ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/352435737

A Framework for Enterprise Cybersecurity Risk Management

Chapter · June 2021

DOI: 10.1007/978-3-030-71381-2_8

CITATIONS
25

READS
2,731

2 authors:

Samir Jarjoui
University of Dallas
4 PUBLICATIONS **41** CITATIONS
SEE PROFILE

Renita Murimi
University of Dallas
44 PUBLICATIONS **367** CITATIONS
SEE PROFILE

All content following this page was uploaded by Renita Murimi on 07 June 2022.

The user has requested enhancement of the downloaded file.

A Framework for Enterprise Cybersecurity Risk Management

Samir Jarjoui, Renita Murimi
sjarjoui@udallas.edu, rmurimi@udallas.edu

Abstract

Many organizations continue to struggle with the implementation of cybersecurity risk assessment and management programs. Navigating the evolving cybersecurity landscape and trends in technology commercialization require an understanding of the relational organizational context within which cybersecurity risks are rooted. While several existing cybersecurity risk management frameworks discuss the importance of identifying a context for cyber risks, they do not provide much guidance on "how" that should be done. Leaning on systems theory, this chapter advances the notion that a business and IT alignment approach can be leveraged to inform and drive subsequent cybersecurity risk management and assessment efforts. We outline a holistic roadmap through the incorporation of multiple interconnected dimensions as the underpinning of cybersecurity risk identification and mitigation. We introduce a novel framework that identifies practical organizational drivers and priorities to improve cyber resiliency within the organizational perspective.

Key words: Business and IT alignment, risk assessment, risk management, organizational dimensions, cybersecurity framework.

I. Introduction

The proliferation of technology and interconnected devices such as Internet of Things (IoT) has introduced unprecedented threats. In 2018, there were 80,000 cyber-attacks per day or over 30 million attacks per year [51]. Prior research recognizes the importance of managing cybersecurity risks as a key topic of concern, and several scholars have presented cybersecurity models and frameworks [30]. However, evidence suggests that despite the wealth of artifacts and insights for this topic, firms continue to struggle with the implementation of programs to effectively mitigate risks [3]. Risk management (RM) efforts in cybersecurity have traditionally revolved around the adaptation of frameworks such as NIST, COBIT, COSO and ISO. While these frameworks provide broad guidelines regarding RM, efforts to standardize and implement RM in diverse organizations have proved to be challenging. The gap between the theoretical frameworks and their practical implementation has attracted numerous studies, with a multitude of approaches and schools of thought aimed at addressing these gaps. For example, some authors attempted to develop technology and process-specific artifacts, while others focused on the holistic integration of cybersecurity risks with Enterprise Risk Management [44, 45, 48].

Aligning business and IT activities has been shown to improve firms' ability to effectively assimilate their capabilities to respond to challenges [7]. Thus, it is logical to argue that business and IT alignment (BITA), which involves applying IT in a harmonious way with business objectives [26], plays a critical role in the coordination and streamlining of organizational efforts to combat cyber risks. Recent literature on BITA enablers and inhibitors has mainly focused on strategic alignment aspects without the consideration of cybersecurity risks [22, 19, 25, 28]. Alternatively, cybersecurity RM scholars omitted the incorporation of BITA challenges and capabilities in the formulation of frameworks and models to address cybersecurity gaps resulting from misalignment [10, 1, 11, 6, 38, 13, 3]. The convergence of the business and IT domains remains to be fully explored, and as a result, many cybersecurity RM programs are implemented superficially based on routine RM processes [31], without integrating critical BITA dimensions that underlie the root cause of cyber risk exposure.

While several cybersecurity RM frameworks discuss the importance of identifying a rich context to understand the high-level environment, they do not provide much guidance on the "how" aspect of framework implementation [23, 24, 15, 44]. There is a need for a novel framework that identifies practical organizational drivers and priorities for subsequent planning and assessment efforts. Our chapter advances the notion that a BITA approach can be used to inform and drive cybersecurity RM efforts as part of the risk management process. The objective of this chapter is to introduce a model that integrates BITA dimensions and considerations in the formulation of cybersecurity RM processes. Fig. 1 shows a schematic of our novel framework which incorporates BITA capabilities as the underpinning of cybersecurity RM activities.

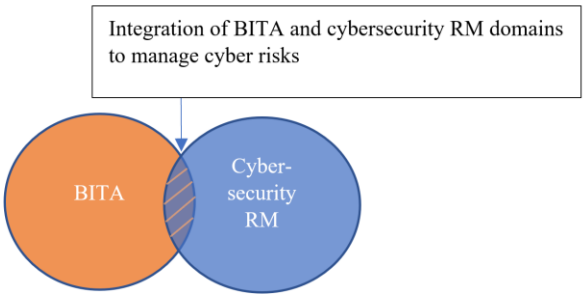

Fig. 1. Assimilation of BITA Capabilities with Cybersecurity RM Domains

Our work in this chapter leverages a systems theory approach to cybersecurity RM by focusing on the interactions and the relationships between organizational entities [29]. There is evidence that organizations continue to struggle with superficial cybersecurity RM implementations [31], due to four limitations in existing frameworks: (i) lack of coherent taxonomy [35]; (ii) impractical context for managing cyber [30]; (iii) limited coordination and transparency for technology deployments across the organization [17, 41]; and (iv) siloed implementations of cybersecurity efforts [40, 3]. The objective of this chapter is to address these gaps and develop a framework that provides additional guidance and a practical context to effectively manage cybersecurity risks in a proactive manner. As outlined in Fig. 2, our model establishes a realistic BITA-enhanced context including formal and informal organizational aspects. Thus, our model drives effective cyber risk mitigation strategies which can subsequently inform the larger organizational RM view.

A. Contributions of our chapter

The work in this chapter contributes to literature in three important ways. First, it highlights the limitations of prominent cybersecurity RM artifacts, in terms of their narrow and reactive approach. These existing RM approaches do not synthesize BITA capabilities and fail to proactively manage cybersecurity challenges in a proper context. We will examine four mainstream frameworks- COBIT, COSO, NIST, and ISO- [23, 24, 15, 44] and discuss the shortcomings and implications stemming from the lack of contextual incorporation of BITA dimensions. While these frameworks provide a systematic process to identify assets, vulnerabilities, and threats, they do not provide an end-to-end holistic mechanism to tackle practical obstacles through a BITA lens. Second, this chapter is among the first to assimilate the fields of BITA and cybersecurity RM, which have been traditionally examined separately. Our goal is to demonstrate the importance of using a BITA perspective in the battle against cyber threats to proactively manage cybersecurity risks and identify the root-cause of exposures. Finally, we develop a framework which integrates six BITA capabilities to measure cybersecurity risks using COBIT as a guideline.

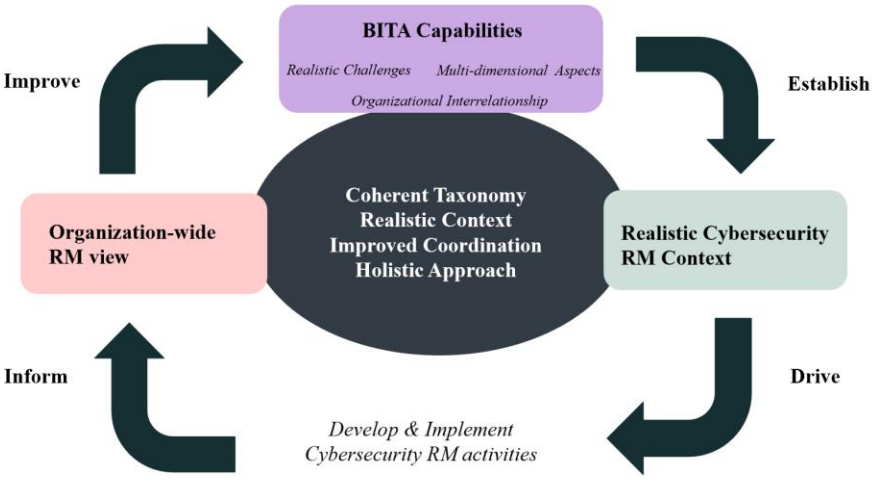

Fig. 2. Cybersecurity Holistic Alignment Roadmap Model (CHARM)

B. Motivation for Business IT Alignment (BITA)

Our chapter departs from previous work in two significant ways. First, we develop the argument that cybersecurity RM can be improved through a focus on BITA capabilities. Using a BITA lens allows us to better examine the relational context within which firms' cybersecurity risks are embedded. Second, we challenge traditional approaches to cybersecurity RM and related artifacts. Specifically, we introduce an alternative baseline to manage cyber risks through the parallel and complementary field of BITA, which can capture real-world challenges and improve the effectiveness of cybersecurity RM.

Our framework builds upon guidelines introduced in [33] for framework development, where the authors point out that a new framework is expected to address problems that are not previously addressed and may include constructs, models, methods, or instantiations. Based on this perspective, our research addresses existing gaps and proposes a new framework. Our novel framework represents a new approach that merges two traditionally separate but complementary fields – business and IT alignment - to address cyber risks and challenges. The framework that we propose in this chapter is titled Cybersecurity Holistic Alignment Roadmap Model (CHARM). Fig. 2 shows how the CHARM framework assimilates the BITA and cybersecurity RM fields to manage cyber risks.

We used the Design Science Research methodology [33] in the development of CHARM. DSR offers a structured approach to develop frameworks related to Information Systems (IS) and includes six steps which result in a framework:

1. **Problem identification and motivation**. There is no shortage of cybersecurity RM research and artifacts, yet organizations continue to struggle with effective cyber risk management. Recent highly publicized incidents offer a grim but realistic view of the dangers and costs of cyber-attacks and emphasize the need for a thorough understanding of the underlying factors [50]. Our proposed CHARM framework addresses the shortcomings of existing RM frameworks and offers proactive steps for organizations to minimize cyber threats.
2. **Objectives of a solution**. Our objective is to develop a novel artifact that dynamically allows us to use BITA capabilities to drive the cybersecurity RM process.
3. **Design & development**. This activity is focused on creating the artifact, which includes the model, framework, and process. We utilize six BITA capabilities based on [25, 27] to lay the foundation for critical alignment capabilities for the cybersecurity RM process. We also use COBIT as a guideline and integrate it with the BITA dimensions to design and develop the framework.
4. **Demonstration**. We propose the development of a software tool to score risks using CHARM that demonstrates the effectiveness of incorporating BITA to manage cybersecurity risks.
5. **Evaluation**. This step will evaluate and measure the effectiveness of CHARM and its related software instrument through tool usage testing and user feedback analysis.
6. **Communication**. This step is represented by the work in this chapter which communicates the problem, its significance, and the proposed framework. We discuss the research problem and its implications, the artifact (its utility and novelty), the design rigor, and the relevance to scholars and RM practitioners.

The remainder of this chapter is organized as follows. Section II describes the evolution of risk management in cybersecurity with relevant work categorized from information systems (IS), information technology (IT) and enterprise risk management (ERM) perspectives and offers motivation for the development of a new BITA-based framework. Section III compares existing frameworks (NIST, COSO, COBIT and ISO). Section IV lays the groundwork for the incorporation of BITA into a cybersecurity RM framework, and Section V presents our proposed framework (CHARM) for cybersecurity RM. Finally, Section VI concludes the chapter and provides directions for future work, as depicted in Fig. 3.

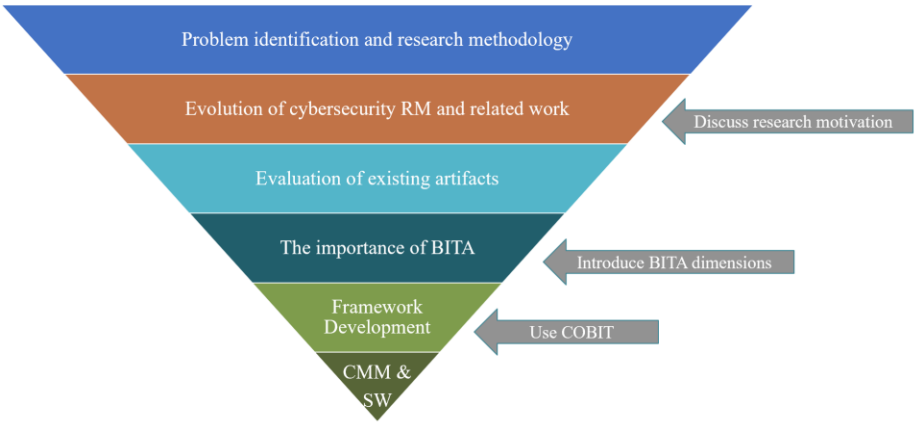

Fig. 3. Hierarchy of CHARM

II. The Evolution of Cybersecurity RM

Evolving cybersecurity RM approaches over the years have led to several discrepant approaches. A review of prior literature indicates inconsistent and siloed practices that are segregated in focus with various priorities that shifted over time [40, 3]. While the role of IT departments has largely shifted from merely being a support function to becoming a strategic business partner [46], cybersecurity RM continues to lag with an IT-centric legacy. As a result, for many years the primary responsibility for managing cybersecurity was viewed from an IT lens (i.e., IT security). Consequent implementation efforts were left to IT departments and cybersecurity professionals. However, in the past decade, new approaches started to emerge which elevated IT existing security efforts and included additional aspects of information security (IS) management. Since then, there have been significant considerations over the years including the integration with Enterprise Risk Management (ERM) [44, 3]. However, there are still unanswered questions and gaps as to why organizations continue to be unsuccessful in implementing effective cybersecurity RM frameworks. Based on our review of literature, we discuss two traditional approaches (IT-centric, IS-centric) to cybersecurity RM, an emerging ERM-centric approach, and highlight their limitations.

A. IT-Centric Approach

An IT-centric approach to cybersecurity RM places IT as the central entity that manages and mitigate risks stemming from online operations. In this approach, while IT is seen as a value-add function to the business through the implementation of technology capabilities [46], and cybersecurity efforts are solely framed from a technology-based lens [3]. As a result, assessing the cyber risk of exposure involves the identification of assets, threats, and vulnerabilities of IT capabilities in support of the organizational capabilities [36]. While an IT-centric focus involves a certain degree of alignment between business and IT strategies, it does not take into considerations the multi-dimensional aspects of cyber risks such as people, processes, and information. As a result, the dominant focus has been on IT governance related to physical IT artifacts (hardware, software, networks) [3], while largely omitting the integration of business in the cybersecurity RM efforts. Thus, this methodology remains grounded in technical aspects of cybersecurity RM and is limited in its ability to synthesize organizational context to develop effective mitigation strategies. In addition, the IT-centric view fails to address additional challenges related to the decentralization of technology, emerging digitization, and regulatory demands, all which introduce unmitigated threats to the organization [17]. We believe that using a BITA lens as proposed in our chapter directly addresses these gaps by providing a mechanism to examine the relational organizational context within which cybersecurity risks are rooted, to address risks at a deeper level.

B. IS-Centric Approach

The IS-centric approach to cybersecurity RM is rooted in the perspective of the confidentiality, integrity, and availability principles (the CIA triad). The CIA triad's focus is on information, and while this security practice

considers implications of people, facilities, processes, and strategy, it is limited due to its siloed perspective (i.e., information) [49, 3]. Information security scholars have consistently criticized this approach for managing cybersecurity risks and questioned its over-reliance on technical controls [39]. In addition, prior literature stresses the limited utility of this approach, which fails to effectively consider wider organizational and social aspects of cybersecurity due to a narrow technical orientation and focus [18, 4].

Recently, some authors signaled a departure from the traditional aspects of the CIA triad which focused on IS and moved toward a wider socio-technical reconsideration of its core concepts [39]. However, we believe that this approach to cybersecurity RM remains limited on "information" and does not address social and cultural dimensions, which are critical to effective risk management efforts in our technologically decentralized age. While it represents an improvement over the IT-centric approach, its core principles merely address manifestations of cyber risk and lack the mechanism to remediate the root-cause of challenges [18]. Our proposed framework transcends this limited view by holistically integrating formal and informal organizational aspects, including strategic, structural, social, cultural dimensions [14, 27], represented in our BITA approach to RM.

C. ERM-Centric Approach

Recent literature has attempted to address the traditionally siloed approaches to cybersecurity RM and recognized the need to elevate this process to achieve enterprise-wide risk oversight [44, 45]. While recent work has touted the importance and benefits of holistically integrating cybersecurity RM with ERM, there is a lack of guidance on "how" this goal can be achieved at the various organizational levels to ensure consistency. In addition, inconsistency of terminology, semantics, and existence of several disjointed frameworks contribute toward an unclear path for this perspective [35]. As a result, the scant research on this topic is incoherent and overlaps several concepts (i.e., RM, ERM, cybersecurity, IT, IS). Our proposed model bridges these gaps by introducing a framework that uses BITA to examine the organizational relational context in an applied manner and to address the multi-sided challenges for cybersecurity risks at all levels.

D. Motivation for a New Approach

Previous studies suggest that for cybersecurity efforts to be successful, it is important to aim for an approach that mitigates such risks from an enterprise-wide perspective [49]. This largely depends on the level of alignment between the business and IT to manage cybersecurity risk within the context of business objectives across the enterprise [47]. Building on this perspective, BITA can provide a systematic mechanism to harmonize cybersecurity RM activities within the organization and deal with the dynamic nature of cyber challenges due to regulatory demands and emerging digital needs. However, despite the recognition in prior literature of the important role that BITA can play in cybersecurity RM, there are hardly any frameworks or artifacts that combine these two distinct but complementary fields to address existing cyber challenges. Our motivation is to address the gaps in literature and develop a practical mechanism that approaches cybersecurity RM through formal and informal organizational aspects of BITA, to facilitate the RM process and address the root-cause of misalignment issues. Our proposed framework advocates the realignment of cybersecurity RM under BITA principles as a core competency to establish a foundation to improve resiliency in the organizational context.

Our systems-based model regards organizations as an interconnected set of elements that are coherently organized to achieve a purpose. Thus, a clear comprehension of the relationship between structure and behavior (i.e., system), can helps us understand the complex organizational dimensions and sub-systems that impact effectiveness cybersecurity RM efforts [29]. BITA can be an effective approach which embodies systems thinking to identify and harmonize formal and informal organizational facets and to effectively address cybersecurity challenges in an interconnected and holistic manner. As a result, our proposed approach allows for the proactive examination of patterns, instead of events, and incorporates strategic, structural, social, cultural dimensions as the underlying structures. The limitations of prior perspectives for cybersecurity RM and our proposed approach are illustrated using "iceberg" model, inspired by systems thinking [29] in Fig. 4. An IT-centric approach represents the "tip of the iceberg" and it is the least effective due to its largely narrow and reactive focus on isolated cybersecurity incidents. The IS-centric view is more effective but is still siloed on the "information" and does not effectively consider other organizational aspects, while the emerging ERM-centric school of thought is largely based on alignment of enterprise RM, without clear guidance on how that this goal can be effectively achieved.

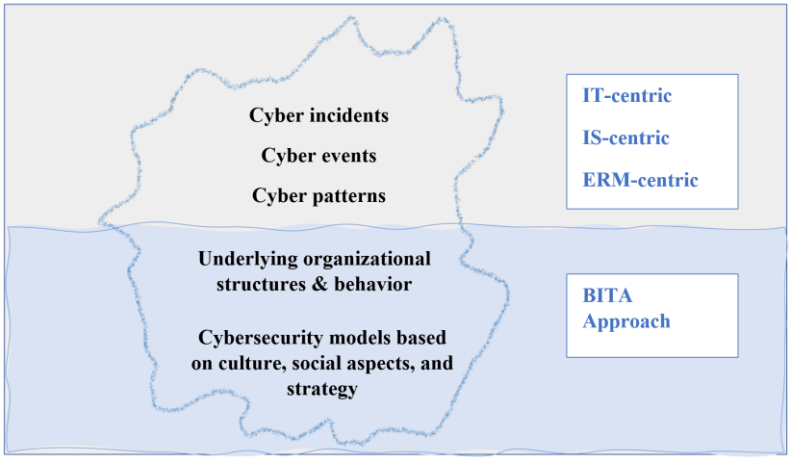

Fig. 4. Cybersecurity RM Iceberg Model

III. Evaluation of Existing Frameworks

Risk management in cybersecurity has benefited from a few prominent frameworks. These include the NIST, COSO, COBIT and ISO [23, 24, 15, 44]. While these frameworks provide a systematic process to identify assets and related vulnerabilities and threats, they do not provide an end-to-end holistic approach to cybersecurity RM. In addition, these tools have a narrow perspective and provide a paucity of guidance on "how" cybersecurity RM should be done to proactively address cyber challenges stemming from the lack of BITA [30, 5]. In this section, we provide an overview for each of these frameworks and discuss their limitations within the context of cybersecurity RM.

A. NIST Framework

The family of NIST frameworks address a variety of areas including information privacy, risk assessments, and cybersecurity to facilitate RM and compliance efforts within organizations. While there have been several publications over the years, very recently, NIST published *Integrating Cybersecurity and Enterprise Risk Management (ERM)* [44] as an attempt to holistically integrate cybersecurity RM with ERM. This document is intended to help organizations identify, assess, and manage their cybersecurity risks in the context of their broader mission and business objectives and a proposes a risk register to track and communicate risk information. While the authors discuss the importance of establishing an organizational context and emphasize a system level focus to consolidate risk data for systems to the organization, the framework does not provide guidance on "how" that can be done. We believe that this document is NIST's best attempt yet to integrate cybersecurity RM within the larger context, however, it fails to translate the conceptual constructs to practice. This limitation is illustrated in Fig. 5, which demonstrates the authors' goal to integrate cybersecurity RM at the various levels of the enterprise, with no direction on how to accomplish this goal.

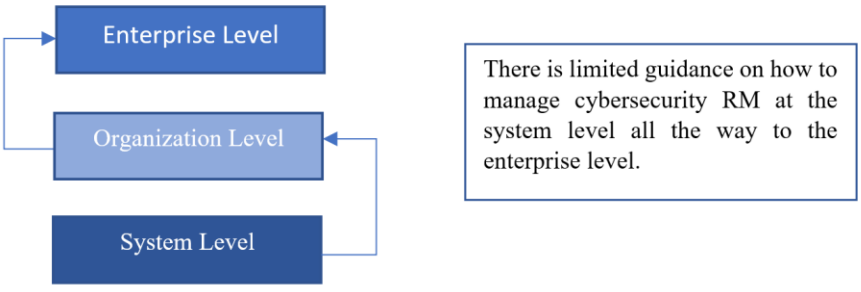

Fig. 5. NIST - Information Flow Between System, Organization, and Enterprise Levels

Other NIST publications, such as the *Framework for improving critical infrastructure cybersecurity* [8], are generally IS-centric and commence with the classification of information systems, without specifying how risks should be framed as part of the risk assessment process. While NIST's publications are useful, they lack practicality and guidance to manage cybersecurity risks through realistic contexts. Furthermore, none of the NIST publications adequately consider critical BITA dimensions as part of the RM process in a direct and purposeful manner. Therefore, these documents do not provide a mechanism to capture cybersecurity risks that arise from the lack BITA in organizations with decentralized technology structures.

B. COSO Framework

The Committee of Sponsoring Organizations (COSO) has published several frameworks over the years to assist organizations achieve their objectives based with the establishment of processes to support goals. COSO's recent update to the framework in 2017, *Enterprise Risk Management— Integrating with Strategy and Performance*, incorporates the element of organizational performance through the integration of strategy, mission, vision, and values. The Executive Summary of the 2017 ERM framework emphasizes the importance of providing additional depth and clarity for considering risk in the strategy-setting process and organizational performance. The updated framework also highlights the importance of using a holistic approach to risk management and acknowledges that many risks are interconnected [15]. COSO's framework is organized into five components: *Governance and Culture, Strategy and Objective-Setting, Performance, Review and Revision, Information, Communication, and Reporting*. Furthermore, these components are supported by several principles designed to support the framework's objectives. The framework recognizes the changing threat landscape and the dynamic nature of risks; however, it does not directly address cybersecurity threats or considerations.

While this framework has been popular for general RM practices, its utility for cybersecurity RM has been limited since it considers technology as an administrative function [5]. COSO's main objectives are geared toward RM in general and do not include cybersecurity RM taxonomies and mechanisms to address cyber risks. While there are limited studies that have utilized the COSO framework to address cyber risks [45, 6, 2], it is ERM-neutral with indirect applicability to cybersecurity RM. We regard the COSO framework as a secondary tool that can be used to manage cyber risks; it does not provide a primary mechanism to integrate technical cybersecurity aspects with other business considerations as part of the RM process.

C. COBIT Framework

COBIT is a framework developed by the ISACA organization for the governance and management of IT to help organizations create value from their IT investments [23]. Over the years, there has been several iterations of this artifact, with the most recent one published in 2019. COBIT (2019) is a framework for the governance and management of information and technology, intended to target the entire enterprise with a clear distinction between governance and management activities. It consists of forty Governance and Management objectives grouped into five domains. The Governance objectives are part of the *Evaluate, Direct and Monitor (EDM)* domain, which is intended to enable management to evaluate strategic options and monitors the achievement of the strategy. On the other hand, Management objectives are organized under the *Align, Plan and Organize (APO)*, *Build, Acquire and Implement (BAI)*, *Deliver, Service and Support (DSS)*, and *Monitor, Evaluate and Assess (MEA)*. Management objectives relate to a management process, typically performed by senior and middle management, while Governance objectives are the accountability of board of directors and executive management [23].

The 2019 COBIT framework refers to Alignment Goals (AGs) that emphasize the alignment of all IT efforts with business objectives through governance or management objectives, however, there are two primary limitations related to the AGs. First, the framework does not provide guidance on how to leverage the AGs to frame and drive cybersecurity RM efforts; instead, the document merely references the AGs with limited example metrics. Second, it is unclear how the AGs would be measured and assessed to identify and address multi-dimensional misalignment issues. The framework's use of AGs is at a high-level and does not offer practical guidance on how to leverage these goals at a deeper level.

While this updated version offers broader RM considerations and discusses the importance of incorporating stakeholder needs into an actionable strategy, it follows an IT-centric approach under a RM umbrella with limited enterprise-wide considerations. COBIT discusses the importance of enterprise governance of IT as a method to enable

business and IT to execute their responsibilities in support of BITA to create value. Perhaps the main drawback for this approach is that it places the enterprise governance of IT as the main step to achieve BITA given the centrality of information and technology. We believe that this is not a sustainable methodology in environments with highly decentralized technology implementations. We argue that BITA is a more effective first step to establish a consistent foundation to manage cybersecurity RM efforts across the organization. In our proposed approach, we rely on BITA as the baseline for subsequent RM efforts. The COBIT framework allows for the use of focus areas, which utilize the Governance and Management objectives and their components to address organizational challenges. While COBIT has its limitations, we see value in using it as a mechanism to assess and identify cyber risks based on established dimensions of BITA as a focus area for our research.

D. ISO/IEC 31000 Framework

The ISO 31000 framework provides RM guidelines for organizations [24]. This framework can be used for various type of risks including business continuity, currency, credit, and operational. The artifact explains basic principles of risk management, and provides a general framework for risk management, including a Plan Do Check Act (PDCA) approach to plan, implement, monitor, and improve. However, since it is applicable to any type of organization and to several types of risk, it does not provide specific methodology for cybersecurity RM. The scope of this framework is very generic to fit diverse organizational RM needs, and the risk identification phase is based on asset identification, which omits critical organizational aspects (i.e., BITA dimensions) for the management of cyber risks. We believe that this framework is useful to assess cyber risks after they have been identified. However, it lacks guidance on how to establish a risk assessment context upfront to aid with the initial process. Our proposed framework provides a clear methodology to establish a solid context for cybersecurity RM based on BITA dimensions to address these gaps.

The siloed approaches and limitations in existing frameworks involve weaknesses in an organization's defense that impact the ability to mitigate risks and minimize duplication of efforts [40]. In summary, evidence points to cybersecurity RM failures due to the existence of multiple incoherent taxonomies and discrepant approaches, with scant guidance on how to establish realistic contexts to drive effective and sustainable cybersecurity RM initiatives. These observations and limitations are illustrated in Fig. 6.

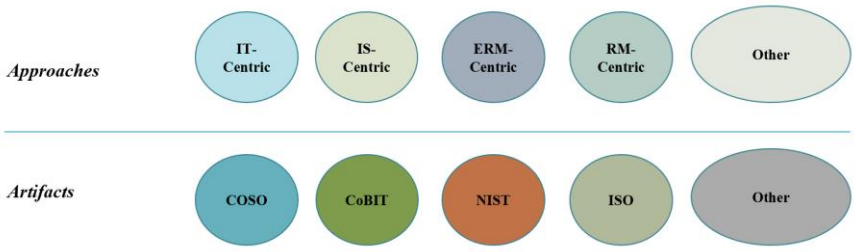

Fig. 6. Cybersecurity RM Approaches and Artifacts

IV. The Importance of BITA in Cybersecurity RM

BITA has been extensively researched over the years and the topic has consistently appeared in literature as a top concern for executives [22, 25, 19, 28]. The study of BITA has evolved over time, with early studies focusing on conceptual considerations to link IT with the business, such as [22] work, which featured the Strategic Alignment Model (SAM). Since then, many scholars discussed enablers and inhibitors that help and hinder alignment, to examine the convergence, fit, and harmonization between the business and IT [28, 25, 14, 12]. The are several definitions of BITA in literature [28, 7], with various alternative terms that refer to the phenomenon of alignment. For example, [22] study emphasizes the theme of *balance*, while other ideas, such as *coordination*, have also been expressed [28]. For this chapter, we define BITA as a process which involves applying IT in a harmonious way with business objectives [26], and consider it to be a bi-directional effort between the business and IT. Therefore, BITA capabilities address how IT is in harmony with the business, and how the business could be in harmony with IT [25]. There are several BITA dimensions which include strategic, structural, social, and cultural perspectives that represent interconnected organizational aspects for optimizing performance [27, 14]. The BITA field continues to evolve to account for the dynamic nature of technology deployment and scholars have called for additional research and contributions [14].

There is hardly any debate among scholars regarding the impact of BITA on firm's performance, and the literature suggests that organizations cannot be competitive if their business and IT strategies are not aligned [7, 26]. Fostering effective BITA capabilities is attributed to several benefits, including enhanced communication, credibility, trust, coordination, and top management support [12, 26]. However, despite the well-recognized benefits of BITA, prior research is mainly focused on the strategic aspects of alignment [27] and is incomplete for current technology developments and cybersecurity considerations [3].

On the other hand, cyberattacks are becoming more sophisticated, with tools and techniques that exploit weaknesses in people, processes, structure, and technology [35]. Successful cybersecurity RM undertakings are a product of deliberate efforts that consider multidimensional organizational perspectives, to effectively fend off threats [49, 32, 47]. BITA is a cornerstone for effective RM efforts [32] and provides an interconnected foundation to integrate cyber-defenses throughout the organization. However, while prior research recognizes that BITA is imperative to meet the dynamic nature of business and cybersecurity landscapes [16, 20], existing cybersecurity artifacts do not integrate the critical aspects of BITA to drive and inform subsequent efforts. Our review of literature confirmed that many cybersecurity RM implementations continue to fail due to limitations in existing artifacts and that BITA capabilities can be leveraged to address these gaps, thus, we advocate the realignment of Cybersecurity RM under BITA principles as a core competency.

Table 1 shows how BITA can be leveraged as an effective mechanism to address the existing cybersecurity RM challenges related to lack of coherent taxonomy, impractical context for managing cyber risks, limited coordination and transparency for technology deployments, and siloed implementations. BITA provides a systematic approach to develop and monitor multilayered capabilities to improve communications, skills, governance, and partnership between the business and IT [25] to deal with cyber threats. The synthesis of strategic, structural, social, and cultural dimensions can help identify and address the root-cause of cyber threat manifestations that stem from lack of BITA. While many cybersecurity efforts lack proper context [31], a BITA approach allows us to holistically examine the relational context within which firms' cybersecurity risks are embedded, which enhances our ability to address realistic challenges.

Cybersecurity RM Challenge	BITA Application
Lack of coherent taxonomy	Improved communications and skills to establish a clear baseline for cybersecurity expectations. Collaboration between business and IT on the development of RM artifacts to clarify semantics and ensure consistency in application.
Impractical context for managing cyber risks	The integration of strategic, structural, social, and cultural aspects provides a realistic mechanism to identify weaknesses due to misalignments and address underlying causes proactively. Cybersecurity investments are tailored based on specific organizational context.
Limited coordination and transparency for technology deployments	Improved visibility for decentralized technology deployments across the organization. Provides a mechanism to effectively identify organization-wide cyber risks and minimize override of security controls.
Siloed implementations	Strong partnership between business and IT improves stakeholders' understanding of organizational objectives and increases by-in for holistic cybersecurity RM implementations.

Table 1. Examples of BITA Application for Cybersecurity RM Challenges

Organizations can improve the RM process through the creation of "feedback loops" [29], which can be used to reinforce, or balance controls based on a BITA viewpoint. A BITA perspective improves the ability to prevent, detect, and correct control deficiencies within the changing cyber landscape, by encompassing critical cybersecurity capabilities, future security requirements, people, and information assets to meet business objectives [9, 49]. Prevention mechanisms can be fostered through the proactive development of BITA capabilities that bridge the gap between business and IT and ensure that cybersecurity strategies are in harmony with the business [21]. On the other hand, detection controls can be enhanced through the assessment of BITA maturity level within a cybersecurity RM context, which is a good indicator of potential cyber-gaps and misalignments [25, 19] that contribute to the root-cause of control deficiencies. Finally, corrective efforts can benefit from BITA which can serve as a vehicle to build a "human firewall" culture and improve adoption of the ever-evolving cybersecurity measures. Organizations can

determine the level of cybersecurity layers needed to protect their assets in a dynamic cyberspace environment, with the proper context, through a BITA lens as illustrated in Fig. 7.

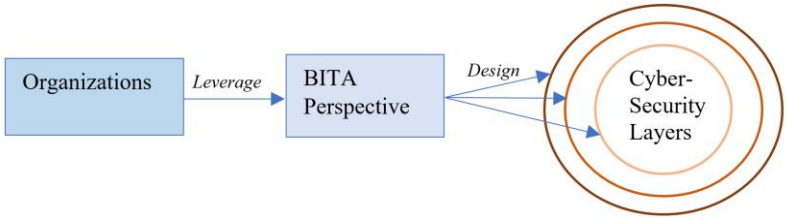

Fig. 7. Cybersecurity Layers Illustration based on a BITA Approach

A. BITA Capabilities

Alignment is a bi-directional process, between business and IT, which evolves over time to adapt to the dynamic landscape and business requirements. For our framework development, we will be adapting existing well-defined capabilities from [25. 27] studies, which include *Communication, Value Measurement, Governance, Partnership, IT scope & Architecture, and Skills Development*. Below is a summary of these BITA capabilities and their significance to cybersecurity RM.

Communication (C) – represents the effective exchange of ideas and a clear understanding of objectives to ensure the successful implementation of organizational strategies. This capability is essential in dynamic environments, where knowledge sharing, and coherent taxonomies are paramount for effective cybersecurity RM implementation and collaboration.

Value Measurement (VM) – this area includes the metrics, service levels agreements (SLAs) and formal assessments that foster continuous improvement based on established success criteria. This capability is critical for the detection of factors that lead to missing the criteria and the subsequent actions to mitigate deficiencies. An understanding of technology metrics along with established SLAs provides a relevant context for cybersecurity investments and activities.

Governance (G) – involves the considerations for ensuring that the appropriate business and IT stakeholders formally collaborate and review the priorities and allocation of IT investments, along with clearly defined decision-making authorities. This capability includes activities such as business strategic planning, IT strategic planning, and steering Committee(s), and provides a foundation to establish organization-wide controls to enforce compliance and capture decentralized technology implementation risks.

Partnership (P) – indicates the relationship that exists between the business and IT organizations which can help build trust and support through the collaboration of business sponsors and champions of IT endeavors. This capability can help develop a sense of "shared purpose" which increases stakeholders' buy-in and minimize siloed approaches to facilitate the holistic implementation of cybersecurity RM.

IT scope & Architecture (ITSA) – this capability encompasses the technology deployments and architecture to support business objectives. It includes IT investments that enable organizational back office and front office capabilities while maintaining the flexibility to managing emerging technology in a transparent manner. Aligning technology implementations with the business within a cybersecurity RM context is important to ensure that only necessary solutions are utilized and to effectively identify digital assets and related cybersecurity layers.

Skills Development (SD) – human resource aspects for the organization which go beyond the traditional considerations to include cultural and social factors. This capability includes activities such as training, change readiness, and education. In an era where threat actors take advantage of social and cultural weaknesses (e.g., social engineering, phishing, etc.), cybersecurity awareness is a cornerstone for establishing a "human firewall" to bolster defenses. This aspect can significantly assist organizations with cybersecurity RM implementations to minimize the circumvention of technical measures.

These six BITA capabilities and related components will be used as the basis for cybersecurity RM efforts in our proposed framework, however, we will also incorporate the COBIT framework to augment the model with specific cybersecurity risks that pertain to each of these capabilities. This approach will allow us to identify a realistic organizational context using BITA and formulate cyber risk management activities accordingly. We will be utilizing the COBIT (2019) framework's governance and management objectives, to support the risk assessment process through a BITA lens and the identification of cybersecurity risks. COBIT (2019) framework can be expanded and customized using focus areas, which describe a certain governance topic, domain or issue that can be addressed by a collection of governance and management objectives and their associated components [23]. The utilization of COBIT in our proposed approach to cybersecurity RM represents as a focus area that addresses cyber risks through BITA considerations.

V. The CHARM Framework Development

The CHARM framework was developed based on our evaluation of existing research and artifacts and from the identified challenges and motivation. In the following sections we discuss the purpose, characteristics, scope and limitations, and high-level design and architecture of the framework. In addition, we examine a case study application of the CHARM framework, using a real-world example, to illustrate how CHARM can be used to address cybersecurity risks. Fig. 8 shows the components of the CHARM framework.

A. The CHARM Framework

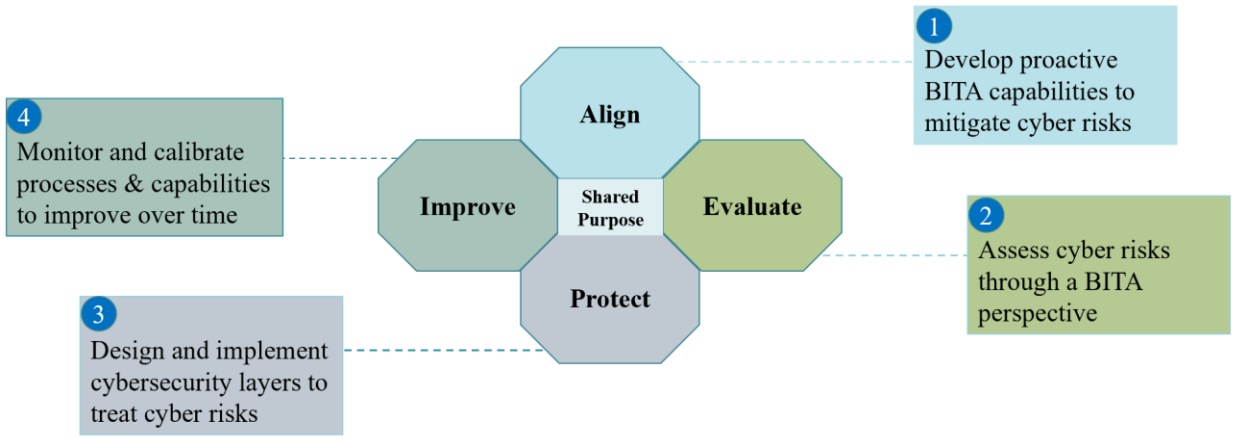

Fig. 8. CHARM Framework

Shared Purpose: Leadership and tone at the top are critical for effective cybersecurity governance efforts and cybersecurity RM depends on the alignment between IT and business objectives [49]. Shared purpose, which is a shared understanding of objectives, values, and vision [42], ensures that RM is integrated into organizational functions with the proper levels of leadership support and commitment. Shared purpose can assist organizations achieve the following:

- Establish a foundation for RM practices within the organization
- Recognize the organizational risk appetite and related control measures
- Facilitate the allocation of resources to manage cyber risks
- Harmonize the formal and informal organizational aspects in the RM process

Align: Aligning BITA capabilities provides a proactive mechanism to identify misalignment gaps through the examination of strategic, structural, social, and cultural dimensions [14]. Effective cybersecurity RM relies on an understanding of organizational structures and context, which varies across organizations and industries. This

framework component facilitates the understanding of BITA capabilities through the performance of a maturity assessment to identify gaps and establish a relevant context, to conduct subsequent RM activities.

Evaluate: Evaluating cybersecurity risks within the context of BITA capabilities, allows organizations to effectively conduct risk assessments and identify the root-cause of threats. This framework component enables the process of identifying cyber risks through the examination of relevant cyber threats based on the BITA misalignment gaps for the organization. A risk assessment process is conducted with input from the BITA maturity assessment to effectively scope the evaluation of cyber risks.

Protect: The organization should develop appropriate plans to formally determine risk treatment approaches and strategies. This framework component allows for the design and implementation of controls, based on COBIT, to effectively minimize cybersecurity risks. This includes the selection of Governance and Management objectives and related activities that pertain to organizational cybersecurity risks for people, processes, and technology.

Improve: Continuous improvement is essential to respond to the dynamic nature of cybersecurity risks. Organizations should leverage the collective knowledge obtain from the implementation of the framework to calibrate BITA capabilities and improve their RM process and collaboration. Providing a feedback loop to address BITA gaps reinforces and balances organizational capabilities to proactively remediate the root-cause of risk manifestation and build a cohesive process.

These components represent a continuous and interconnected process designed to identify and remediate multilayered weaknesses throughout the organization. The CHARM framework process steps are illustrated in Fig. 9.

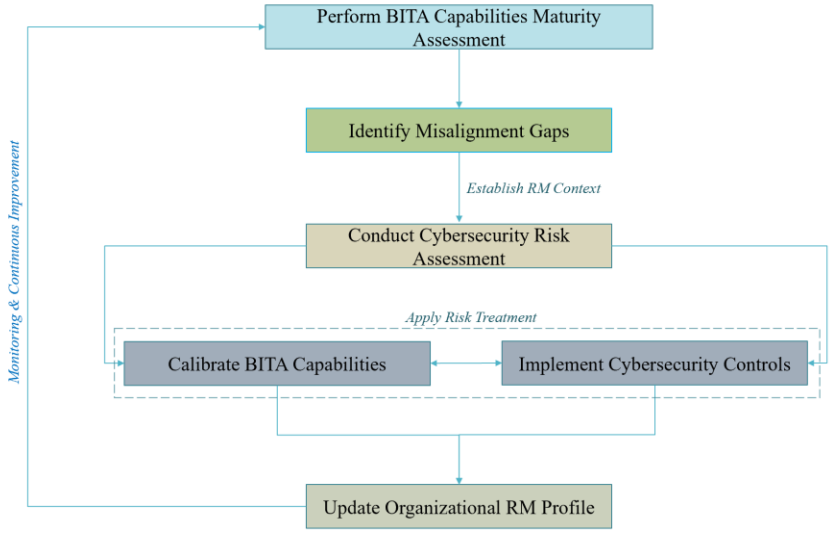

Fig. 9. CHARM Framework Process Steps

The CHARM framework is focused on the organizations' internal alignment capabilities as the baseline to identify and address cybersecurity threats. While the framework establishes a multi-faceted foundation for conducting the cybersecurity RM, threats emanating from sources that are outside the organization's control are out of scope. Threat actors situated in external environments which may impact the organization indirectly, or unknown "zero-day" vulnerabilities, are not covered by the CHARM framework. The Framework considers the root causes of cybersecurity threats which may result in cyber incidents through the assessment of BITA capabilities. The BITA maturity assessment provides organizations with a mechanism to evaluate these activities and a roadmap that identifies opportunities for enhancing the harmonious relationship of business and IT within a cybersecurity RM context.

B. A Case Study Application of the CHARM Framework

To illustrate the importance of both technical and non-technical capabilities, we discuss a real word cyberattack example to demonstrate the importance of incorporating BITA in the RM process. In 2013, during the holiday season, Target Corporation was impacted by a cybersecurity breach which compromised personal and financial data of 70 million customers. Before the breach, Target had a team of dedicated cybersecurity experts and had successfully complied with the Payment Card Industry Data Security Standard (PCI-DSS) audit, which involved a review of critical security controls and systems configurations [34]. In addition, the organization had implemented a robust malware detection software developed by the cybersecurity company FireEye [37]. The attackers were able to initially infiltrate Target's network using the compromised credentials of a third-party service provider (Fazio Mechanical Services). Additional vulnerabilities such as weak passwords, lack of business-driven firewall restrictions, and limited network segmentation [34, 43], allowed the hackers to escalate access privileges and circumvent the security measures in place. The negative reputational impact decreased Target's profits and caused top management turnover, and the company continued to incur costs for two years related this incident with over $290 million in total expenses [34]. A cybersecurity RM design based on BITA could have allowed Target to properly configure their defenses with a relevant business context, to proactively implement cybersecurity layers throughout the organization and minimize risks. Below we discuss how the CHARM framework could be applied in Target's breach, to leverage a BITA approach to better address the cybersecurity risks within the firm's multi-dimensional aspects.

Align: There are several BITA shortcomings that contributed to Target's failure to prevent and detect the cybersecurity attack. It is evident that many of the security controls were implemented without an understanding of the relevant business context, which is a critical part of this CHARM framework component. The attackers were able to establish and maintain a connection to Target's internal networks using the stolen credentials of Fazio Mechanical Services, which were used to access segments outside the scope of this service provider without being detected. In addition, Target's firewall, a device which manages network traffic, was not configured based on the business operating model to block outbound communications to non-business approved destinations. As a result, the hackers were able to extract and transfer the stolen data to servers in Russia [43]; an activity which should have been identified as suspicious. A BITA maturity assessment, outlined in this step, could have facilitated the understanding of BITA dimensions to proactively identify gaps, and implement cybersecurity layers based on organizational business needs and objectives. This approach could have allowed Target's cybersecurity personnel to configure the firewall and monitor network traffic to flag intrusions within a relevant business perspective.

Evaluate**:** Establishing a relevant organizational context is essential for conducting subsequent cybersecurity RM activities. While Target had successfully complied with the PCI-DSS standard and other audits, such RM efforts appear to have been largely superficial and did not consider the root-cause of cyber threats through a BITA lens. Prior to the attack, Target had received several industry and government alerts of increased cyber threats [43], however, the company was investing in technical tools without paying attention to other important facets such as structural and cultural considerations. In addition, Target's cybersecurity professionals received multiple alerts related to the breach and did not act [43]. Evaluating cybersecurity risks within the context of BITA capabilities, could have allowed Target to identify and mitigate the weaknesses related to cyber-response metrics, personnel competencies, and governance.

Protect**:** This CHARM framework component enables organizations to implement cybersecurity layers based on BITA capabilities as the baseline to identify and address cybersecurity threats. Target's breach investigation uncovered that that the company's internal network was not segmented based on business-driven access restrictions, and as a result, the hackers were able to access the point of sale (POS) terminals. This lack of network segmentation allowed attackers to traverse the internal network without being detected. In addition, while Target had implemented a password policy based on industry-standard practices, there were significant issues related to the enforcement of such policies. Weak passwords were widespread within the Target's systems, and the incident investigation team was able to extract around 500,000 passwords (86% of accounts). Furthermore, the investigation also flagged weaknesses in the maintenance and software patching process [34]. Applying the CHARM framework to implement cybersecurity layers within a proper context, based on the BITA maturity assessment and subsequent risk assessment process, could have allowed Target to properly segment its internal network using business logic and rules. Furthermore, an understanding of the social and cultural BITA gaps could have helped the Target detect the laxed security-culture and foster commitment, instead of compliance, to improve the adoption of password best practices.

***Improve*:** The CHARM framework calls for continuous improvement to respond to the dynamic nature of cybersecurity threats. It was apparent that many of Target's RM practices and controls were implemented using a static and siloed approach which was largely IT-centric. A BITA approach could have provided Target with a systems perspective to address cybersecurity challenges and continuously calibrate capabilities in holistic manner. Leveraging the strategic, structural, social, and cultural BITA dimensions could have allowed Target to establish an internal feedback process to manage cybersecurity risks effectively and proactively.

VI. Conclusions

Prior literature showed that cybersecurity risk assessment and management efforts continue to be fragmented and reactionary in nature. On the other hand, cyber-attacks continue to be on the rise, with no clear guidance on how to counter these threats systematically and consistently in our digital age. Many organizations find it challenging to identify, evaluate, and respond to cyber risks with the proper organizational context. Based on our evaluation, there several artifacts that are used to facilitate cybersecurity RM with discrepant approaches, however, there is a lack of uniformity and standardization in terms of how they approach the risk management process for cybersecurity risks. While these frameworks provide a systematic process to identify assets and related vulnerabilities and threats, they do not provide an end-to end holistic approach for the risk management process. In addition, there is a scant guidance on "how" cybersecurity RM should be done, and existing literature does not clearly address BITA risks in a proactive manner.

It is our belief that cybersecurity RM can be approached through a systems-based thinking, which regards organizations as an interconnected set of elements that are coherently organized to achieve a purpose. BITA can be an effective approach which embodies systems thinking to identify and harmonize formal and informal organizational facets and to effectively address cybersecurity challenges in an interconnected and holistic manner. As a result, our proposed model and framework allow for the proactive examination of patterns, instead of events, and incorporates strategic, structural, social, cultural dimensions as the underlying foundation.

This research addresses the gaps in literature and approach cybersecurity RM through formal and informal organizational aspects of BITA, to facilitate the RM process and address the root-cause of misalignment issues. Our ongoing research efforts include the development of a capability maturity model (CMM) based on key factors of governance, BITA, and cybersecurity RM to define average, more advanced, and leading-edge practices for the proposed model. In addition, future phases of this chapter will focus on the development of a software tool to score risks based on the proposed RM framework, to provide a practical mechanism to measure cybersecurity exposures using BITA dimensions. We anticipate important managerial implications for the CMM and software tool (SW), which will provide practitioners with a hands-on roadmap to assess and mitigate cyber risks.

VII. References

[1] Almgren K (2014) Implementing COSO ERM framework to mitigate cloud computing business challenges. International Journal of Business and Social Science 5

[2] Alslihat N, Matarneh AJ, Moneim UA, Alali H, Al-Rawashdeh N (2018) The impact of internal control system components of the COSO model in reducing the risk of cloud computing: The case of public shareholding companies. Ciência E Técnica Vitivinícola 33:188-202

[3] Althonayan A, Andronache A (2019) Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment. In: 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA); Oxford, United Kingdom, pp 1-9

[4] Anderson J (2002) Why we need a new definition of information security. Computer & Security 22:308-313

[5] Andronache A (2019) Aligning cybersecurity management with enterprise risk management in the financial industry. Doctoral Thesis, Brunel University, London, United Kingdom

[6] Apostolou B, Apostolou N, Schaupp LC (2018) Assessing and responding to cyber risk: The energy industry as example. Journal of Forensic & Investigative Accounting 10

[7] Avison D, Jones J, Powell P, Wilson D (2004) Using and validating the strategic alignment model. Journal of Strategic Information Systems 13:223-246

[8] Barrett MP (2018) Framework for improving critical infrastructure cybersecurity version 1.1: NIST Cybersecurity Framework. National Institute of Standards and Technology, Gaithersburg, MD, USA

[9] Bernroider EW (2008) IT governance for enterprise resource planning supported by the DeLone-McLean model of information systems success. Information & Management 45:257–269

[10] Boyson S (2014) Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation 34:342-353

[11] Camillo A (2016) Cybersecurity: Risks and management of risks for global banks and financial institutions. Journal of Risk Management in Financial Institutions 10:196-200
[12] Campbell B, Kay R, Avison D (2005) Strategic alignment: a practitioner's perspective. Journal of Enterprise Information Management 8:653-664
[13] Cebula JJ, Popeck ME, Young LR (2014) A taxonomy of operational cyber security risks version 2. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA
[14] Chan Y, Reich BH (2007) IT Alignment: what have we learned?. Journal of Information Technology 22:297-315
[15] COSO (2017) Enterprise Risk Management—Integrating with Strategy and Performance. Executive Summary. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf Accessed 23 Nov 2020
[16] Coutaz J, Crowley JL, Dobson S, Garlan D (2005) Content is key. Communications of the ACM 48:49-53
[17] D'Arcy P (2011) CIO strategies for consumerization: The future of enterprise mobile computing. Dell CIO Insight Series
[18] Dhillon G, Backhouse J (2000) Technical opinion: Information system security management in the new millennium. Communications of the ACM 43:125-128
[19] El-Talbany O, Elragal A (2014) Business-information systems strategies: A focus on misalignment. Procedia Technology 16:250-262
[20] Grover V, Segars AH (2005) An empirical evaluation of stages of strategic information systems planning: Patterns of process design and effectiveness. Information & Management 42:761-779
[21] Hardy G (2006) Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. Information Security Technical Report 11:55-61
[22] Henderson JC, Venkatraman H (1993) Strategic alignment: Leveraging information technology for transforming organizations. IBM Systems Journal 32:472-484
[23] ISACA (2018) COBIT 2019: Framework Governance and Management Objectives. Schaumburg, Illinois, USA
[24] ISO (2018) Risk Management – Guidelines. ISO 3100:2019, Geneva, Switzerland
[25] Luftman J (2000) Assessing business alignment maturity. Communications of AIS 4
[26] Luftman J, Brier T (1999) Achieving and sustaining business-IT alignment. California Management Review 41:109-122
[27] Luftman J, Lyytinen K, Zvi TB (2015) Enhancing the measurement of information technology (IT) business alignment and its influence on company performance. Journal of Information Technology 32:26–46
[28] Maes R, Rijsenbrij D, Truijens O, Goedvolk H (2000) Redefining business: IT alignment through a unified framework. PrimaVera Working Paper Series, University of Amsterdam, Amsterdam, The Netherlands
[29] Meadows DH (2008) Thinking in Systems: A Primer. In: Wright D (eds), Chelsea Green Publishing, White River Junction, Vermont, USA
[30] Meszaros J, Buchalcevova A (2017) Introducing OSSF: A framework for online service cybersecurity risk management. Computers & Security 65:300-313
[31] Moore T, Dynes S, Chang FR (2015) Identifying how firms manage cybersecurity investment. Southern Methodist University, Dallas, Texas, USA
[32] Oppliger R (2007) IT security: In search of the holy grail. Communications of the ACM 50:96-98
[33] Peffers K, Tuunanen T, Rothenberger M, Chatterjee S (2007) A design science research methodology for information systems research. Journal of Management Information Systems 24:45-77
[34] Plachkinova M, Maurer C (2018) Teaching case security breach at target. Journal of Information Systems Education 29:11–20
[35] Ramirez R, Choucri N (2016) Improving interdisciplinary communication with standardized cyber security terminology: A literature review. IEEE Access 4:2216–2243
[36] Reynolds P, Yetton P (2015) Aligning business and IT strategies in multi-business organisations. Journal of Information Technology 30:101–118
[37] Riley M, Elgin B, Lawrence D, Matlack C (2014) Missed alarms and 40 million stolen credit card numbers: How target blew it. Bloomberg News. https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data Accessed 17 Nov 2020
[38] Ruan K (2017) Introducing cybernomics: A unifying economic framework for measuring cyber risk. Computers & Security 65:77-89
[39] Samonas S, Coss D (2014) The cia strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security 10
[40] Servaes H, Tamayo A, Tufano P (2009) The theory and practice of corporate risk management. Journal of Applied Corporate Finance 21:60-78
[41] Silic M, Back A (2014) Shadow IT–a view from behind the curtain. Computers & Security 45:274-283
[42] Sims S, Hewitt G, Harris R (2015) Evidence of a shared purpose, critical reflection, innovation and leadership in interprofessional healthcare teams: a realist synthesis. Journal of Interprofessional Care 29:209-215
[43] Srinivasan S, Paine L, Goyal N (2019) Cyber breach at Target. Harvard Business School Case Studies. www.hbsp.harvard.edu
[44] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating cybersecurity and enterprise risk management (ERM). NISTIR 8286, National Institute of Standards and Technology, Gaithersburg, Maryland, USA
[45] Suroso JS, Harisno, Noerdianto J (2017) Implementation of COSO ERM as security control framework in cloud service provider. Journal of Advanced Management Science 5
[46] Tallon PP (2008) Inside the adaptive enterprise: An information technology capabilities perspective on business process agility. Information Technology and Management 9:21-36
[47] Wilkin CL, Chenhall RH (2010) A review of IT governance: A taxonomy to inform accounting information systems. Journal of Information Systems 24:107- 146
[48] Wolden M, Valverde R, Talla M (2015) The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. IFAC-PapersOnLine 48:1846-1852

[49] Yaokumah W, Brown S (2015) An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. Journal of Business Systems, Governance and Ethics, 9:50-65
[50] Zou Y, Mhaidli AH, McCall A, Schaub F (2018) I've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data Breach. In: USENIX Symposium on Usable Privacy and Security (SOUPS)
[51] Cyber Security Statistics (2020) The ultimate list of stats, data & trends. Purplesec.us. https://purplesec.us/resources/cyber-security-statistics Accessed 7 Dec 2020

View publication stats