International Journal of Science and Technology Research Archive

ISSN: 0799-6632 (Online)

Journal homepage: https://sciresjournals.com/ijstra/

(REVIEW ARTICLE)

Check for updates

Improving cybersecurity readiness with a maturity framework for organizations in U.S. and Canada

Gideon Opeyemi Babatunde [1, *], Olukunle Oladipupo Amoo [2], Sikirat Damilola Mustapha [3] and Adebimpe Bolatito Ige [4]

[1] *KPMG, Calgary, Canada.*
[2] *Amstek Nigeria Limited.*
[3] *Kwara State University, Malete, Nigeria.*
[4] *Independent Researcher, Canada.*

International Journal of Science and Technology Research Archive, 2022, 03(01), 232-250

Publication history: Received on 08 June 2022; revised on 23 July 2022; accepted on 27 July 2022

Article DOI: https://doi.org/10.53771/ijstra.2022.3.1.0068

Abstract

The increasing frequency and sophistication of cyber threats have underscored the need for enhanced cybersecurity readiness among organizations in the U.S. and Canada. To address this need, this paper introduces a Cybersecurity Maturity Framework (CMF) designed to assist organizations in systematically assessing and improving their cybersecurity capabilities. The framework provides a structured approach for evaluating current security postures, identifying gaps, and prioritizing investments to mitigate risks effectively. The proposed CMF consists of five maturity levels: Initial, Developing, Established, Advanced, and Optimized. Each level encompasses critical domains, including governance, threat intelligence, incident response, and workforce development, with defined benchmarks to measure progress. By incorporating best practices from the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Canada's Cyber Security Strategy, the CMF ensures alignment with regional regulatory requirements and industry standards. A key feature of the framework is its adaptability to organizations of various sizes and sectors. The CMF integrates advanced technologies such as artificial intelligence (AI) and machine learning (ML) for threat detection and predictive analytics while emphasizing the importance of human factors, including continuous employee training and leadership engagement. Moreover, the framework promotes collaboration between public and private sectors to facilitate information sharing and collective defense against evolving cyber threats. Through case studies, the application of the CMF is demonstrated in enhancing cybersecurity readiness for small and medium enterprises (SMEs) and large organizations in critical sectors such as healthcare, finance, and energy. Results indicate improved incident detection rates, faster response times, and strengthened resilience against sophisticated cyberattacks. This research highlights the necessity of adopting a maturity-based approach to cybersecurity, ensuring organizations can evolve their capabilities to counter dynamic threats. The Cybersecurity Maturity Framework provides a roadmap for sustainable improvement, empowering organizations in the U.S. and Canada to achieve a higher state of preparedness and resilience in the face of an ever-changing cyber threat landscape.

Keywords: Cybersecurity Maturity Framework; U.S.; Canada; Cybersecurity Readiness; Threat Intelligence; Incident Response; AI; Machine Learning; Governance; Public-Private Collaboration

1. Introduction

The growing prevalence of cyber threats poses significant challenges to organizations worldwide, with critical sectors in the United States and Canada being particularly vulnerable. As digital transformation accelerates across industries, the complexity and frequency of cyberattacks have increased, exposing organizations to risks that threaten data

* Corresponding author: Gideon Opeyemi Babatunde

integrity, operational continuity, and public trust (Onoja & Ajala, 2022, Parraguez-Kobek, Stockton & Houle, 2022). Organizations operating in sectors such as healthcare, finance, energy, and government have become primary targets for sophisticated cybercriminals, making robust cybersecurity readiness an essential component of organizational resilience.

Despite efforts to strengthen cybersecurity defenses, organizations in the U.S. and Canada continue to face several challenges, including limited resources, outdated systems, insufficient training, and evolving threat landscapes. Regulatory requirements further compound these challenges, demanding compliance with complex standards while adapting to new threats. Many organizations struggle to identify their current cybersecurity maturity level and lack a clear roadmap to enhance their cybersecurity capabilities systematically (Dalal, Abdul & Mahjabeen, 2016, Shafqat & Masood, 2016). This situation underscores the urgent need for comprehensive, scalable frameworks to guide organizations in improving their cybersecurity readiness.

This paper introduces a Cybersecurity Maturity Framework (CMF) designed to address these challenges by providing organizations with a structured approach to assess and improve their cybersecurity posture. By leveraging the CMF, organizations in the U.S. and Canada can systematically evaluate their cybersecurity capabilities, identify gaps, and implement targeted improvements. This framework serves as a roadmap, guiding organizations through iterative steps to enhance their defenses, ensure compliance with regulatory standards, and build a culture of proactive cybersecurity awareness (Bodeau, McCollum & Fox, 2018, Georgiadou, Mouzakitis & Askounis, 2021).

The goal of this initiative is to equip organizations with practical tools and methodologies to fortify their cybersecurity strategies against an increasingly complex threat landscape. By adopting the CMF, organizations can achieve greater resilience, mitigate risks, and foster a more secure digital environment, ultimately contributing to the broader goals of national and economic security (Bello, et al., 2022, Elujide, et al., 2021).

2. Overview of Cybersecurity Maturity Models

Cybersecurity maturity refers to an organization's ability to develop and optimize its defenses against cyber threats through a structured, incremental approach. Maturity in cybersecurity involves evaluating and enhancing an organization's preparedness, detection, response, and recovery capabilities to address existing and emerging threats. By systematically increasing maturity levels, organizations can strengthen their defenses and adapt to the ever-evolving cybersecurity landscape (Buchanan, 2016, Clemente, 2018, Djenna, Harous & Saidouni, 2021). This concept is particularly significant in an era where cyber threats are more sophisticated and pervasive, impacting critical sectors such as healthcare, finance, and energy.

A maturity model provides a framework for organizations to assess their cybersecurity posture and progress toward desired objectives. These models delineate stages of development, enabling organizations to identify where they currently stand and what steps are necessary to reach higher levels of security. Applying a maturity model fosters continuous improvement, which is essential for keeping pace with the dynamic nature of cyber risks. It also allows organizations to allocate resources effectively, prioritize initiatives, and measure progress over time (Aliyu, et al., 2020, Shameli-Sendi, Aghababaei-Barzegar & Cheriet, 2016).

The benefits of using cybersecurity maturity models extend beyond technical improvements. They promote a culture of security awareness and accountability within organizations, encouraging proactive management of cyber risks. Moreover, these models support compliance with regulatory requirements and industry standards, which are critical for maintaining stakeholder trust and avoiding legal penalties. By embedding cybersecurity maturity within organizational strategies, businesses can enhance operational resilience, reduce vulnerabilities, and safeguard their digital assets more effectively (Cohen, 2019, Lehto, 2022, Onoja, Ajala & Ige, 2022). Aliyu, et al., 2020, presented Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) requirements are divided into three groups as shown in figure 1.

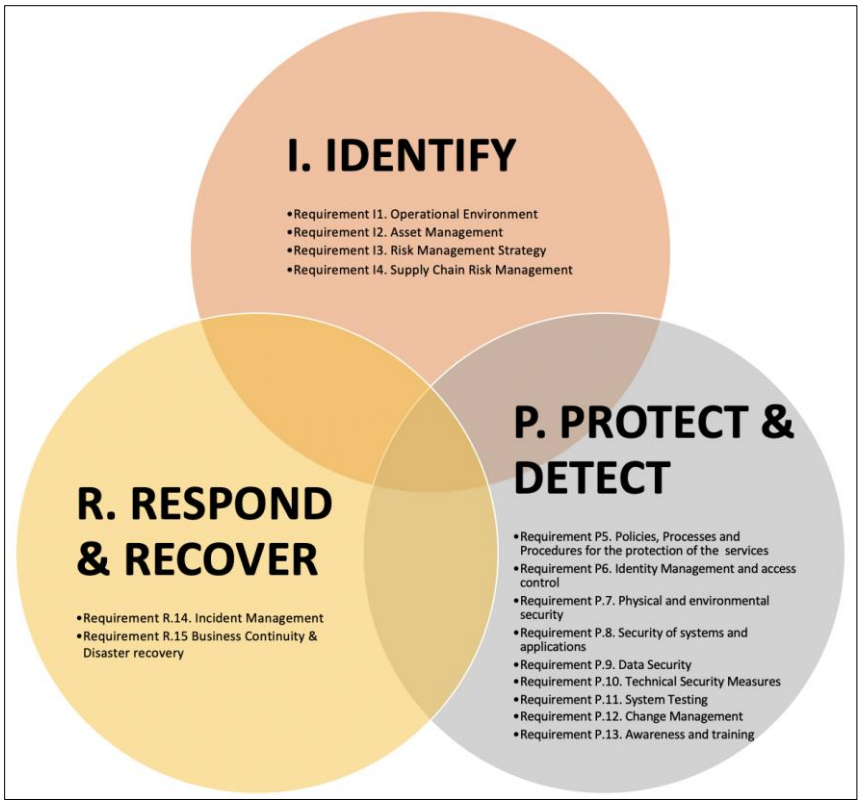

Figure 1 Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) requirements are divided into three groups (Aliyu, et al., 2020)

Several existing cybersecurity frameworks have been developed to assist organizations in improving their cybersecurity readiness. In the United States, the National Institute of Standards and Technology (NIST) Cybersecurity Framework is widely recognized. This framework provides a comprehensive guide for organizations to manage and mitigate cyber risks. It comprises five core functions: Identify, Protect, Detect, Respond, and Recover. Each function includes categories and subcategories that outline specific cybersecurity activities and outcomes, offering organizations a flexible approach to addressing their unique risk environments (Djenna, Harous & Saidouni, 2021, Sabillon, Cavaller & Cano, 2016). The NIST Cybersecurity Framework has gained traction across various sectors, offering scalability and adaptability to organizations of different sizes and complexities.

In Canada, the government has introduced the Cyber Security Strategy, which focuses on enhancing national cybersecurity capabilities and supporting businesses in improving their defenses. This strategy emphasizes public-private collaboration, the development of skilled cybersecurity professionals, and the implementation of robust security measures to protect critical infrastructure. The Canadian Centre for Cyber Security (CCCS) plays a pivotal role in providing organizations with guidance, tools, and resources to bolster their cybersecurity posture (Amin, 2019, Cherdantseva, et al., 2016, Dupont, 2019).

Despite the strengths of these frameworks, gaps and challenges remain in addressing the rapidly evolving cyber threat landscape. One significant challenge is the lack of integration and alignment between existing frameworks. While NIST and the Canadian Cyber Security Strategy provide valuable guidelines, organizations often struggle to implement them cohesively due to differences in terminology, scope, and objectives. This misalignment can lead to fragmented cybersecurity practices, reducing the overall effectiveness of security efforts (Adepoju, et al., 2022, Oladosu, et al., 2022). Cyber-Security Culture Framework presented by Georgiadou, Mouzakitis & Askounis, 2021 is shown in figure 2.

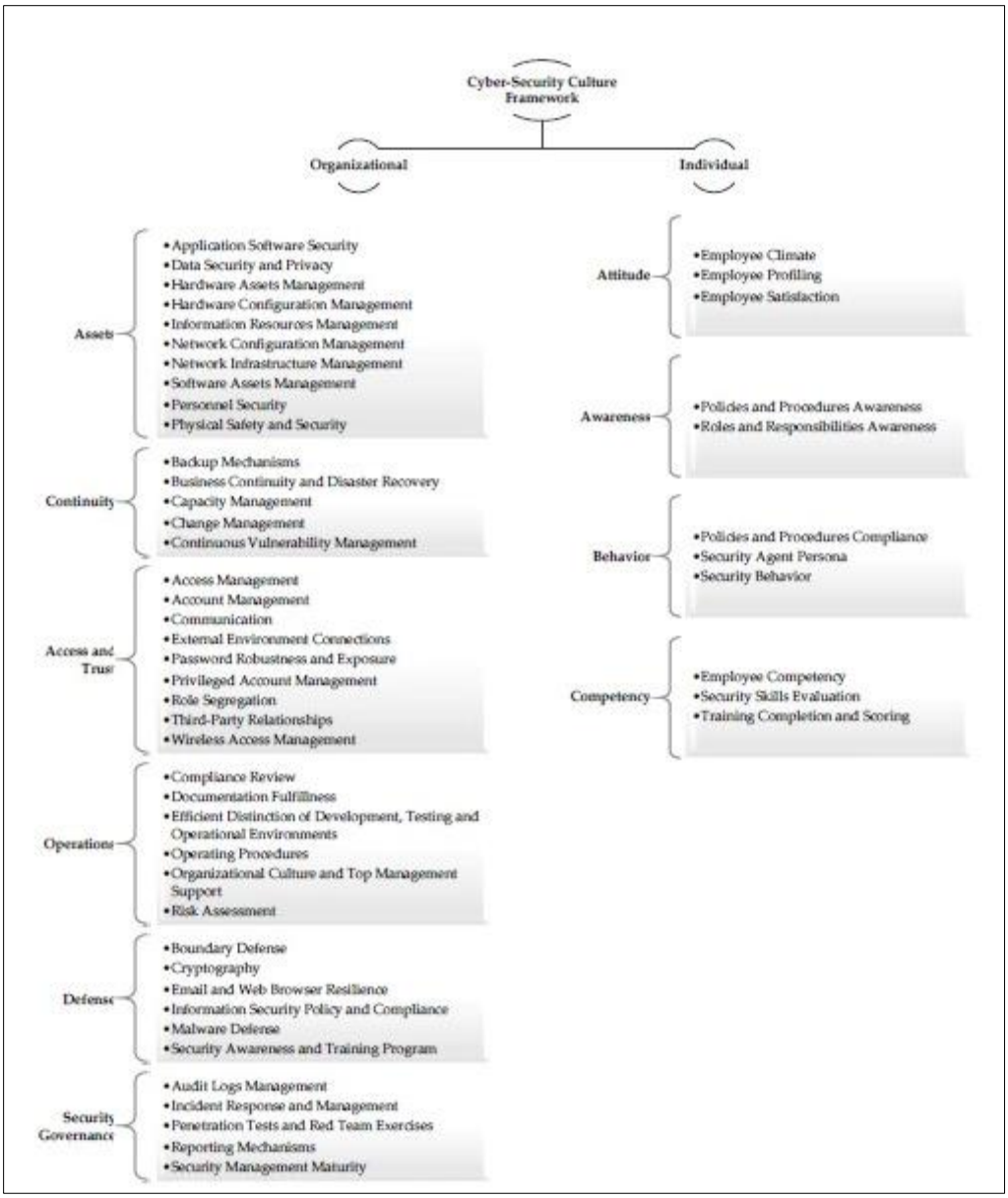

Figure 2 Cyber-Security Culture Framework. (Georgiadou, Mouzakitis & Askounis, 2021)

Another challenge is the difficulty of addressing emerging threats such as ransomware, supply chain attacks, and advanced persistent threats (APTs) within existing models. Cybercriminals are continually developing new tactics, techniques, and procedures (TTPs), outpacing the capabilities of traditional security measures. Consequently, organizations need more dynamic and adaptive frameworks that can evolve alongside these threats.

Resource constraints further complicate the adoption and implementation of cybersecurity frameworks. Many organizations, particularly small and medium-sized enterprises (SMEs), lack the financial and human resources necessary to invest in comprehensive cybersecurity programs (Kovacevic & Nikolic, 2015, Pomerleau, 2019). The complexity of existing frameworks can be overwhelming for these organizations, leading to partial or ineffective implementation. Moreover, the absence of clear metrics for measuring cybersecurity maturity makes it challenging for organizations to evaluate their progress and demonstrate value to stakeholders.

Given these challenges, there is a growing need for a unified, scalable, and adaptable maturity framework that caters to the specific needs of organizations in the U.S. and Canada. Such a framework should build on the strengths of existing models while addressing their limitations. It should provide organizations with a clear roadmap for improving their cybersecurity posture, incorporating best practices, and enabling continuous improvement.

A robust cybersecurity maturity framework would integrate key elements of NIST and Canada's Cyber Security Strategy while offering additional guidance on addressing emerging threats. It should emphasize the importance of collaboration among stakeholders, including government agencies, industry leaders, and academia, to share knowledge and resources (Armenia, et al., 2021, Dupont, 2019, Elujide, et al., 2021). Furthermore, the framework should be designed to accommodate organizations of varying sizes and capabilities, ensuring that even resource-constrained entities can enhance their cybersecurity readiness.

By adopting a cybersecurity maturity model, organizations in the U.S. and Canada can achieve several critical outcomes. They can better align their security practices with industry standards and regulatory requirements, reducing the risk of non-compliance. They can also strengthen their ability to detect and respond to cyber incidents, minimizing the potential impact of attacks on their operations and reputation. Over time, these improvements can lead to increased trust among customers, partners, and stakeholders, further solidifying the organization's position in the market (Hussain, et al., 2021, Ike, et al., 2021).

In conclusion, cybersecurity maturity models are indispensable tools for improving cybersecurity readiness in organizations across the U.S. and Canada. By providing a structured approach to assessing and enhancing security capabilities, these models enable organizations to address current challenges and prepare for future threats. While existing frameworks such as NIST and Canada's Cyber Security Strategy offer valuable guidance, the development of an integrated and adaptable maturity framework is essential for overcoming their limitations and fostering a more secure digital ecosystem (Mishra, et al., 2022, Onoja, Ajala & Ige, 2022). Through continuous improvement and collaboration, organizations can build resilience against cyber threats, ensuring the protection of their assets, operations, and stakeholders.

3. Proposed Cybersecurity Maturity Framework (CMF)

The rapidly evolving cyber threat landscape demands that organizations continuously assess and improve their cybersecurity readiness. To effectively guide organizations in this endeavor, a Cybersecurity Maturity Framework (CMF) can provide a structured and systematic approach to enhance cybersecurity capabilities. The proposed CMF is designed to address the diverse needs of organizations in the U.S. and Canada, offering a roadmap for improving cybersecurity defenses while adapting to evolving risks (Austin-Gabriel, et al., 2021, Clarke & Knake, 2019, Oladosu, et al., 2021). The framework is based on five maturity levels, each corresponding to specific stages of development, and focuses on critical domains such as governance, threat intelligence, incident response, and workforce development. This structured approach enables organizations to assess their current cybersecurity posture, identify gaps, and implement targeted improvements to achieve long-term resilience.

The structure of the proposed CMF is built around five maturity levels: Initial, Developing, Established, Advanced, and Optimized. These levels represent the progression of an organization's cybersecurity capabilities, starting from basic and ad-hoc security practices to a highly integrated and proactive security posture. The Initial level represents organizations that have limited or no formal cybersecurity processes in place. At this stage, organizations are reactive, often responding to incidents as they arise without structured policies or strategies (Akinade, et al., 2022, Oladosu, et al., 2022, Ukwandu, et al., 2022). As organizations move through the Developing and Established levels, they begin to formalize their cybersecurity practices, implement basic security controls, and improve their response to incidents. The Advanced level reflects organizations that have robust cybersecurity processes, integrate advanced technologies, and proactively manage risk. Finally, the Optimized level represents organizations that have achieved a state of continuous improvement, with highly integrated security processes that are adaptive to emerging threats and seamlessly embedded into the organization's overall strategy.

The framework also identifies critical domains that are essential to building a mature cybersecurity posture. These domains include governance, threat intelligence, incident response, and workforce development. Governance encompasses the policies, procedures, and organizational structures that guide cybersecurity activities. It includes risk management frameworks, compliance with relevant standards, and the establishment of roles and responsibilities for cybersecurity across the organization (Austin-Gabriel, et al., 2021, Oladosu, et al., 2021). Threat intelligence involves the collection, analysis, and dissemination of information about potential threats, enabling organizations to anticipate and mitigate cyber risks before they materialize. Incident response focuses on the organization's ability to detect, contain, and recover from cyberattacks in a timely and effective manner, minimizing operational disruption and financial loss. Workforce development is crucial for ensuring that organizations have the necessary skills, knowledge, and training to manage cybersecurity challenges effectively. It includes initiatives for continuous education, certification, and awareness to cultivate a culture of cybersecurity throughout the organization.

Each maturity level within the framework is accompanied by defined benchmarks that organizations can use to assess their progress across these critical domains. At the Initial level, organizations may have rudimentary governance structures in place, with limited threat intelligence capabilities, ad-hoc incident response procedures, and a workforce with basic cybersecurity awareness (Aaronson & Leblond, 2018, Newlands, et al., 2020). As organizations progress through the Developing and Established levels, they implement more formalized policies, integrate basic threat intelligence tools, develop incident response plans, and provide basic cybersecurity training to their staff. The Advanced level represents organizations with comprehensive governance models, proactive threat intelligence capabilities, well-established incident response frameworks, and highly skilled cybersecurity teams. At the Optimized level, organizations continuously refine their cybersecurity practices, utilizing cutting-edge technologies, threat intelligence platforms, and advanced analytics to stay ahead of emerging threats. Figure. 3 shows the cyber-security assessment presented by Aboelfotoh & Hikal, 2019.

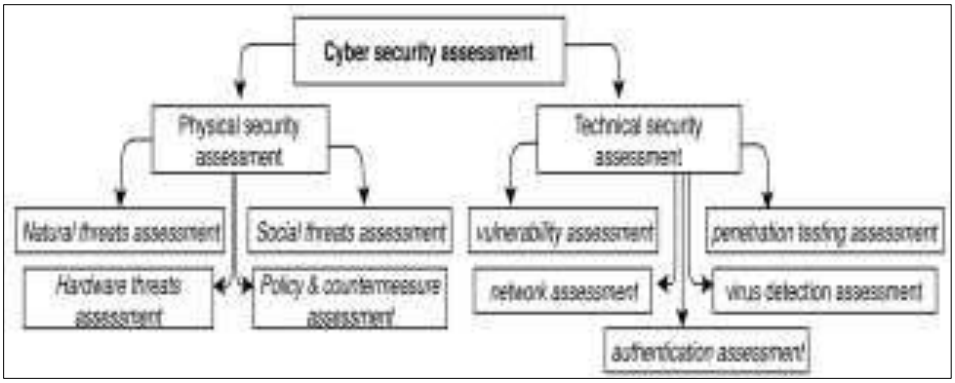

Figure 3 Cyber-security assessment (Aboelfotoh & Hikal, 2019)

One of the key aspects of the proposed CMF is its emphasis on risk management, technology integration, and human factors. Risk management is at the core of the framework, with organizations expected to identify, assess, and mitigate cybersecurity risks at every stage of maturity. At the Initial and Developing levels, organizations may focus primarily on mitigating immediate risks through basic security controls (Igo, 2020). As organizations mature, they shift toward a more proactive and strategic approach to risk management, incorporating risk assessments into their overall business continuity and disaster recovery plans.

Technology integration is another crucial element of the CMF. At lower maturity levels, organizations may rely on basic technology solutions such as firewalls and antivirus software. As they advance, they begin to integrate more sophisticated technologies such as intrusion detection systems (IDS), security information and event management (SIEM) platforms, and advanced analytics tools to enhance their security posture (Dwivedi, et al., 2020, Feng, 2019). The Optimized level represents organizations that fully integrate cybersecurity technologies into their overall IT infrastructure, utilizing automation, artificial intelligence, and machine learning to proactively detect and mitigate threats in real time.

Human factors play a central role in the success of any cybersecurity program. The CMF emphasizes the importance of workforce development and continuous training to ensure that employees are equipped to handle cybersecurity challenges. At lower maturity levels, organizations may focus on basic security awareness training and reactive incident response drills. As organizations mature, they begin to develop specialized cybersecurity teams, invest in professional development programs, and cultivate a culture of cybersecurity awareness throughout the organization (Bamberger & Mulligan, 2015, Voss & Houser, 2019). By the time organizations reach the Advanced and Optimized levels, cybersecurity is integrated into every facet of the organization, from executive decision-making to day-to-day operations.

The proposed CMF is designed to be adaptable for organizations of different sizes and across various industries. Small and medium-sized enterprises (SMEs) often face unique challenges, such as limited resources and personnel, which can make implementing a comprehensive cybersecurity program difficult. The CMF provides a tailored approach for SMEs, offering practical steps and benchmarks that are scalable and achievable within their constraints. For SMEs at the Initial or Developing levels, the framework suggests focusing on basic cybersecurity hygiene, such as regular software updates, employee training, and the use of strong passwords (Jathanna & Jagli, 2017). As these organizations mature, they can gradually adopt more advanced security practices and technologies.

Large enterprises, on the other hand, typically have more resources at their disposal but may face greater complexity in managing cybersecurity across multiple departments and regions. The CMF addresses the needs of large enterprises by emphasizing the integration of cybersecurity practices across the organization's structure. It encourages the development of centralized governance models, the establishment of dedicated cybersecurity teams, and the implementation of advanced security technologies that can scale to meet the demands of large, complex systems.

Critical sectors such as healthcare, finance, and energy require specialized cybersecurity measures due to the sensitive nature of the data and systems they manage. The CMF recognizes the importance of sector-specific risks and regulatory requirements, offering tailored recommendations for these industries (Bello, et al., 2021, Yang, et al., 2017). For example, healthcare organizations may need to prioritize the protection of patient data and comply with healthcare-specific regulations such as HIPAA, while financial institutions must focus on securing financial transactions and meeting compliance standards such as PCI DSS. The CMF provides sector-specific guidance, ensuring that organizations in these fields can address the unique cybersecurity challenges they face while advancing their overall maturity.

In conclusion, the proposed Cybersecurity Maturity Framework offers a comprehensive and adaptable approach for organizations in the U.S. and Canada to assess, enhance, and optimize their cybersecurity readiness. By focusing on key domains such as governance, threat intelligence, incident response, and workforce development, and providing a clear path through five maturity levels, the framework helps organizations achieve a higher level of security resilience. Its emphasis on risk management, technology integration, and human factors ensures that organizations can build a holistic cybersecurity posture that is both effective and sustainable. Whether for SMEs, large enterprises, or critical sectors, the framework offers the flexibility to meet the diverse needs of organizations, ultimately fostering a more secure digital environment for all.

4. Methodology

The methodology for developing and evaluating a Cybersecurity Maturity Framework (CMF) to improve cybersecurity readiness in organizations across the U.S. and Canada involves several key stages. These stages include the development of the framework, data collection from a variety of sectors, and the evaluation of organizational performance in implementing and advancing cybersecurity practices. Through a combination of literature review, consultations with industry experts, and the collection of data through surveys, interviews, and case studies, the methodology ensures that the framework is both comprehensive and adaptable to the needs of diverse organizations. Additionally, performance indicators and evaluation metrics will be defined to assess the effectiveness of the proposed framework in enhancing cybersecurity preparedness.

The development of the framework begins with an extensive literature review of existing cybersecurity frameworks and best practices. This process involves reviewing a wide array of academic articles, industry reports, government documents, and international standards that outline the principles, guidelines, and strategies for cybersecurity improvement (Cherdantseva, et al., 2016, Kaplan & Mikes, 2016, Yang, et al., 2017). By analyzing frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and other internationally recognized cybersecurity standards, the goal is to identify gaps, challenges, and opportunities for improvement in existing models. Through this review, the development team can assess the effectiveness of current cybersecurity practices and determine how best to tailor the maturity framework for organizations in the U.S. and Canada. This step also includes examining case studies of organizations that have successfully implemented cybersecurity maturity models, identifying common practices and lessons learned that can inform the proposed CMF.

Consultation with cybersecurity experts and industry stakeholders plays a pivotal role in refining the framework. Engaging experts from a variety of sectors such as healthcare, finance, energy, and government ensures that the framework addresses sector-specific needs and regulatory requirements. These consultations provide valuable insights into the unique challenges organizations face in implementing cybersecurity measures and the evolving nature of cyber threats (Atkins & Lawson, 2021, Robinson, 2020). Interviews and discussions with professionals in the field help to align the framework with industry expectations and current trends. Input from these stakeholders also informs decisions about the most critical domains to focus on within the framework, ensuring that it addresses the most pressing cybersecurity concerns for different organizations.

The next step in the methodology is the collection of data from organizations across different sectors. Surveys and interviews will be conducted to gather a wide range of perspectives on the current state of cybersecurity readiness in these organizations. These data collection methods will be designed to capture detailed information about the cybersecurity practices, challenges, and needs of organizations operating in critical sectors such as healthcare, finance, and energy. By including a broad spectrum of participants, the survey and interview process allows for the identification

of sector-specific cybersecurity challenges as well as common themes that span multiple industries (Lanz, 2022, Shackelford, Russell & Haut, 2015, Shackelford, et al., 2015). Participants will be asked about their current cybersecurity policies, the maturity of their cybersecurity practices, and the obstacles they encounter when attempting to improve their cybersecurity posture. This information will be used to inform the structure and design of the maturity framework, ensuring that it is tailored to the real-world needs of organizations.

In addition to surveys and interviews, case studies of organizations that have successfully used maturity models for cybersecurity improvement will be analyzed. These case studies provide in-depth examples of how organizations have progressed through different maturity levels and the outcomes they have achieved as a result. By studying these cases, the development team can identify best practices, lessons learned, and successful strategies for overcoming common barriers to cybersecurity improvement (Atkins & Lawson, 2021, Cohen, et al., 2022, Sabillon, Cavaller & Cano, 2016). This analysis also allows for the identification of common challenges that organizations face when trying to advance through the maturity levels, such as resource limitations, cultural resistance, or lack of skilled personnel. Understanding these challenges will help refine the proposed CMF to make it more applicable and actionable for organizations at various stages of maturity.

The final stage of the methodology involves the establishment of evaluation metrics to assess the effectiveness of the proposed framework. Performance indicators will be defined to measure how well organizations are performing in terms of their cybersecurity maturity and readiness. These indicators include metrics such as incident detection rates, response times, and resilience measures (Abraham, Chatterjee & Sims, 2019, Ustundag, et al., 2018). Incident detection rates refer to the organization's ability to identify and detect cyber threats before they cause significant damage. Response times are an important metric that measures how quickly an organization can react to and mitigate a cyberattack once it has been detected. Resilience measures assess the organization’s ability to recover from a cyberattack, minimizing the impact on operations and ensuring business continuity. These performance indicators will be tracked over time to assess organizational progress in adopting cybersecurity best practices and technologies.

Another key aspect of the evaluation process is measuring organizational progress in adopting cybersecurity best practices and technologies. This includes tracking the implementation of critical cybersecurity controls, the integration of advanced technologies such as security information and event management (SIEM) systems, intrusion detection systems (IDS), and threat intelligence platforms. Evaluating the adoption of best practices, such as regular risk assessments, employee training, and the implementation of multi-factor authentication (MFA), provides insight into how effectively organizations are improving their overall cybersecurity posture (Ani, He & Tiwari, 2017, Djenna, Harous & Saidouni, 2021). Furthermore, the evaluation metrics will help determine whether the organizations are progressing through the different maturity levels, from Initial to Optimized, and if they are making meaningful improvements in terms of governance, threat intelligence, incident response, and workforce development.

Throughout the data collection and evaluation process, feedback loops will be established to allow for continuous refinement of the CMF. As organizations implement the framework and track their progress, ongoing evaluations will help identify any gaps in the framework’s effectiveness. These feedback mechanisms ensure that the framework remains adaptable to the changing cyber threat landscape and continues to meet the evolving needs of organizations in both the U.S. and Canada.

The methodology for developing and evaluating the Cybersecurity Maturity Framework aims to ensure that the final product is practical, actionable, and evidence-based. By incorporating input from a wide range of experts and stakeholders, analyzing real-world case studies, and gathering data from organizations across multiple sectors, the CMF will be a comprehensive tool that organizations can use to improve their cybersecurity readiness (Smart, 2017, Yeung, et al., 2017). Furthermore, the use of clear performance indicators and evaluation metrics allows for the ongoing assessment of organizational progress, ensuring that organizations are continuously improving and adapting their cybersecurity practices to stay ahead of emerging threats. Ultimately, the methodology provides a robust foundation for improving cybersecurity resilience in organizations across the U.S. and Canada.

5. Application of the CMF

The application of the Cybersecurity Maturity Framework (CMF) in organizations across the U.S. and Canada demonstrates its potential to enhance cybersecurity readiness, resilience, and operational efficiency. This section explores the implementation of the CMF, with a focus on case studies in small and medium-sized enterprises (SMEs) as well as large enterprises in critical infrastructure sectors. Through these case studies, we analyze the improvements in cybersecurity readiness and the lessons learned from applying the CMF. Additionally, we discuss the results and findings

of implementing the CMF across different organizations, highlighting the tangible benefits and challenges that organizations face.

In both small and large enterprises, the application of the CMF helps organizations assess their cybersecurity maturity and provides a clear roadmap for improving their cybersecurity posture. SMEs often face unique challenges, including limited resources and budget constraints. However, by applying the CMF, these organizations can prioritize their cybersecurity investments based on their current maturity level, thus ensuring they achieve meaningful improvements over time without overwhelming their limited resources. For example, an SME in the healthcare sector may begin at an initial maturity level, focusing on establishing basic cybersecurity practices such as endpoint protection, user awareness training, and basic incident response protocols (Flores, 2019, Park, 2015). As the organization progresses through the maturity levels, it can implement more advanced measures, including threat intelligence integration, advanced incident response frameworks, and automated security tools.

For large enterprises, particularly those in critical infrastructure sectors such as energy, finance, and healthcare, the CMF offers a structured approach to addressing complex cybersecurity challenges. These organizations often have more sophisticated security systems in place but face heightened risks due to the nature of their operations. The application of the CMF in these organizations helps ensure that their cybersecurity strategies are aligned with industry standards and best practices, improving their resilience against cyberattacks (Callaghan, 2018, Trew, 2021). In a large financial institution, for example, the CMF might help identify gaps in threat intelligence integration, leading to the adoption of more advanced security technologies such as machine learning-based anomaly detection systems. Additionally, large enterprises can leverage the CMF to assess their governance structures, ensuring that cybersecurity policies and practices are consistently enforced across the organization.

One key aspect of the CMF application is its ability to drive improvements in cybersecurity readiness over time. Through its five maturity levels—Initial, Developing, Established, Advanced, and Optimized—the framework provides organizations with a clear pathway for continuous improvement. As organizations progress through the levels, they develop a more comprehensive and effective cybersecurity posture (Al-Hassan, et al., 2020, Haugh, 2018, Zaccari, 2016). Case studies show that organizations that have implemented the CMF see significant improvements in their ability to detect and respond to cyber threats. For instance, a large energy company that adopted the CMF in its operations saw a notable increase in its incident detection rates. The organization implemented advanced intrusion detection systems (IDS) and security information and event management (SIEM) platforms, allowing it to identify and mitigate cyber threats more quickly (Aliyu, et al., 2020, Brown, 2018, Miron, 2015). This enhanced detection capability, coupled with a more streamlined and efficient response process, significantly reduced the time it took to address security incidents and minimized the potential impact on operations.

Similarly, organizations applying the CMF report faster response times and improved resilience during cyberattacks. A case study involving an SME in the financial sector revealed that the organization's response times to cyber incidents were drastically reduced after adopting the CMF. The organization had implemented a formal incident response plan, which included predefined procedures for identifying, containing, and mitigating security breaches. This preparedness, driven by the CMF's focus on incident response, allowed the SME to recover quickly from a ransomware attack, minimizing the impact on customer data and business continuity (Ele & Oko, 2016, Nicho, et al., 2017, Papazafeiropoulou & Spanaki, 2016).

The enhanced resilience against cyberattacks is another key outcome of CMF application. Organizations that have adopted the framework report increased business continuity and reduced downtime in the aftermath of cyber incidents. For example, a healthcare organization that had implemented the CMF saw improvements in its ability to maintain essential operations during a cyberattack. The organization had invested in business continuity planning and disaster recovery measures, which ensured that critical healthcare services continued uninterrupted, even when the organization was under attack. This resilience was particularly important in the healthcare sector, where downtime can have severe consequences for patient care and safety.

Despite the significant improvements in cybersecurity readiness, the application of the CMF is not without its challenges. One of the primary challenges organizations face is the need for sufficient resources to implement the framework effectively. While SMEs may struggle with limited budgets and staffing, larger enterprises often face challenges in coordinating the implementation of the CMF across diverse departments and business units (Recor & Xu, 2016, Sanaei, et al., 2016, Sikdar, 2021). The complexity of managing cybersecurity at scale in large organizations requires a high level of coordination and communication between teams, and ensuring that all stakeholders are on board with the framework can be challenging. Additionally, the evolving nature of cyber threats presents another challenge. Cybercriminals are constantly developing new techniques, and organizations must continuously adapt their

cybersecurity practices to stay ahead of these threats. While the CMF offers a structured approach for improvement, organizations must remain agile and proactive in their cybersecurity efforts.

Another challenge identified in applying the CMF is the need for ongoing training and workforce development. As organizations advance through the maturity levels, they often need to invest in upskilling their workforce to handle more sophisticated cybersecurity tools and processes. This requires both time and resources, and organizations may encounter resistance to change from employees who are unfamiliar with new technologies or practices. However, organizations that have successfully applied the CMF report that employee engagement and training are key to achieving lasting improvements in cybersecurity readiness (Govindji, Peko & Sundaram, 2018023). Workforce development, which is a critical component of the CMF, ensures that employees are equipped with the knowledge and skills to identify and respond to cyber threats, thus strengthening the organization's overall cybersecurity posture.

The benefits of applying the CMF across organizations are evident in the improvements seen in their cybersecurity practices. These benefits include enhanced detection capabilities, faster response times, and greater resilience against cyberattacks. Organizations that have implemented the CMF have reported better alignment with industry standards, improved governance structures, and the successful integration of advanced security technologies (AlDaajeh, et al., 2022, Miron & Muita, 2014). These improvements translate into reduced risk exposure, minimized downtime, and enhanced business continuity, all of which contribute to a stronger overall cybersecurity posture. At the same time, the challenges faced by organizations, including resource limitations, workforce development needs, and the evolving threat landscape, highlight the importance of a tailored approach to implementing the CMF. By addressing these challenges and leveraging the benefits of the CMF, organizations in the U.S. and Canada can improve their cybersecurity readiness and better prepare for the growing threat of cyberattacks.

6. Challenges in Enhancing Cybersecurity Readiness

Enhancing cybersecurity readiness is a crucial objective for organizations in both the U.S. and Canada, particularly as the threat landscape continues to evolve. However, there are numerous challenges that organizations face in strengthening their cybersecurity defenses and adopting a Cybersecurity Maturity Framework (CMF). These challenges, while varied, are common across industries and sectors, impacting organizations regardless of their size or domain. Among these challenges are resource limitations, resistance to change, and the complexities of aligning cybersecurity practices with legal and compliance requirements (Flores, 2019, Park, 2015). Addressing these challenges is critical to improving cybersecurity maturity and ensuring organizations are better prepared to defend against cyber threats.

One of the most significant barriers to enhancing cybersecurity readiness is resource limitations, particularly for small and medium-sized enterprises (SMEs). SMEs often face constraints in both financial resources and human capital, making it difficult to implement comprehensive cybersecurity measures. Unlike large enterprises that can allocate substantial budgets to cybersecurity initiatives, SMEs typically have to operate within tight financial limits (Callaghan, 2018, Trew, 2021). This resource constraint can make it challenging for SMEs to invest in necessary security tools, technologies, and personnel to adequately protect their networks and data. While cybersecurity maturity models, such as the CMF, provide a structured approach to improving cybersecurity readiness, SMEs may find it difficult to prioritize cybersecurity improvements when faced with competing demands on their limited resources.

For example, investing in advanced cybersecurity technologies like intrusion detection systems (IDS), security information and event management (SIEM) platforms, or machine learning-based threat detection tools may seem out of reach for SMEs due to the high costs associated with these solutions. Similarly, hiring skilled cybersecurity professionals or providing regular cybersecurity training to employees may be perceived as too expensive or time-consuming for organizations operating with lean teams (Ele & Oko, 2016, Nicho, et al., 2017, Papazafeiropoulou & Spanaki, 2016). As a result, SMEs may find themselves at a disadvantage when competing against larger enterprises in terms of cybersecurity preparedness, leaving them more vulnerable to cyberattacks.

Another significant challenge in enhancing cybersecurity readiness is the resistance to change within organizations, especially when it comes to shifting organizational culture and implementing new cybersecurity practices. Many organizations face internal resistance when attempting to adopt new frameworks, tools, or processes, and this resistance is often fueled by a lack of awareness or understanding of cybersecurity risks. Employees may perceive cybersecurity practices as cumbersome or irrelevant to their day-to-day work, leading to a lack of buy-in from key stakeholders (Aliyu, et al., 2020, Brown, 2018, Miron, 2015). This resistance is particularly prevalent in organizations where cybersecurity is not seen as a strategic priority and is instead treated as a technical issue handled by IT departments alone.

The lack of cybersecurity expertise within organizations can also exacerbate this resistance to change. Many organizations, particularly SMEs, struggle to recruit and retain skilled cybersecurity professionals. The cybersecurity skills gap is a well-documented issue, with a shortage of qualified professionals to meet the growing demand for cybersecurity expertise. This shortage is particularly problematic for organizations attempting to implement and sustain a CMF, as successful implementation requires a deep understanding of cybersecurity principles, tools, and practices. Without the necessary expertise, organizations may struggle to properly assess their maturity level, identify gaps in their cybersecurity practices, or make informed decisions about security investments. This lack of expertise also makes it difficult for organizations to train employees or develop the necessary internal capabilities to defend against cyber threats.

The absence of cybersecurity expertise can also hinder an organization's ability to stay current with emerging threats and evolving attack techniques. Cybercriminals are continually developing new methods to exploit vulnerabilities in organizational systems, and organizations must remain agile and proactive in adapting their defenses. Without a skilled cybersecurity team, organizations may struggle to implement necessary changes in response to new threats, which can leave them vulnerable to cyberattacks.

In addition to resource limitations and resistance to change, organizations also face legal and compliance challenges when trying to enhance their cybersecurity readiness. Both the U.S. and Canada have established a range of regulations and standards designed to ensure the protection of sensitive data and critical infrastructure. For organizations to improve their cybersecurity posture effectively, they must ensure that their practices align with regional regulations and cybersecurity standards. Failure to comply with these regulations can result in severe consequences, including fines, reputational damage, and legal liabilities.

In the U.S., for example, regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Modernization Act (FISMA) impose strict requirements on organizations handling sensitive data, particularly in sectors like healthcare and government. Organizations must implement robust cybersecurity controls and demonstrate compliance with these regulations to avoid penalties (Ele & Oko, 2016, Nicho, et al., 2017, Papazafeiropoulou & Spanaki, 2016). Similarly, Canada has its own set of cybersecurity regulations, such as the Personal Information Protection and Electronic Documents Act (PIPEDA), which governs the collection, use, and disclosure of personal information in the private sector. Organizations must ensure that their cybersecurity practices comply with these regulations, which can be a complex and resource-intensive task.

The challenge of ensuring alignment with these regulations is compounded by the dynamic nature of cybersecurity standards. As cyber threats continue to evolve, regulations and standards must also adapt to address emerging risks. This creates a challenge for organizations attempting to stay compliant while simultaneously improving their cybersecurity posture. For instance, organizations may face difficulties in understanding and implementing the latest cybersecurity requirements or ensuring that their systems remain in compliance as new laws and standards are enacted (Aliyu, et al., 2020, Brown, 2018, Miron, 2015). This can be particularly challenging for organizations operating across both the U.S. and Canada, as they must navigate different regulatory environments and ensure compliance with both sets of regulations.

In addition to navigating legal and compliance challenges, organizations must also contend with the complexity of integrating cybersecurity practices into their existing operations. Many organizations have legacy systems or processes that may not be compatible with modern cybersecurity tools and practices. For example, an organization that still relies on outdated software or hardware may find it difficult to implement newer, more effective cybersecurity solutions. Additionally, the process of updating or replacing legacy systems can be costly and time-consuming, which further complicates the task of improving cybersecurity readiness.

To address these challenges, organizations must take a holistic approach to cybersecurity that includes not only technical measures but also a strong emphasis on governance, culture, and workforce development. This approach requires a commitment from senior leadership to prioritize cybersecurity as a strategic objective and ensure that resources are allocated appropriately. Additionally, organizations must invest in ongoing employee training to foster a culture of cybersecurity awareness and responsibility. By empowering employees to recognize and respond to cyber threats, organizations can improve their overall cybersecurity posture and reduce the risk of successful attacks.

In conclusion, enhancing cybersecurity readiness with a maturity framework is a complex process that requires overcoming several significant challenges. Resource limitations, resistance to change, and the need to navigate legal and compliance requirements are all barriers that organizations in the U.S. and Canada must address to improve their cybersecurity defenses (Ele & Oko, 2016, Nicho, et al., 2017, Papazafeiropoulou & Spanaki, 2016). By adopting a

comprehensive approach that includes investing in technology, developing internal expertise, fostering a culture of cybersecurity, and ensuring compliance with regulations, organizations can make meaningful strides toward improving their cybersecurity maturity and better protecting their critical assets.

6.1. Recommendations for Enhancing Cybersecurity Readiness

To enhance cybersecurity readiness within organizations across the U.S. and Canada, strategic and policy-driven approaches are essential to overcoming the barriers to effective implementation. Organizations face a dynamic and increasingly sophisticated threat landscape, and adopting a maturity framework, such as the Cybersecurity Maturity Framework (CMF), is vital to strengthening cybersecurity defenses (Aliyu, et al., 2020, Brown, 2018, Miron, 2015). However, simply adopting a framework is not enough—organizations must take proactive steps to embed cybersecurity into their culture, invest in ongoing training, and foster collaboration across public and private sectors. These efforts should be accompanied by strong policy and governance initiatives to support the development of a robust cybersecurity infrastructure that addresses emerging threats and enhances organizational resilience.

A key recommendation for enhancing cybersecurity readiness is the development of a strong organizational culture of cybersecurity. Organizations in both the U.S. and Canada must prioritize cybersecurity as an integral component of their overall strategy. Cybersecurity should not be seen as the responsibility of the IT department alone but as a shared responsibility that spans the entire organization, from leadership to front-line employees. This cultural shift requires active leadership engagement, clear communication, and a commitment to making cybersecurity a core value (Burke, et al., 2019, Demchak, et al., 2016, Kour, Karim & Thaduri, 2020). Senior leaders must lead by example, demonstrating the importance of cybersecurity and ensuring it is embedded in every aspect of organizational operations. This cultural transformation can be achieved through consistent messaging, reinforced policies, and the establishment of cybersecurity as a critical performance metric.

Building a culture of cybersecurity also involves encouraging employees to view cybersecurity as part of their everyday responsibilities. Security should be seen as everyone's responsibility, not just that of IT specialists. This cultural shift can be supported through clear policies that mandate secure behaviors, such as the use of strong passwords, regular system updates, and adherence to data protection protocols. Furthermore, organizations should establish channels for employees to report potential security incidents and provide them with the tools and training needed to identify and mitigate risks.

Ongoing training and awareness programs are essential components of an effective cybersecurity readiness strategy. Given the rapid evolution of cyber threats, organizations must ensure that their workforce remains up to date with the latest cybersecurity trends and best practices. These programs should not be one-time events but should be part of an ongoing, proactive effort to continuously build the cybersecurity capabilities of employees at all levels (Pawar & Palivela, 2022, Sabillon, et al., 2017, Shackelford, Russell & Haut, 2015). Training programs should be tailored to different roles within the organization, with more in-depth technical training for IT and security staff and awareness programs for non-technical employees to recognize phishing attempts, social engineering tactics, and other common forms of cyberattacks.

In addition to formal training, organizations should cultivate a habit of cybersecurity awareness through regular simulations and awareness campaigns. For example, conducting simulated phishing attacks can help employees practice identifying and responding to phishing emails in a controlled environment. This type of training not only improves the technical competence of employees but also reinforces the importance of cybersecurity in the organizational culture. Awareness programs should be designed to engage employees regularly, keeping them informed about the latest threats, security policies, and best practices for maintaining a secure work environment.

At the policy level, organizations should engage in public-private collaboration to improve cybersecurity resilience. Cyber threats are increasingly global in nature, and no organization can effectively address them alone. Public-private partnerships provide opportunities for sharing threat intelligence, leveraging resources, and addressing cybersecurity challenges in a coordinated manner (Franco, Lacerda & Stiller, 2022, Georgiadou, Mouzakitis & Askounis, 2021, Knowles, et al., 2015). Collaboration between government agencies, private companies, and industry groups can help facilitate the exchange of information about emerging threats, attack techniques, and vulnerabilities. This information-sharing network can help organizations stay ahead of cybercriminals and improve their ability to prevent, detect, and respond to attacks.

Governments in both the U.S. and Canada have already established cybersecurity strategies aimed at promoting national security and protecting critical infrastructure. These strategies provide a foundation for public-private collaboration,

but more can be done to strengthen these partnerships. For instance, creating cybersecurity information-sharing platforms and regular forums for discussion between public and private sectors can facilitate the exchange of insights, best practices, and lessons learned (Aboelfotoh & Hikal, 2019, Garrett, 2018, Shackelford, et al., 2015). These partnerships should focus not only on threat intelligence but also on the development of cybersecurity technologies and frameworks that can be adopted by organizations across various industries.

Another important aspect of improving cybersecurity readiness is encouraging investment in cybersecurity technologies and workforce development. As the cybersecurity landscape becomes more complex, organizations must invest in advanced security technologies to protect their networks, data, and systems. This includes investing in solutions like endpoint detection and response (EDR), intrusion prevention systems (IPS), encryption tools, and cloud security platforms (Malhotra, 2018, Mishra, 2022, McCubbrey, 2020). However, technology alone is not enough. Organizations must also invest in developing a skilled cybersecurity workforce capable of managing and responding to increasingly sophisticated threats.

Governments and industry bodies can play a critical role in supporting these investments. Policy recommendations include incentivizing businesses to invest in cybersecurity technologies through tax breaks, grants, and other financial incentives. Additionally, governments can encourage workforce development by supporting cybersecurity education and training programs, especially in high-demand fields such as network security, incident response, and digital forensics (Celeste & Fabbrini, 2020, Mattoo & Meltzer, 2018, Tehrani, Sabaruddin & Ramanathan, 2018). Collaboration with educational institutions to develop and promote cybersecurity curricula can help ensure that the future workforce is equipped with the necessary skills to meet evolving cybersecurity challenges.

Cybersecurity workforce development should also include initiatives aimed at diversifying the talent pool. The cybersecurity industry faces a significant skills gap, and efforts must be made to attract a broader range of talent to the field. This can be achieved by offering training programs and career pathways to underrepresented groups, including women, minorities, and veterans. By promoting inclusivity and expanding the talent pipeline, organizations will have access to a broader pool of skilled professionals to strengthen their cybersecurity defenses.

Moreover, organizations should adopt a risk-based approach to cybersecurity, focusing resources on protecting their most critical assets. The development of a cybersecurity maturity framework can help organizations assess their current cybersecurity posture, identify vulnerabilities, and prioritize investments based on the likelihood and potential impact of cyberattacks (Chin & Zhao, 2022, Minssen, et al., 2020, Tian, 2016). By continuously improving their cybersecurity maturity, organizations can reduce their risk exposure, enhance their ability to detect and respond to threats, and ensure business continuity in the event of an incident.

At the governance level, organizations should also ensure that cybersecurity is aligned with business objectives and integrated into broader organizational governance structures. This includes establishing clear cybersecurity policies, assigning dedicated resources to cybersecurity management, and regularly reporting on cybersecurity performance to senior leadership. By embedding cybersecurity into corporate governance, organizations can ensure that cybersecurity initiatives are given the necessary attention and resources to succeed.

Finally, organizations must remain adaptable and resilient in the face of evolving cyber threats. This requires a commitment to continuous improvement and the ability to respond quickly to new vulnerabilities and attack techniques. A flexible cybersecurity strategy should allow organizations to scale their defenses as needed, adapt to emerging threats, and ensure that cybersecurity practices evolve in line with technological advancements and changing business needs.

In conclusion, enhancing cybersecurity readiness through a maturity framework requires strategic approaches that embed cybersecurity into the organizational culture, invest in training, foster public-private collaboration, and promote investment in cybersecurity technologies and workforce development (Fefer, 2019, Sullivan, 2019, Voss, 2019). By addressing these recommendations, organizations in the U.S. and Canada can improve their cybersecurity posture, strengthen their defenses against cyber threats, and ensure resilience in the face of an ever-changing threat landscape.

7. Conclusion

In conclusion, the Cybersecurity Maturity Framework (CMF) presents a comprehensive and structured approach for organizations in the U.S. and Canada to enhance their cybersecurity readiness. By focusing on key domains such as governance, threat intelligence, incident response, and workforce development, the CMF helps organizations assess their current cybersecurity posture, identify gaps, and implement improvements across various levels of maturity. The

framework provides a clear pathway for organizations to progressively strengthen their defenses, fostering continuous improvement and resilience against the evolving landscape of cyber threats.

The impact of adopting the CMF is profound, as it enables organizations to align their cybersecurity efforts with industry best practices and recognized standards. It supports the development of a robust cybersecurity culture and empowers organizations to better manage risks, respond effectively to incidents, and mitigate potential damages. Furthermore, by tailoring the framework to fit the needs of different organizations, from SMEs to large enterprises and critical sectors, the CMF ensures that cybersecurity readiness is scalable and adaptable to the specific context of each organization.

As the cyber threat landscape continues to evolve with increasing sophistication and frequency of attacks, the need for a maturity-based approach to cybersecurity is more critical than ever. A maturity framework allows organizations to move beyond reactive measures, focusing on proactive preparedness and resilience. By adopting such an approach, organizations are better positioned to adapt to emerging threats, ensuring that their cybersecurity practices evolve in tandem with technological advancements and changing business needs. Ultimately, the CMF offers a strategic tool that can significantly enhance an organization's ability to protect its assets, maintain business continuity, and safeguard its reputation in an increasingly digital world.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law*, *21*(2), 245-272.

[2] Aboelfotoh, S. F., & Hikal, N. A. (2019). A review of cyber-security measuring and assessment methods for modern enterprises. *JOIV: International Journal on Informatics Visualization*, *3*(2), 157-176.

[3] Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business horizons*, *62*(4), 539-548.

[4] Adepoju, P. A., Austin-Gabriel, B., Ige, A. B., Hussain, N. Y., Amoo, O. O., & Afolabi, A. I. (2022). Machine learning innovations for enhancing quantum-resistant cryptographic protocols in secure communication. *Open Access Research Journal of Multidisciplinary Studies*. https://doi.org/10.53022/oarjms.2022.4.1.0075

[5] Akinade, A. O., Adepoju, P. A., Ige, A. B., & Afolabi, A. I. (2022). Advancing segment routing technology: A new model for scalable and low-latency IP/MPLS backbone optimization. *Open Access Research Journal of Science and Technology*.

[6] Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(10), 8176-8206.

[7] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754.

[8] Al-Hassan, A., Burfisher, M. E., Chow, M. J. T., Ding, D., Di Vittorio, F., Kovtun, D., ... & Youssef, K. (2020). *Is the whole greater than the sum of its parts? Strengthening caribbean regional integration*. International Monetary Fund.

[9] Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, *10*(10), 3660.

[10] Amin, Z. (2019). A practical road map for assessing cyber risk. *Journal of Risk Research*, *22*(1), 32-43.

[11] Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32-74.

[12] Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580.

[13] Atkins, S., & Lawson, C. (2021). An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review*, *81*(5), 847-861.

[14] Atkins, S., & Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity*, *7*(1), tyab024.

[15] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. *Open Access Research Journal of Engineering and Technology*. https://doi.org/10.53022/oarjet.2021.1.1.0107

[16] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. *Open Access Research Journal of Engineering and Technology*. https://doi.org/10.53022/oarjet.2021.1.1.0107

[17] Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the ground: driving corporate behavior in the United States and Europe*. MIT Press.

[18] Bello, O. A., Folorunso, A., Ogundipe, A., Kazeem, O., Budale, A., Zainab, F., & Ejiofor, O. E. (2022). Enhancing Cyber Financial Fraud Detection Using Deep Learning Techniques: A Study on Neural Networks and Anomaly Detection. International Journal of Network and Communication Research, 7(1), 90-113.

[19] Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441.

[20] Bodeau, D. J., McCollum, C. D., & Fox, D. B. (2018). Cyber threat modeling: Survey, assessment, and representative framework. *Mitre Corp, Mclean*, 2021-11.

[21] Brown, R. D. (2018). Towards a Qatar cybersecurity capability maturity model with a legislative framework. *International Review of Law*.

[22] Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.

[23] Burke, W., Oseni, T., Jolfaei, A., & Gondal, I. (2019, January). Cybersecurity indexes for eHealth. In *Proceedings of the australasian computer science week multiconference* (pp. 1-8).

[24] Callaghan, R. (2018). *The impact of protectionism on the completion and duration of cross-border acquisitions* (Doctoral dissertation, Open Access Te Herenga Waka-Victoria University of Wellington).

[25] Celeste, E., & Fabbrini, F. (2020). Competing jurisdictions: Data privacy across the borders. *Data Privacy and Trust in Cloud Computing*, 43-58.

[26] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, 1-27.

[27] Chin, Y. C., & Zhao, J. (2022). Governing cross-border data flows: International trade agreements and their limits. *Laws*, *11*(4), 63.

[28] Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin.

[29] Clemente, J. F. (2018). *Cyber security for critical energy infrastructure* (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

[30] Cohen, N., Hulvey, R., Mongkolnchaiarunya, J., Novak, A., Morgus, R., & Segal, A. (2022). *Cybersecurity as an Engine for Growth*. New America..

[31] Cohen, S. A. (2019). Cybersecurity for critical infrastructure: addressing threats and vulnerabilities in Canada.

[32] Dalal, A., Abdul, S., & Mahjabeen, F. (2016). Leveraging Artificial Intelligence for Cyber Threat Intelligence: Perspectives from the US, Canada, and Japan. *Revista de Inteligencia Artificial en Medicina*, *7*(1), 18-28.

[33] Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2016). Cyber readiness at a glance. *Potomac Institute for Policy Studies*, 1-44.

[34] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580.

[35] Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013.

[36] Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., ... & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International journal of information management*, *55*, 102211.

[37] Ele, S. I., & Oko, J. O. (2016). Governance, risk and compliance (Grc): a. *Journal of Integrative Humanism*, *6*(1), 161.

[38] Elujide, I., Fashoto, S. G., Fashoto, B., Mbunge, E., Folorunso, S. O., & Olamijuwon, J. O. (2021). Application of deep and machine learning techniques for multi-label classification performance on psychotic disorder diseases. Informatics in Medicine Unlocked, 23, 100545.

[39] Elujide, I., Fashoto, S. G., Fashoto, B., Mbunge, E., Folorunso, S. O., & Olamijuwon, J. O. (2021). Informatics in Medicine Unlocked.

[40] Fefer, R. F. (2019). Data flows, online privacy, and trade policy. *Congressional Research Service*.

[41] Feng, Y. (2019). The future of China's personal data protection law: challenges and prospects. *Asia Pacific Law Review*, *27*(1), 62-82.

[42] Flores, M. C. (2019). Challenges for Macroprudential Policy in the Euro Area: Cross-Border Spillovers and Governance Issues.

[43] Franco, M. F., Lacerda, F. M., & Stiller, B. (2022). A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises. *Revista de Gestão e Projetos*, *13*(3), 10-37.

[44] Garrett, G. A. (2018). *Cybersecurity in the Digital Age: Tools, Techniques, & Best Practices*. Aspen Publishers.

[45] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9), 3267.

[46] Govindji, S., Peko, G., & Sundaram, D. (2018). A context adaptive framework for IT governance, risk, compliance and security. In *Context-Aware Systems and Applications, and Nature of Computation and Communication: 6th International Conference, ICCASA 2017, and 3rd International Conference, ICTCC 2017, Tam Ky, Vietnam, November 23-24, 2017, Proceedings 6* (pp. 14-24). Springer International Publishing.

[47] Haugh, T. (2018). Harmonizing governance, risk management, and compliance through the paradigm of behavioral ethics risk. *U. Pa. J. Bus. L.*, *21*, 873.

[48] Hussain, N. Y., Austin-Gabriel, B., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). AI-driven predictive analytics for proactive security and optimization in critical infrastructure systems. *Open Access Research Journal of Science and Technology*. https://doi.org/10.53022/oarjst.2021.2.2.0059

[49] Ige, A. B., Austin-Gabriel, B., Hussain, N. Y., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Developing multimodal AI systems for comprehensive threat detection and geospatial risk mitigation. *Open Access Research Journal of Science and Technology,* 6(1), 63. https://doi.org/10.53022/oarjst.2022.6.1.0063

[50] Igo, S. E. (2020). The known citizen: A history of privacy in modern America. Harvard University Press.

[51] Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. Magna Scientia Advanced Research and Reviews, 2(1), 074–086. https://doi.org/10.30574/msarr.2021.2.1.0032

[52] Jathanna, R., & Jagli, D. (2017). Cloud computing and security issues. International *Journal of Engineering Research and Applications*, *7*(6), 31-38.

[53] Kaplan, R. S., & Mikes, A. (2016). Risk management—The revealing hand. *Journal of Applied Corporate Finance*, *28*(1), 8-18.

[54] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, *9*, 52-80.

[55] Kour, R., Karim, R., & Thaduri, A. (2020). Cybersecurity for railways–A maturity model. *Proceedings of the institution of mechanical engineers, Part F: Journal of Rail and Rapid Transit*, *234*(10), 1129-1148.

[56] Kovacevic, A., & Nikolic, D. (2015). Cyber attacks on critical infrastructure: Review and challenges. *Handbook of research on digital crime, cyberspace security, and information assurance*, 1-18.

[57] Laidlaw, E. (2021). Privacy and cybersecurity in digital trade: The challenge of cross border data flows. *Available at SSRN 3790936*.

[58] Lanz, Z. (2022). Cybersecurity risk in US critical infrastructure: An analysis of publicly available US government alerts and advisories. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(1), 43-70.

[59] Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.

[60] Malhotra, Y. (2018). Bridging networks, systems and controls frameworks for cybersecurity curriculums and standards development. *Journal of Operational Risk*, *13*(1).

[61] Mattoo, A., & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law*, *21*(4), 769-789.

[62] McCubbrey, D. S. (2020). *Cybersecurity Penetration Assessments in the Context of a Global Cybersecurity Skills Gap* (Doctoral dissertation, Capella University).

[63] Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019, November). Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals. In *2019 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-13). IEEE.

[64] Minssen, T., Seitz, C., Aboy, M., & Compagnucci, M. C. (2020). The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR: What are the legal challenges and how might these affect cloud-based technologies, big data, and AI in the medical sector?. *EPLR*, *4*, 34.

[65] Miron, W. R. (2015). *Adoption of Cybersecurity Capability Maturity Models in Municipal Governments* (Doctoral dissertation, Carleton University).

[66] Miron, W., & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review*, *4*(10), 33.

[67] Mishra, A. (2022). *Modern Cybersecurity Strategies for Enterprises: Protect and Secure Your Enterprise Networks, Digital Business Assets, and Endpoint Security with Tested and Proven Methods (English Edition)*. BPB Publications.

[68] Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*, 102820.

[69] Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*(2), 2053951720976680.

[70] Nicho, M., Khan, S., & Rahman, M. S. M. K. (2017, September). Managing information security risk using integrated governance risk and compliance. In *2017 International Conference on Computer and Applications (ICCA)* (pp. 56-66). IEEE.

[71] Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Next-generation network security: Conceptualizing a unified, AI-powered security architecture for cloud-native and on-premise environments. *International Journal of Science and Technology Research Archive, 3*(2), 270-280. https://doi.org/10.53771/ijstra.2022.3.2.0143

[72] Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Revolutionizing data center security: Conceptualizing a unified security framework for hybrid and multi-cloud data centers. *Open Access Research Journal of Science and Technology*. https://doi.org/10.53022/oarjst.2022.5.2.0065

[73] Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Reimagining multi-cloud interoperability: A conceptual framework for seamless integration and security across cloud platforms. *Open Access Research Journal of Science and Technology*. https://doi.org/10.53022/oarjst.2022.4.1.0026

[74] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). The future of SD-WAN: A conceptual evolution from traditional WAN to autonomous, self-healing network systems. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2021.3.2.0086

[75] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premises integrations. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2021.3.1.0076

[76] Onoja, J. P., & Ajala, O. A. (2022). Innovative telecommunications strategies for bridging digital inequities: A framework for empowering underserved communities. GSC Advanced Research and Reviews, 13(01), 210–217. https://doi.org/10.30574/gscarr.2022.13.1.0286

[77] Onoja, J. P., Ajala, O. A., & Ige, A. B. (2022). Harnessing artificial intelligence for transformative community development: A comprehensive framework for enhancing engagement and impact. GSC Advanced Research and Reviews, 11(03), 158–166. https://doi.org/10.30574/gscarr.2022.11.3.0154

[78] Onoja, J. P., Ajala, O. A., & Ige, A. B. (2022). Harnessing artificial intelligence for transformative community development: A comprehensive framework for enhancing engagement and impact. *GSC Advanced Research and Reviews*. https://doi.org/10.30574/gscarr.2022.11.3.0154

[79] Papazafeiropoulou, A., & Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, *18*, 1251-1263.

[80] Park, S. K. (2015). Special economic zones and the perpetual pluralism of global trade and labor migration. *Geo. J. Int'l L.*, *47*, 1379.

[81] Parraguez-Kobek, L., Stockton, P., & Houle, G. (2022). Cybersecurity and Critical Infrastructure Resilience in North America. *Forging a Continental Future*, 217.

[82] Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), 100080.

[83] Pomerleau, P. L. (2019). Countering the Cyber Threats Against Financial Institutions in Canada: A Qualitative Study of a Private and Public Partnership Approach to Critical Infrastructure Protection. *Order*, (27540959).

[84] Recor, J., & Xu, H. (2016). GRC technology introduction. In *Commercial Banking Risk Management: Regulation in the Wake of the Financial Crisis* (pp. 305-331). New York: Palgrave Macmillan US.

[85] Robinson, R. (2020). *Exploring strategies to ensure United States critical infrastructure of the water sector maintains proper cybersecurity* (Doctoral dissertation, Colorado Technical University).

[86] Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67.

[87] Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017, November). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In *2017 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 253-259). IEEE.

[88] Sanaei, M. R., Movahedi Sobhani, F., & Rajabzadeh, A. (2016). Toward An E-business Governance Model Based on GRC Concept. *The International Journal of Humanities*, *23*(3), 71-85.

[89] Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Tex. Int'l LJ*, *50*, 305.

[90] Shackelford, S. J., Russell, S., & Haut, J. (2015). Bottoms up: A comparison of voluntary cybersecurity frameworks. *UC Davis Bus. LJ*, *16*, 217.

[91] Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129-136.

[92] Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & security*, *57*, 14-30.

[93] Sikdar, P. (2021). *Strong Security Governance Through Integration and Automation: A Practical Guide to Building an Integrated GRC Framework for Your Organization*. Auerbach Publications.

[94] Smart, C. (2017). Regulating the Data that Drive 21st-Century Economic Growth.

[95] Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *computer law & security review*, *35*(4), 380-397.

[96] Tehrani, P. M., Sabaruddin, J. S. B. H., & Ramanathan, D. A. (2018). Cross border data transfer: Complexity of adequate protection and its exceptions. *Computer law & security review*, *34*(3), 582-594.

[97] Tian, G. Y. (2016). Current issues of cross-border personal data protection in the context of cloud computing and trans-Pacific partnership agreement: join or withdraw. *Wis. Int'l LJ*, *34*, 367.

[98] Trew, S. J. (2021). *International Regulatory Cooperation and the Making of "Good" Regulators: A Case Study of the Canada–US Regulatory Cooperation Council* (Doctoral dissertation, Carleton University).

[99] Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. *Information*, *13*(3), 146.

[100] Ustundag, A., Cevikcan, E., Ervural, B. C., & Ervural, B. (2018). Overview of cyber security in the industry 4.0 era. *Industry 4.0: managing the digital transformation*, 267-284.

[101] Voss, W. G. (2019). Cross-border data flows, the GDPR, and data governance. *Wash. Int'l LJ*, *29*, 485.

[102] Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: providing a competitive advantage for US companies. American Business Law Journal, 56(2), 287-344.

[103] Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. International Journal of Digital Earth, 10(1), 13-53.

[104] Yeung, M. T., Kerr, W. A., Coomber, B., Lantz, M., & McConnell, A. (2017). Declining international cooperation on pesticide regulation: frittering away food security. Springer.

[105] Zaccari, L. (2016). Addressing a successful implementation of a governance, risk and compliance management system.