacity to protect its cybersecurity and stakeholder interests.

3.1. Innovative Perspectives on Cybersecurity

While the previous text explained how the paradigmal shift is visible through current cybersecurity policies, further studies discuss the previous standards that need to be followed for further evolvement. New studies provided new ways to overcome such issues that arise with the changing nature of the security threat possibilities. Establishing a proactive threat intelligence framework is one of the modern paradigms discussed in current studies implemented in a technological environment [6]. Compared to the past policies, the modern framework encouraged a shift from the routine implementation of cybersecurity policy standards to an emerging standard framework that moves proactively and seeks to understand the potential threats before they occur. Further technological development also provides further advancements in how policies could adapt to the changing nature of the environment. The implementation of artificial intelligence was proposed in the framework as a breakthrough in how vast amounts of data could be processed and its applicability in security coding to detect and respond in real-time [6].

In complementing the matter further, the decision-making framework suggested machine learning applications that could optimize risk analysis and reaction policy and improve the specific case uniqueness and the system's capabilities and response [7]. The policy, accompanied by advanced strategies, further projects the advancement of technological policies and the importance of what both current and future studies could bring. With the advancements that arise, the need for dynamic policies is observed through previous standards and their evolvement through the changing times and possibilities.

While integrating new innovative and proactive cybersecurity strategies to

existing New York State cybersecurity strategies, significant attention should be given to aligning technological solutions. Innovative strategies should ensure the adoption of technology into the existing cybersecurity strategies in New York State. More specifically, there should be a strategy to enhance the utilization of artificial intelligence (AI) systems related to threat detection and response. Artificial intelligence systems could significantly enhance New York State's ability to carry out data-driven analysis concerning cyber threats and deliver immediate insights into potential threats and challenges, thereby ensuring a timely response [7].

In addition, the move towards proactive threat intelligence systems is an important step forward in cybersecurity approaches. Proactive threat intelligence systems, as opposed to the more defensive techniques reliant on prior intelligence that are common in traditional systems, allow cybersecurity experts to take preemptive action against threats. Rather than focusing mainly on how to tactically respond to an impending threat after the fact, a proactive threat intelligence system only deals with potential threats that can be predicted. By altering the chief concern of the threat intelligence system, it is possible to ensure that threats are far less likely to succeed.

In addition, a crucial aspect of cyber security for New York State is the need for a unique approach for different sectors. Each sector's vulnerabilities and needs differ, which is why there should be a unique approach to the security parameter obtained for each sector. This also specifies the need for the sector-specific adaptation of the maturity models, which is necessary to implement cybersecurity [5] correctly. New York's cybersecurity infrastructure will be enhanced by incorporating value-added techniques. The potentiality of the strategic enhancement of the cybersecurity framework will empower the state to enhance its preparedness and resilience further.

3.2. Comparative Analysis of Maturity Models

A comparative analysis of various cybersecurity maturity models highlights important insights into their use for addressing New York State's cybersecurity needs. Georgiev [4] notes that these models offer a structured approach to assessing cybersecurity capabilities, which is crucial for state-level organizations dealing with complex cyber threats. Models like the Cybersecurity Capability Maturity Model (C2M2) and the Smart Grid Interoperability Maturity Model (SGIMM) provide unique frameworks tailored to different sector-specific challenges [5]. While C2M2 is adaptable due to its focus on organizational processes and workforce investments, SGIMM concentrates more on the technological facets of cybersecurity, addressing integration challenges utilities face [4]. The adaptability of these models allows them to be customized to New York State's diverse sectoral needs, enhancing defense against evolving cyber threats while aligning with existing regulatory frameworks.

The practical implementation of cybersecurity maturity models in New York

State has positive aspects and challenges that deserve thorough analysis. One of the notable strengths of these models is their structured approach, which provides a detailed methodology that organizations can follow to assess their cybersecurity capabilities systematically. This structured approach allows companies to pinpoint their current strengths and weaknesses, facilitating a clear pathway toward prioritizing enhancement and targeted improvement efforts in their cybersecurity posture [4].

Despite these advantages, there are challenges primarily related to the adaptability of these models across different industries. Each sector often has specific challenges and unique demands, which these models may not fully address. For instance, the Cybersecurity Capability Maturity Model (C2M2) and the Smart Grid Information Model Maturity (SGIMM) exhibit variations in implementation, underscoring the difficulty in creating a one-size-fits-all solution that fully meets the diversified needs of each industry [5]. Moreover, these models contain stakes as an effective map to enhance certain cybersecurity protections but lack in providing real-time adaptive responses to the ever-growing dynamic cyber threats; the non-implementable adaptive processes may lead to ineffectiveness of the model proposed due to the progressive nature of cyber risk and mandate an agile approach from the organization to quick defense mechanisms.

Hence, there is a demand to keep working to adapt and improve maturity models to respond to existing and emerging cyber threats promptly. Adapting the maturity models in this direction will make them more usable and relevant.

4. Critical Evaluation of Governance and Maturity Models

The in-depth study of the governance and maturity models used in New York State reveals significant pros and cons. Governance models are critically important as they synchronize cybersecurity efforts at various levels and across numerous industries. They formulate rules and policies necessary to ensure the coherency and relevance of digital infrastructure protection practices. At the same time, the fundamental issue confronting the governance models is their inefficiency in dynamically adapting to the changes in the nature and methods of cybercrime. The nature of cyber threats is constantly changing, and the attack methods and vectors are permanently evolving, yielding advanced threats of unpredictable origin [3].

While these governance frameworks offer structural organization, they also tend to have inflexibility due to that design, which can hinder one's ability to shift quickly in response to a new threat. When the policies and protocols of a given framework appear to be "carved in stone", the ability to react quickly and develop an adaptive response is restricted. An inability to respond to emerging cyber threats promptly reflects a key advancement opportunity for these frameworks and their capabilities to produce resilience and adaptability in the face of future cyber threats.

In line with governance structures, reviewing frameworks and association as-

sessment tools such as the Cybersecurity Capability Maturity Model (C2M2) are equally important. Assessment and evaluation frameworks assist in understanding organizations' preparedness in terms of their information security stature and practices. It allows organizations to analyze and evaluate their weaknesses and strengths in their cybersecurity domains by providing systematic and articulated descriptions Cybersecurity Capability Maturity Model (C2M2) [5]. Nonetheless, an associated challenge is that assessment models are generic and not aligned with the core properties of the sectors.

However, sector-specific nuances and vulnerabilities may require a different approach, which advocates further developments of these maturity models to provide a more accurate depiction of varying risk landscapes across industries. Customization of these models is essential to cater to specific vulnerabilities. The current governance structures and maturity models must be developed toward flexibility and adaptability. This becomes a prerequisite for their sustainability in today's environment and efficiency in fighting the upcoming cyber risks. Thus, consolidating the existing approach will guarantee the organizational ability to comply with the current cybersecurity requirements, sustain the resilience to future threats, and provide a strong safeguard from upcoming vulnerabilities.

4.1. Assessing Governance Structures

New York State's cybersecurity governance structures represent a complex tapestry of strengths and challenges that are crucial in maintaining the state's overall security infrastructure. An essential strength of this system is its centralized and coordinated governance approach. This model ensures a more cohesive and unified application of cybersecurity strategies across multiple public, private, and governmental sectors [3]. By fostering such integration, the state is better positioned to develop and implement broad-ranging, effective cybersecurity measures to address various simultaneous threats more efficiently.

However, the centralized nature of this governance framework is not without its challenges. There are significant concerns regarding the potential impact on privacy protection. A centralized authority might pose risks of overreach, where the balance between security and individual privacy becomes precarious. Moreover, centralization can potentially lead to bureaucratic inefficiencies. These inefficiencies may manifest as delays or obstacles in decision-making processes, mainly when a swift response is necessary to counter emerging threats [3]. In addition to these concerns, the governance structures must be flexible enough to adapt to the ever-changing landscape of cybersecurity threats. Threat actors consistently evolve their tactics, and new vulnerabilities emerge regularly, demanding that the governance system remain dynamic and responsive. This necessity for adaptability often clashes with the inherent rigidity of structured governance frameworks, which can impede the required agility and quick adaptation to new challenges [2].

Therefore, ongoing analysis and evaluation of these governance models are crucial. By continuously identifying and addressing weaknesses within the system,

the state can work to enhance the agility and effectiveness of its cybersecurity strategies. This proactive approach ensures that the governance structures meet the immediate needs and remain robust and responsive to future cybersecurity challenges.

4.2. Maturity Models in Practice

Implementing the Cybersecurity Capability Maturity Model (C2M2) and the Smart Grid Interoperability Maturity Model (SGIMM) within New York State has led to a range of outcomes, significantly impacting the state's preparedness in cybersecurity. The C2M2 plays a pivotal role due to its focus on enhancing both organizational processes and workforce skillsets. This enhancement is critical for cultivating a coordinated and efficient response to the ever-evolving landscape of cybersecurity threats [4]. The model is designed with adaptability, providing state agencies with the necessary tools to pinpoint areas that require development and align their strategies with these insights to address vulnerabilities effectively.

In contrast, the SGIMM deals with the technical hurdles of integrating heterogeneous systems and offers peculiar solutions that are viably applicable to the utility industry. This focus is important in enhancing the security of intelligent grid systems, making them resilient to accidental and malicious attacks [5]. The integration of the two frameworks, C2M2 and SGIMM, demonstrates the importance of cybersecurity practices that are both strong and sector-specific to New York State's adaptability and alertness to secure its infrastructure from new and constantly changing threats in the digital world.

5. Crisis Escalation Procedures

New York State established crisis escalation processes for cybersecurity incidents, which are carefully designed processes and procedures that guarantee a timely and effective response to cyber threats. The established processes and procedures include a broad spectrum of activities from the initial detection of the threat to the implementation of targeted incident response plans. According to Colombo [8], New York State implemented a framework that precisely defines the roles and responsibilities of relevant parties that promote coordinated work during a cyber crisis.

This framework facilitates rapid communication and streamlined decision-making to manage the intricate dynamics that accompany cyber incidents. Such efficiency is vital in minimizing disruptions that might result from cyber threats. By design, the framework supports a swift and organized response, ensuring that all parties involved in a cyber incident know precisely what actions to take and when to take them. Even though relevant procedures are already strong, further improvement is still needed. This is because cyber threats are becoming increasingly complex. Therefore, the state response framework should also be improved to remain effective. Altogether, continuous improvement should be initiated to have a response framework that is not only strong but also very effective in re-

sponding to the new and emerging threats of cyber threats.

5.1. Frameworks for Escalation

Considering the frameworks utilized for crisis escalation in New York State, it is vital to note how these are established to promote operational efficiency in the response to cybersecurity events. One of the approaches adopted is the presence of escalation levels, wherein each identifies certain conditions and indicates appropriate response measures that may include both the activation of crisis procedures and the mobilization of stakeholders. In the work by Colombo [8], it is emphasized how these frameworks promote coordination among identified stakeholders, providing a mechanism by which their designated roles and responsibilities are clarified to ensure the timely execution of decisions during cyber-related crises. Also, the framework enables scalable crisis responses based on identifying the severity of the threat posed by the cyber attacks in question. This feature is essential to ensure that operational developments are retained while damage is minimized during the undertaking of crisis resolutions. It is crucial, however, that ongoing evaluations be conducted concerning the crisis escalation frameworks. Through this, the response mechanisms may be enhanced to ensure adequate consideration of the changing cyber threats while the current protocols remain practical and applicable in the long run.

A thorough review and analysis of the Cybersecurity Capability Maturity Model (C2M2) application in financial organizations operating in New York State demonstrates the effectiveness of a structured approach when enhancing institutions' cybersecurity preparedness. Using the Cybersecurity Capability Maturity Model (C2M2) as a coherent framework has allowed New York-based financial institutions to analyze their cybersecurity practices comprehensively. They have been able to carry out a complete and organized examination of their cybersecurity practices to discover vulnerabilities in their systems. It permits institutions to focus on areas that require improvement, thereby improving their cybersecurity preparedness.

A key feature of the C2M2 is its emphasis on process maturity and workforce development, which are crucial for fortifying defenses against cyber threats. By focusing on these areas, financial institutions have been able to enhance the training of their staff and increase awareness about potential cyber risks. This has reinforced their defenses and cultivated a culture of cybersecurity awareness throughout the organization. Enhanced staff training ensures that employees are better equipped to recognize and respond to emerging cyber threats, thus decreasing the likelihood of successful cyberattacks.

The analysis conducted by Colombo [8] further underscores the importance of establishing clear escalation procedures. By adopting such procedures, these organizations have improved their ability to respond swiftly to cybersecurity incidents. Well-defined escalation protocols ensure that any cyber incident is managed promptly and effectively, significantly reducing the potential disruption to

operations. These findings from case studies highlight how tailored applications of maturity models and escalation frameworks can considerably enhance an organization's cybersecurity posture. Even in sectors such as finance, which encounter a wide range of complex threats, these structured approaches can provide significant improvements in managing and mitigating cybersecurity risks.

5.2. Best Practices in Crisis Management

In recent years, the examination of cybersecurity incidents within New York State has revealed several critical best practices in the realm of crisis management that significantly contribute to enhancing operational resilience. One of the foundational elements of these best practices is establishing a robust coordination framework among key stakeholders. This framework is essential as it ensures that information can flow seamlessly among all parties involved, enabling a rapid and coordinated response when crises arise. The framework is designed to adapt to various levels of threat severity, guided by well-defined escalation procedures. These procedures are pivotal in tailoring the response to the specific nature of the threat, allowing for the swift implementation of measures that are both appropriate and effective [8].

Additionally, a vital aspect of readiness improvement is the ongoing training and simulation exercises designed for cyber professionals. Not all such activities are routine; instead, the simulations significantly improve readiness by allowing experts to assess and resolve possible vulnerabilities beforehand, where exploits could lead to adverse outcomes. As pointed out by Bechara and Schuch [2], simulation activities represent the first-hand learning opportunity for cyber experts. This allows professionals to tweak their tactical approaches and improve their measures for dealing with possible incidents. Such increased readiness reduces the fallout from exploits when disruptions occur across impacted systems, further reducing the effects of incidents on the organization and its stakeholders.

6. Case Studies: Success Factors and Limitations

The thorough examination of the case studies pertaining to New York State further provides an in-depth exploration of the complexity associated with cybersecurity efforts while revealing prominent achievements and important shortcomings. One of the most notable successes includes using and implementing the Cybersecurity Capability Maturity Model (C2M2) within the financial industry. This model has played a pivotal role in increasing cyber-attack resilience by emphasizing refining and improving organizational processes and empowering workforce skills. Applying this model allows for systematically evaluating and addressing weaknesses while reinforcing defenses against the multiple cyberattacks directed toward the financial industry [4].

Notwithstanding these achievements and progress, issues remain, especially regarding scaling these models in various industries. Each industry brings its struggles, thereby creating complexities and sometimes blocks that prevent the easy

application and adjustment of universal structures like the C2M2 across many industries. These elements particular to a certain industry require more specific and precise attempts to cater and respond to the operational environment and threats experienced by the industries [5].

In New York State, the execution of the Cybersecurity Capability Maturity Model (C2M2) has become a crucial approach intended to develop the state's cybersecurity capabilities exponentially. More so, this implementation highlights the recognition of the C2M2 model-equipped strategies, which proffer a high degree of impact on the security of cyber infrastructures by applying a clear and organized model that assumes the role of methodically eliminating vulnerabilities and threats. Nevertheless, these implications are undoubtedly beneficial but have certain limitations. The case studies demonstrate that the C2M2 provides a structured and well-defined methodology for enhancing an organization's cybersecurity capabilities, which involves identifying the shortcomings of specific systems and providing the necessary actions to eliminate them. At the same time, the healthcare and finance industries experience some challenges in the implementation of C2M2 principles. This is mainly due to the peculiarities of these sectors' operational criteria and regulatory standards, which require adopting C2M2 principles as per existing protocols and maintaining compliance with applicable industry regulations.

Also, it must be noted that the model is to be revised and updated regularly since the threat landscape is dynamic and subject to constant evolution C2M2 is quite demanding in terms of resources for the institutions with low budgets for cybersecurity [9], as most of the funds will be spent on the regular processes of model revision. As for the effectiveness of the model, it must be pointed out that according to Lewis, uninterrupted performance operation is an essential component of the success, which does not depend on the incident elimination process, ensuring operational performance stability demands proper actions in the pre-incident phase, rather than adequate reaction in the post-incident period.

A case of a successful application of the Smart Grid Interoperability Maturity Model (SGIMM) in New York State highlights the complexities and potential benefits of the implementation of contemporary cybersecurity models in energy systems. One of the most remarkable studies in the state demonstrates the successful implementation of SGIMM on the state level. The model focused on establishing statewide communication systems and further outreach for improved interoperability among various energy suppliers. This strategic initiative accomplished the goal of emphasizing that conspicuously the deploying approaches of technological infrastructures are not enough, hence it is significant to cultivate communications with a great number of stakeholders, such as governmental agencies, regulatory bodies, other involved participants, private sector businesses, etc., which matter in this field [9]. Accordingly, only such efforts may be beneficial for realizing that the deploying SGIMM is an instrument for increasing the smart grid's capabilities in resisting and preventing cybersecurity attacks.

Despite the already described advantages, moving towards SGIMM was not pain-free. The difficulty of adapting the existing legacy systems to the modern requirements of SGIMM arose as a significant challenge. Most legacy systems were outdated, and upgrading adaptation would require significant investments. Such an expectation of investment proved to be a challenge for smaller providers within the state. These challenges point to a more extensive scope, and continuous adjustments and initiatives towards the infrastructure imply that the full evolutionary and revolutionary potential of a more advanced and resilient intelligent grid network will only be recognized by such commitment and investment.

Overcoming these challenges is important to improve the broader state cybersecurity steps, making the energy grid secure, resilient, and postured for the future. SGIMM advancements show that it can be transformative in its scope and outcome. It highlights the necessity for integrated frameworks encompassing technological, budgeting, and collaboration measures to support the intelligent grid system's security and resilience progress on the broader level. The government and private sector must work together to improve the country's cybersecurity resilience. A collaborative effort will ensure a better and stronger approach to the challenges posed by new-age cyber threats. Collectively, the government and private sector will enhance the state's resistance and preparation to avoid and counter cyber adversities.

Cybersecurity frameworks are required to be up-to-date and relevant, which is a constant challenge. As cyber-attacks can adapt and rapidly change, there is a continuous need for systemic and dynamic updates of the models' structures and elements. Hence, they stay relevant and resilient against new threats. Updates must be incorporated into current systems to secure resilient cyber-defense mechanisms and sensitive data from breaches [8].

6.1. Analysis of Successful Implementations

In New York State, analysis of the effective cybersecurity practices assists in understanding how a clear focus on proper governance patterns and training procedures is critical to improving security results for most organizations. For example, evidence suggests that including established and well-understood incident management processes in public sector organizations has effectively improved their capacity to resolve cyber-attacks. This allows organizations to respond to threats promptly and limit the impact of these vulnerabilities.

Colombo [8] accentuated that effective escalation frameworks are in place for leaders to establish prompt and orderly responses to cybersecurity incidents. Incidents that can lead to a full-scale crisis can be effectively avoided through these frameworks. Predefined protocols and duties are set when responding to varying incidents and threats. Adopting these best practices makes it easier for organizations to curb a cybersecurity incident and avoid a full-fledged crisis. Additionally, based on the article, the C2M2 provides a structure for continuously growing and improving an organization's cybersecurity maturity. Conducting periodic assess-

ments using this model supports prioritizing this facet to discover the organization's deficiencies, weaknesses, or top hazards needing more attention or advance action [4]. Subsequently, constantly improving the organization's cybersecurity capabilities allows it to strengthen and defend itself against emerging hazards.

The case studies highlighted in this section reflect the need for customized adaptive frameworks and strategies to overcome these challenges imposed by the evolving cybersecurity landscape. These adaptive strategies would help organizations develop a strong cybersecurity posture to fight against potential risks.

6.2. Lessons from Challenges Faced

Among the lessons learned from less successful implementations, it is important to underline the opportunity to enhance the cybersecurity initiatives existing in New York State. One highlighted issue is that some maturity models lack flexibility in quickly implementing positive sector-related changes. A lack of flexibility occurs due to models being too generalized and, therefore, failing to engage with a particular industry. Unfortunately, such overgeneralization hinders the development of industry-specific cybersecurity programs associated with increased risk [4].

These generic strategies may fail to recognize the specific requirements of particular industries, such as finance, healthcare, or energy, which all present unique challenges and vulnerabilities. To illustrate, an energy company may have different concerns than a healthcare organization, as integrity and transaction-related issues may be of higher concern to the finance industry. Without this specificity, a generic approach may have forced specific vulnerabilities and threats that would not have been applicable against breaches and exploits.

Moreover, one of the critical weaknesses observed in specific organizations is their lack of proper incident response planning. As a result, they may fail to respond on time to cyber threats, allowing their potential consequences to elevate over time, leaving the compromised systems exposed to longer-term breaches. Suppose there is no appropriate incident response plan. In that case, organizations usually become more proactive and respond to threats compared to employing measures that could mitigate the threats and vulnerabilities, elevating the risks and consequences of cyber threats [8]. Improvements should be made to the cybersecurity models and monitoring systems to meet these requirements. The existing cybersecurity models should be more flexible and adaptive to the targeted sector-specific requirements to provide customized security solutions to the organizations. Security monitoring systems should be improved to provide real-time feedback and adopt a proactive strategy to manage any possible threat.

7. Methodological Assessment of Strategies

Assessing how cybersecurity initiatives work in New York State is challenging and requires different methods covering different aspects of the cyber environment. One approach is to utilize maturity models; one is the Cybersecurity Capability

Maturity Model (C2M2). Maturity models are developed as structured frameworks to assess and improve an organization's preparedness and resiliency against cybersecurity threats [4]. This assessment process will take into account essential aspects, like incident response readiness and thorough risk management, to get a picture of the organization's cybersecurity capabilities, identify strengths, and reveal gaps and weaknesses that should be covered to adjust and adapt how cybersecurity initiatives are working since cyber threats are ever-changing.

Moreover, along with the maturity models, frameworks for strategic decisions such as PRISM have allowed state agencies to maximize the effectiveness of cybersecurity risk assessment procedures. With the framework, the state agencies can perform an integrated level of risk assessment that will enable the identification and mitigation of threats that may not be accommodated using conventional risk assessments [7]. This will allow the emerging threats to be countered with proactive and dynamic risk assessment techniques.

These methodologies used in concert emphasize the ongoing need for dynamic assessment methodologies. As the cyber threat landscape evolves, so do the cybersecurity strategies implement and their assessment methodologies. With dynamic assessment methodologies, New York's cybersecurity strategies are dynamic and strong enough to address the cyber threat landscape's evolution adequately.

8. Conclusion

This paper has thoroughly assessed the challenges and opportunities associated with enhancing cybersecurity frameworks within New York State. A central focus of this evaluation has been the vital role played by robust governance models and well-defined crisis escalation procedures. By examining these factors closely, it becomes evident that their practical implementation is crucial for maintaining a secure cyber environment. One of the major strengths of New York State's cybersecurity efforts is the utilization of advanced maturity models, such as the Cybersecurity Capability Maturity Model (C2M2) and the Security Governance Maturity Model (SGIMM). These models are particularly beneficial because they provide a structured approach for measuring and improving the state's cybersecurity capabilities. They enable organizations within the state to adapt strategies based on their specific sector needs while ensuring the integration of consistent security practices across the board.

The assessment of existing approaches indicates that although there are particular strengths in the present mechanism, it is necessary to improve upon it further to match the rapidly changing technological environment. Cyber threats are becoming increasingly intelligent, and permanent solutions may not work efficiently to address the ever-changing issue. Providing a better cybersecurity infrastructure for New York State is not enough to improve the current cybersecurity strategies. The new strategies that are to be implemented must also include innovative technologies. For instance, advanced technologies like artificial intelligence (AI) can detect possible anomalies and threats better. AI can analyze volumes of data in

real-time and detect irregularities from normal behaviors, which could indicate a security threat. Furthermore, implementing proactive threat intelligence systems can improve the capacity of the state's cyber defenses to predict and prevent attacks.

From this thorough analysis, a key takeaway is that New York State must be dedicated to flexible and adaptable cybersecurity efforts to be prepared to traverse the many intricacies seen today in the cybersecurity landscape.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Oluomachi, E., Ahmed, A., Ahmed, W. and Samson, E. (2024) Assessing the Effectiveness of Current Cybersecurity Regulations and Policies in the US. https://arxiv.org/abs/2404.11473

[2] Bechara, F.R. and Schuch, S.B. (2020) Cybersecurity and Global Regulatory Challenges. *Journal of Financial Crime*, **28**, 359-374. https://doi.org/10.1108/jfc-07-2020-0149

[3] Pylant, A.C. (2020) Initiating a Collaborative Cybersecurity Governance Framework at the State Level. https://digitalcommons.wcupa.edu/all_doctoral/59/

[4] Georgiev, V. (2021) Comparative Analysis of the Cyber Security Capabilities Maturity Models. *Yearbook of UNWE*, **2**, 31-42. https://www.ceeol.com/search/article-detail?id=1035872

[5] Rabii, A., Assoul, S., Ouazzani Touhami, K. and Roudies, O. (2020) Information and Cyber Security Maturity Models: A Systematic Literature Review. *Information & Computer Security*, **28**, 627-644. https://doi.org/10.1108/ics-03-2019-0039

[6] Sharkov, G. (2020) Assessing the Maturity of National Cybersecurity and Resilience. *Connections*: *The Quarterly Journal*, **19**, 5-24. https://doi.org/10.11610/connections.19.4.01

[7] Goel, R., Kumar, A. and Haddow, J. (2020) PRISM: A Strategic Decision Framework for Cybersecurity Risk Assessment. *Information & Computer Security*, **28**, 591-625. https://doi.org/10.1108/ics-11-2018-0131

[8] Colombo, R. (2020) On the Escalation from Cyber Incidents to Cyber Crises. Master's Thesis, University of Twente. http://essay.utwente.nl/83051/

[9] Lewis, T.G. (2019) Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. John Wiley & Sons. https://books.google.com/books?hl=en&lr=&id=Yz6-DwAAQBAJ&oi=fnd&pg=PA15&dq=critical+information+infrastructure+protection+cybersecurity+new+york+state+governance+models&ots=eYa6P3rlde&sig=zvibvc5txQwVAIzhhtBLOSQnpqQ