Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management Alignment

Abraham Althonayan
Brunel Business School
Brunel University London
Uxbridge, UK
Abraham.Althonayan@brunel.ac.uk

Alina Andronache
Brunel Business School
Brunel University London
Uxbridge, UK
Alina.Andronache@brunel.ac.uk

***Abstract*— Rethinking organisations' risk resiliency against cyber risks has been found both successful and lacking because it is more challenging when organisations mirror past siloed approaches. In pursuit of effectiveness and resiliency, this paper examines the antecedents of Cybersecurity Management (CsM) to explore how siloed risk controls influence business effectiveness. At the same time, it explores the additional strengths in enhancing CsM through alignment with Enterprise Risk Management (ERM) to ensure that handling risk is proactively, strategically, and comprehensively managed. To explore the problem, this research commenced by considering both secondary and primary qualitative data to determine the current state of strategic foresight of organisations. The authors found evidence of a granular legacy, stranded in different security domains and siloed strategic approaches.**

Keywords—IT Security, Information Security, Cybersecurity Management, Enterprise Risk Management, strategic alignment

I. INTRODUCTION

Recent years have raised concerns regarding how business models change once deploying commercial online activities and/or online operations. Regardless of business opportunities gained, the cyberspace environment also triggers exposure to a threatening landscape. This is known as a so-called 'paradox of progress' brought by digitisation progress. As more organisations are facing increasing cybersecurity attacks, organisations need to address the critical issues of resiliency fragility [1, 2].

In this paper, we address the question of why organisations are still unsuccessful in applying effective risk controls at all levels when deploying online activities or operations. While organisations benefit from countless business opportunities, the cyberspace environment also triggers exposure to an increasingly dangerous landscape. Correspondingly, cyberspace risk exposure prompts the need for integrated strategies to deal more efficiently with risks and likely impact. Despite vast research in securing organisations against cyber threats, the highly publicised security breaches and cases of organisational failures have reaffirmed that challenges of cybersecurity exposure continue to be a severe problem, one that deserves serious consideration [3]. Given the systematic rise in risk velocity over recent years and risk types as well as an advancement of cybercriminals' capabilities, safeguarding organisations from cyber risks reveal many gaps. A closer look at literature on cybersecurity show a growing body of research that has been centered around separate approaches to information technology (IT) and information security (IS). This has brought into focus the reactive approach towards cyber vulnerabilities (hardware/software access), breaches, and business disruptions, (recognised as IT/IS-centric controls). Prior literature omits to emphasise proactive safeguards to ensure the achievement of an organisation's mission, strategy, and objectives, namely, risk resiliency and effectiveness. Besides, research on IT/IS-centric controls has failed to oversee the management of risks strategically. So, the authors of this paper argue that strategising management of cyber risks effect an organisation' capability to downsize the likely affect of the threat landscape.

In pursuit of effectiveness and resiliency, this paper examines the antecedents of Cybersecurity Management (CsM) with a specific focus on strategic alignment paradigm conceptual evolution, aiming to indicate why siloed risk controls influence business effectiveness. At the same time, it explores the benefits of implementing a CsM and Enterprise Risk Management (ERM) alignment. The reasons for outlining strategic alignment conceptual evolution are that it provides an overview of the root cause and why past literature has neglected to incorporate the integrative dimension of ERM and does not entirely move towards an approach of holistically mitigating risks. Undeniably, the way organisations deal with technology, and cyber-related risks have changed over time, as well as cyber vulnerabilities, threat velocity type, and dimensions [4], 5]. Having a robust mechanism to deal efficiently with a variety of risks has always been something that organisations strive to achieve [6, 7]. Consequently, changes in risk exposure have forced organisations to turn their attention from technological, to managerial tactics, to strategic approaches, and to better ensuring the achievement of the organisation's mission, strategy, and objectives [8].

II. RESEARCH BACKGROUND

Upon decomposition of what cybersecurity means, uncovering its legacy and dependencies across various fields related to the Information Technology (IT) and Information Security (IS), this paper extends its analysis exploring the antecedents and rationale of aligning CSM with ERM; aiming to provide an understanding of how organisations can manage their exposure to risks more strategically (employing all efforts in one single scope). Henceforth, a lack of unified risk oversight can have ripple effects due to unclear paths of

how controls apply to asset valuation, risk prioritisation, risk reporting, analysis, mitigation, and resiliency [6, 9].

Consequently, this paper portrays a discrepant legacy; leading to and proving confusions and siloed practices. This has led to the need for governance to control and align business strategy [10, 11]. Although, implementation of risk governance (risk oversight and controls) has proven a challenging task for boards over recent years [12, 13], some organisations still manage risk in silos within departments of their organisation. ERM's purpose is to guide organisations in dealing with risks and responding to uncertainties [14]. Whilst siloed approaches involve weaknesses in an organisation's defence (i.e. each department has its own way of dealing with risks), it may also cause severe issues in holistically understanding an organisation's exposure to risks or duplication of efforts [15]. Thus, the authors of this paper advocate realignment of risk control under ERM oversight principles as a core competency to establish enterprise-wide risk governance to increase resiliency in the current context. This paper emphasises the value of strategic alignment as a core competency when correlating CsM with ERM. An enterprise-wide alignment of CsM with ERM can yield harmonised risk reporting, analysis, mitigation, and resiliency. It has been found that their alignment (interconnectivity and partnership) can place the entire organisation in a more enhanced state of security through a unified perspective of control, accountability and decision making [16, 17]. The authors of this paper argue that CSM is a multi-faceted strategic mechanism that proactively makes use of risk controls and risk oversight functions (technical, cultural, and operational components) ingrained at all levels in order to ensure both value protection and value enhancement across an organisation; it is driven by organisational strategy and is dependent on variables such as cyberspace, people, practices, processes, assets, technology, and information.

Since the concept of CsM fails to be defined by prior literature, its meanings fluctuate from covering the control of unauthorised access, which is grounded in information technology [18], to management function designed to protect an organisation [19]. Failure to identify a common meaning and definition leads to a discussion regarding the CsM potential; whether that be a strategic function, operational function, or technological control function.

Consequently, some studies consider cybersecurity a continuing prevention, detection and recovery function [20]. However, other paths of research [21, 22] define the same concept through the perspective of confidentiality, integrity and/or the availability principles (CIA triad). The latter definition is incomplete and only partially correct (foundation). Even though the previous description related to security refers to information, a few authors articulate that CsM is more than information assurance or data security [18, 23, 24]. The interest in risk resiliency of organisations has registered significant consideration over the years. Nonetheless there are still unanswered questions as to why organisations are unsuccessful in effectively implementing security at all levels. In today's global digital economy, cybersecurity risks are among the most important factors considered [25, 26, 27] due to their impact, velocity, sophistication, and dynamic [28, 2]. Thus, literature recognises the pivotal role of CsM for the organisation despite the fact that there are on-going open debates regarding what it is [24].

On the other hand, another stream of research has been carried out with regards to risk management (RM) and in particular its relationship with Information Technology (IT) risk function. A focused strategic approach can optimise the effectiveness of risk oversight and sustain an organisation's objectives achievement [9]. Additional evidence outlines that despite extensive research, risk alignment remains a top issue; a fact confirmed by other authors such as [29, 30, 31, 12, 32, 33, 34, 35].

Risk alignment has become challenging given organisations' shift to the cyber environment, emerging digital developments, regulatory demands, risk, threats, market volatility, and competition [36]. The relatively scarce literature focusing specifically on this matter reiterates unclear strategic directions when outlining the current state-of-art research problematic. In addition to risk governance immaturity, a lack of a holistic approach, a misguidance of terminology, semantics (e.g. information security, IT security), definitions, and a variety of frameworks all lead to confusion and contribute towards an unclear path for organisations to follow [37, 38, 28, 39]. Based, on the identified evidence mentioned above, the authors of this paper believe that risk governance has not reached a mature level hence failures exist. Alongside inconsistencies in practice, academics lack a coherent theory and lack agreed terminology that specifically addresses the alignment of CsM and ERM. Thus, the legacy is constructed on partial approaches to this research problematic. Without aligned strategies in dealing with all types of risks, it appears to be a foregone failure for organisations. Identifying how to handle risk holistically is imperative for the reason that it has broader implications. Specifically, organisations need to move from a subjective perspective (i.e. that of return-on-investment) to incorporate and assure value creation for others in the long-term (economically and sociologically).

While literature findings demonstrate that alignment benefits are significant in the long-term, achieving alignment would be a milestone for so many organisations that lack a clear strategical approach. The extant literature related to the alignment is conceptual (descriptive) [40], and evidence shows that more research is mandatory in order to accomplish the alignment of CsM with ERM and that selecting a solitary view of academics would perhaps not have tapped into the same outcome. A more systematic and theoretical analysis is required to understand organisational cyber strategic implications, and thus this paper urges acknowledgement of organisational antecedent; henceforward shifting towards a cyber risk foresight which reinforces proactive acknowledgement of future trends in addition to strategic planning and decisions [41, 42]. This is based on a deep understanding of evolving technology, security threats, opportunities, and agile strategic transformation on longer terms [42]. In contrast, an organisational cyber resilience would only react to attacks and recover losses. More importantly, cybersecurity proves to evolve from technical disciplines toward a holistic and strategic approach in managing risks.

III. RESEARCH METHODS

This paper is exploratory in nature and thus outlines findings in two streams of theoretical and empirical research.

So, this investigation has collected and analysed qualitative data as it seeks to explore the qualitative aspect of the problem. In this regard, this investigation commenced by evaluating past literature, employing a systematic literature evaluation. Therefore, the first stream relies on theoretical antecedents which thematically analysed, evaluated, and assessed prior literature in order to identify the current state of research (including limitations and gaps) so as to validate the position and contribution of this research [43, 44]). Accordingly, the literature was identified and categorised to support understanding and evaluation of existing literature's concentration and limitations [43]. With the intention of also incurring knowledge from applied knowledge, the interview method is addressed to senior executives from different financial organisations (26 semi-structured interviews) to determine the current state of strategic foresight. In this manner, the paper incorporates techniques of collecting data (research methods) and instruments (interviews) that help in the exploration of the phenomenon on the practical side. Accordingly, analysis of data relied on an interpretivist philosophy to provide a practical and theoretical perspective of the phenomenology through an inductive approach.

IV. Research Findings

For the above-mentioned reasons, research findings conclude the following:

*A. **Findings - Stream 1: Theoretical Antecedents***

From analysing prior research, it has been identified that risk oversight shifted through various phases, segregated in focus, and encompassing various priorities, thus resulting in different dimensions of alignment (strategic, structural, social, operational) [45]; progression of strategic risk oversight seems dependent on various components in ensuring strategic alignment. This opens the discussion that strategic alignment composites a multi-dimensional view that supports achievement of informed decisions, risk prioritisation, partnerships across organisations, and enterprise-wide valuation (tangible and intangible assets). In order to leverage a unified enterprise-wide risk mechanism to mitigate risks, the alignment is broken in a multitude of variables [46, 47, 32, 35]. Thus, successful alignment coordinates and adjusts activities, processes, people, structures, and contingencies to increase business value [48]. A major drawback is that silo security is a risk for organisations and thus alignment of CSM with ERM management, (e.g. strategies, planning, structure, processes, skills, competencies, culture alignment) must be acknowledged and addressed at all levels as a strategic risk control baseline. By achieving alignment, an organisation is less vulnerable to market changes or/and internal inefficiency because the alignment creates a common and centric/unified solution [49]. In deploying the exploration of strategic evolution for risk oversight, various factors, approaches, enablers, and inhibitors were identified. Though IT and business strategy represent the foundation and an opening point, a forward-looking, integrative approach that aligns more components is desirable. With a prevalence of cybersecurity and ERM, the following section synthesises progression in themes identified in the literature:

- THEME 1: IT-CENTRIC AND BUSINESS STRATEGY ALIGNMENT

A focus on IT-centric and business strategy alignment — implies an approach that focuses on processes and technology risk landscape to coordinate relating operational aspects [50]. While some other authors have referred to it through the lens of aligning strategies of both IT and business [35], the extent of alignment of this type of approach focuses on technology as technical assistance. When it comes to being IT-centric, it refers to how IT delivers value for an organisation's business strategy, respectively alignment performance [50]. It thus focuses more on the applicability, risk control, execution, and implementation of IT capabilities in the context of an organisation's capabilities [35]. While conceptually the alignment of IT with business strategy is planned, evidence shows that the alignment focuses on integration of organisations' processes and how physical and information artefacts (whether hardware, software, networks or information) fit together [50, 51]. This suggests that one of the main characteristics of this phase is that it remains rooted in the technical side of computerisation and its causal effects [47]. Despite its technical characteristics, the IT-centric approach brings together various benefits (e.g. competitive advantage, performance evaluation, value creation) through information technology governance [50, 51, 52]). An earlier approach of measuring IT-centric and business strategy alignment is conceptually considered by the work of [53] Henderson and Venkatraman [53], who indicate the role of aligning the strategy, organisation infrastructure, and processes in order to increase capabilities through the SAM model (Strategic Alignment Model). Many other researchers later applied this model's contribution and further developed to analyse the alignment implementation. For example, some authors [54, 32] analysed the alignment based on primary data, investigating whether the mutual consideration of Chief Executive Officer and Chief Information Officer could underpin an adequate alignment between IT and enterprise. Consequently, IT-driven alignment remains a challenging approach for many organisations to achieve; hence it requires dynamic capabilities to re-align [55]. While significant progress has been made, this type of alignment has remained the most considered strategy and baseline of research for more than 30 years [48], yet incomplete for current technology advancement and threat velocity.

- THEME 2: IS-CENTRIC AND BUSINESS STRATEGY ALIGNMENT

IS-centric and business strategy alignment — addresses and underpins operational and technical control perspectives in order to generate resilience and assess information security risk through a siloed perspective (information) even though it considers the security implication of people, facilities, technology, infrastructure, processes, and strategy [56]; [55]. Embedded in the operational side, this type of alignment combines both strategic and operation (i.e. processes alignment, infrastructure, and technology integration) using the strategic approach as a 'map' to maintain directions [56]. The approach predominantly depends on the CIA triad (confidentiality, integrity, and availability principles) and due to its partial focus, it represents a siloed approach.

- THEME 3: IT GOVERNANCE, RM AND STRATEGIC ALIGNMENT

IT governance, RM and strategic alignment — adopt a strategic approach to embed IT in business capabilities.

Although IT governance in this type of alignment focuses on operational, managerial, and strategic aspects [52], it focuses on " embedding IT within its work system" [52]. Henceforth, IT-related risks are translated into the RM philosophy, respectively IT Risk Management [52]. This approach advances towards a more mature risk oversight yet is still siloed.

- THEME 4: IS CENTRIC, RM AND BUSINESS STRATEGY ALIGNMENT

IS centric, RM and business strategy alignment — represents control of risk over three approaches: technical, operational, and strategic. A key limitation of this approach is that it mainly considers the security of information assets and omits to consider other components. It also discusses the alignment from the perspective of RM and neglects to address the problem of the siloed approach to risk oversight. Subsequent studies as [57] constructed a framework through STOPE perspective (strategy, technology, organisation, people, and environment) based on IS and RM principles. A key aspect of this framework is that although it does not make use of alignment terminology, it takes into consideration an integration of both theories (IS and RM) in order to establish a favourable and safe environment for business. Even so, [58] indicate that alignment continues to be a challenge. Similar to previous approaches, it depends on the CIA triad (confidentiality, integrity, and availability) because its primary attribute is defined based on 'information' protection and its core value for the organisation [59] However, regardless of semi-siloed characteristics of this approach, it complements security practices through the lens of RM in mapping risk across the entire organisation.

- THEME 5: IS CENTRIC AND ERM ALIGNMENT

IS centric and ERM alignment — focuses on aligning IS strategy to enterprise-wide risk oversight. Part of this perspective, Information Security, focuses on the security of data, information, or metadata (a large amount of data) and the information systems involved [30]. It also focuses on the basic premises evidenced by [47] who analyse the practicality of alignment and aspects that play significant roles (organisation's culture). Similar to the previous theme it addresses a semi-siloed perspective when compared with this paper's focus.

- THEME 6: CYBERSECURITY, RM AND BUSINESS STRATEGY ALIGNMENT

Cybersecurity, RM and business strategy alignment — merits lie in the fact that this alignment addresses a semi-siloed solution of RM domain but omits to discuss alignment enterprise-wide. It applies the principle of RM and aligns it with business strategy. Stemming from various disciplines, cybersecurity has progressively built its current position upon its early roots in computer science, information security, information assurance, and RM principles [60].

- THEME 7: CYBERSECURITY, ERM AND BUSINESS STRATEGY ALIGNMENT

Cybersecurity, ERM and business strategy alignment — provides holistic support for risk oversight. In short, it aligns all strategies towards one (organisational strategy) in order to employ all forces in one single scope to protect the organisation and to offer comprehensive capabilities to achieve its goal. Alignment of CSM with ERM yields an avoidance of risk siloed approaches and reduces organisational exposure owing to a single, unified mechanism that can deal with all risk portfolios. However, this theme is hardly ever discussed in literature.

Per total, the themes identified outline maturity progression with a prevalence of IT and RM alignment that remains embedded in some organisations legacy. Examining IT security management and strategic alignment conceptual evolution, this paper provides an overview of how risk oversight antecedents can influence a business planning decision. Results from earlier studies demonstrate a consistent and robust association between the risk oversight paradigm shift over the years and how some of the silo approaches remain applicable even though they partially respond to a modern organisation's needs. Prior contribution to the strategic alignment discipline has registered various levels, whether a combination of tactical, operational, or strategic approaches. The strategic alignment has become a more challenging task when compounding more dimensions [35] components (IT, IS, CSM, RM, ERM), and factors (enabler or inhibitors) that are vital to ensure strategic effectiveness. Where initially IT was seen as front-line value creation, the consequent phase outlined a focus on information, RM, and governance. Recognising the alignment implications in all dimensions, it sets to prioritise and translate business needs in terms of ensuring the achievement of objectives prompting an opportunistic risk approach rather than risk-averse strategy. Another aspect that leads to variation in alignment dimension is the fact that cybersecurity is rooted in IT. Barriers in achieving alignment vary from a lack of shared language, willingness to share knowledge [12], culture, training requirements and an ever-evolving risk landscape [30].

On the other hand, the advantages yielded by the traditional approach are noticeable but nonetheless limited to risk controls technical-related issues. The review of literature regarding CsM has exposed that the discipline of cybersecurity is stranded in previous terminology and dimensions. In the context of risk oversight alignment, additional evidence outlines that despite extensive research, alignment remains a top issue; a fact confirmed by other authors such as [29, 30, 31, 12, 32, 33, 35, 61]. Besides, [33] suggests that many organisations fail to align their strategies due to their size (large national organisations versus multinational organisations), yet a broader strategy might yield success. While most authors have focused on strategic alignment and discuss internal strategic alignment, other studies [62, 63] propose an alignment that also considers the external environment. As such, the environment and the strategy could 'co-align' and lead to a consensus on strategies that could prevent possible failures of alignment.

In the early stages, past literature investigating alignment [49] proposed focusing on IT/IS alignment without explicitly paying attention to information security. This demonstrates that literature related to alignment is scarce when researching the CSM alignment to ERM and is more oriented to IT. It is not surprising that some authors believe alignment represents a complete picture of maturity exposure since it unifies all the organisation's risks and in particular management activities in order to build common goals for the business

and IT [64]. Granting that many scholars have investigated the topic, it seems that research remain insufficient.

Based on literature examination of prior research on alignment, it has been found that literature significantly focused on IT alignment with business strategies rather than other alignment domains, which were left on the side as suboptimal research. Seeing that alignment entails various types (i.e. IT security with business strategy, IS with RM, IS with ERM), the research problem is justified as the literature for CsM alignment with ERM is scarce, if not non-existent. The evidence compiled in thematic synthesis points towards the scarceness of literature on the alignment of CsM with ERM and focuses instead on siloed IT and IS security. Therefore, the findings of thematic analysis determine that despite various efforts to increase resiliency, the approaches prove to be partially addressed in literature. This reconfirms that organisational risk oversight is under-researched and the alignment of CsM with ERM is a justified joint effort that contributes to the holistic control of risks. Above and beyond rethinking organisations' strategic resiliency has been found to have hits and misses for the reason that it is more challenging when organisations mirror past siloed approaches of IT security, Information Security, or siloed RM.

Although a lot of guidance and regulations have been released, the silo approach seems to continue [65]. On these grounds, it can be concluded that organisations manage risks in a variety of ways, depending on their understanding of managing a silo or holistic approach regarding probable losses (e.g. intellectual property, business interruption, reputation, customer trust, loss of sensitive information, financial loss, etc.).

*B. **Findings - Stream 2: Empirical results***

Empirical results — the analysis of empirical data revealed that the alignment of CsM with business strategy can enhance superior risk handling, risk reporting, analysis, mitigation, and resiliency across all of an organisation. Nevertheless, integrating strategic foresight appears to be challenging for organisations; henceforth it is segregated in various strands of technical and operational legacy. Thus, the evidence found sheds light on current organisational cyber resiliency maturity. Correspondingly, implications of these findings reassure the value of aligning organisational risk resiliency capabilities (instead of siloed and reactive controls). Furthermore, alignment of CsM with ERM and business strategy deploys interconnectivity and partnership that can place an entire organisation in a more enhanced state of security through a unified perspective of control, oversight, accountability, and decision making. As noted, by empirical findings, the holistic approach of CsM is settled internally by:

Category One: CsM determinants

a) Internal pressure

• Organisations' own initiative to proactively initiate adoption. Evidence shows that initiative taken by the organisation's board is a determinant in proportion of 14.29%.

• Internal culture was indicated as being the second determinant for CsM adoption (10.20%) because of various security human-related failures. Likewise, literature emphasises cultivating risk culture as being a way of influencing behaviour and attitudes among individuals within an organisation [66]. So, cybersecurity culture aims to change the mindset towards awareness of risks among employees as well as adherence to internal policies [67]. In addition to the generic research findings, the literature highlights different dimensions of culture that overlap, either behaviour, perception, assumptions, knowledge, commitment, accountability, awareness, attitude, communication, norms, responsibilities, habits, and/or values [68, 67, 66]. Nonetheless, all of those mentioned above are believed to be influenced by artefacts (procedures) and exposed values (guidelines) [23]. For instance, communication is perceived as being the component that ensures transparency [69]. Previous studies have based their criteria on selecting a few elements and have articulated either a top-down approach or mid-level approach (operational) while some other studies focused more on awareness and stresses a bottom-up approach. Specifically, for this research, culture determinants refer to overall, strategically driven cybersecurity culture. To keep pace with cybersecurity challenges some authors contend a need for an institutionalised cybersecurity culture that standardises everything [23]. Determining the impact of risk culture on organisations is important for establishing good practices, either originating from policy or compliance requirements [69].

b) External pressure

• Cyber threats' velocity and complexity are one of the main reasons stipulated by respondents. The relative frequency for this determinant was 16.33%. Over the past two decades, major advances in cyber threats were reported by the industry as being a designated effect. Moreover, it is believed that cyber risk poses significant challenges for most organisations [70].

• Regulatory pressure is a second external determinant identified with a relative frequency of 14.29%. Similarly, literature found that regulation is a driver which influences investments for internal control as well as influencing risk oversight transparency and disclosure of practices [71].

• Standards were referred by research findings as being in percentage of 31%. The sampled organisations preferred either a customised approach to the employment of a mix of standards and frameworks and/or create their own frameworks. Most prevalent were ISO 27000 series, COBIT and NIST cybersecurity frameworks. As some respondents stated (e.g. Respondent [18]), standards are used as a point of reference and they are referred to as main guidance, despite being 'customised'. Little literature refers to mixed/custom approaches that sustained a tailored oversight for organisational needs and capabilities even though it is believed that a customised approach is easy to implement [72]. In short, standards represent a significant determinant in implementing CsM.

Category Two: CsM reimbursement

While the previous category referred to what determines CsM, this category refers to the benefits of implementation. Thus, reimbursement category is performance-centric and refers to key benefits of implementing CsM. Among

reimbursements, evidence articulates five main benefits, as set below.

• Compliance was pointed by 24% of respondents, though in this case it is reported as a benefit/reimbursement.

• Competitive advantage is indicated by 20% of respondents as being an effect of implementing CsM. Competitive advantage is found to be a cascade effect of all the other categories (e.g. performance, resilience, compliance). Competitive advantage was seen in terms of revenue and profits, the achievement of organisational targets.

• Resilience (20%) has an equal value to competitive advantage. Regarding resilience, it is well known that leadership plays an important role; hence both strategy and culture are interdependent as well as tactic oriented [70]. The empirical findings found that resilience is among the expected reimbursement of implementing CsM. Evidence suggests that resiliency is driven from the top, thus aligning strategy of cybersecurity with organisational strategy is a recommended approach that proactively acknowledges responsibilities, integration, risk appetite, resilience planning, and assessment of effectiveness. Within literature, it is recognised that apart from being led from the top, resiliency is also a shared responsibility within an organisation's lower levels [70].

• Organisational effectiveness was indicated by 14% of respondents. A significant trait of effectiveness is that it defines the effectiveness of the relationship between two or more variables. Evidence shows that measuring the reimbursement of CsM respective effectiveness has a positive effect as it endorses results, recommends security needs, and implies mapping results of security measures against the overall organisational strategy and objectives achievement [73].

Category Three: CsM inhibitors

This category emphasises main CsM inhibitors in order to understand what issues should be addressed in an organisation's environment.

a) People-centric

• Culture can be both a proponent and an impediment in reaching organisation resiliency and performance [69]. Culture is a CsM inhibitor that is people-centric. Considering that the culture of an organisation emphasises different dimensions that overlap, it is clear that it encompasses a multitude of components. For instance, research findings identified that only 7.46% emphasised culture as effecting CsM. However, awareness and skills (knowledge) are recognised to be part of cybersecurity culture. Thus, a lack of awareness was agreed by 17.91% of respondents as being an inhibitor. Additionally, 10.45% of respondents believe that a lack of personnel competencies (skills and knowledge) affect implementation. This is also highlighted in theory as being a potential threat vector [1].To understand the role of culture, this category encompasses both a lack of awareness and a lack of skills, and thus it represents subcategories, respectively dimensions of cybersecurity culture [68, 67, 66], and not disparate concepts as had previously been understood by respondents.

b) Strategic centric

• Cost, 11.94% of respondents agreed that the cost of implementation inhibits CsM. Again, literature emphasises that there is a tendency for organisations to underinvest due to the latency of results about the uncertainty of the likelihood of a cost being associated with a breach of security [71]. One possible explanation for mistrust is because cybersecurity investments generate cost avoidance instead of revenue [71].

• Silos, 10.45% of respondents mention silo approaches and silo strategies as impeding CsM. Similar findings were signalled by literature.

Additionally, 24% of respondents indicated that a lack of maturity triggers reputational loss, 17.33% emphasise that has regulatory consequences, and 16% indicated financial loss. Given the fragmented management practices related to cybersecurity, the issue of global cybersecurity losses is almost incalculable due to the fact that estimation/prediction often relies on surveys [74, 75]. Losses were estimated in 2014 to be approximately $400 billion and later on in 2018 to be $600 billion [76, 77]. Nonetheless, it seems that 'biased' surveys and unreported cyber malicious incidents (i.e. events that were maybe not realised in full yet had criminal intention) contribute to the inability to understand the implications of cyber threats at a global level [65]. In keeping with these theories, [78] emphasises that there are four patterns of governance failures: overreliance on intuition, weak security foundation, overreliance on traditional solutions, and known attacks patterns and frail governance.

Category Four: Alignment Maturity of CsM and ERM

Despite various efforts of securing organisations, the research findings show that managing risk holistically remains a challenge for most organisations. In particular, organisations struggle in aligning the function of control and risk oversight to tie together all risk functions. Variations among the three disciplines (CsM, ERM and Alignment) explain why practices remain fragmented. Consideration for CsM alignment with ERM was found by 69.23% of respondents who considered alignment an enabler and were thus interested in applying the alignment paradigm principle.

Results from the interviews show that alignment deliverables are understood as a means of translating priorities for each function (26.2%), defining a common strategy (16.67%), evaluating/assessing performance (25%), ensures recognition of due care for strategy contribution (10.71%), implying education at every level of implementation (10.71%) and ensuring executive level support (10.71%).

However, despite significant credence for alignment, in reality, a lack of resources and specialisation impede deployment of alignment (Respondent 10). CsM aligned with ERM is understood to play an essential role in holistically managing and controlling risks. Among the main inhibitors that were pinpointed by respondents were skilling deficiencies (13.04%), cultural deficiencies (11.59%), and lack of appropriate governance (10.14%).

V. DISCUSSION AND IMPLICATIONS

The empirical results revealed that overcoming cyber risks holistically is a current issue for organisations. Even though ensuring cybersecurity is dependent on multiple determinants (i.e. internal and external, pressure), the findings exposed that understanding the reimbursement it is valuable. Accordingly, in driving security practices, four main reimbursements were emphasised by respondents: compliance, competitive advantage, resiliency and organisational effectiveness. These results evidence that decisions in implementing controls are beyond security and protection purposes henceforth long-term viability and opportunistic sights for businesses are echoed.

At the same time, prior literature showed that previous research is fragmented and stimulated reactive cybersecurity in detriment of proactive practices. Whereas previous research focused on various streams, a re-frame/realignment for an effective and integrated assurance plan for both risk control and risk oversights seem feasible. Our result agreed that alignment has a positive impact on the achievement of the organisation's mission, strategy, and objective. In general, it would be more useful for organisations to carry out alignment, incorporating principles of ERM, deploying alignment with CsM, and business strategy, thus employing all efforts in one single scope.

On the opposite, a lack of unified risk oversight can have ripple effects due to unclear paths of how controls shall apply to asset valuation, risk prioritisation, risk reporting, analysis, mitigation, and resiliency. It may also trigger weaknesses in an organisation's defence (i.e. each department having its way of dealing with risks), causing severe issues in understanding an organisation's broad exposure to risks as well as potentially duplicating efforts. Thus, alignment of CsM with ERM would help in understanding points of interconnections, holistic view of risks (if systemic), break down the risk to gain more significant insights, deploy risk oversight and create foresight capabilities in controlling, managing and governing risks.

VI. CONCLUSION

The antecedent of strategic alignment showed a conceptual evolution which demonstrates the value for organisations when associating CsM with ERM. Based on the results of the thematic analysis, it has been determined that literature focus varied. Due to the limited literature that aligns risk governance holistically, the investigation has explored prior literature based on separate domains (e.g. IT, IS, RM, ERM, CsM and alignment). The evidence compiled in thematic synthesis points towards the scarceness of literature on the alignment of CsM with ERM. Therefore, the findings of thematic analysis determine that despite various efforts to increase resiliency, approaches prove to be partially addressed in literature. This reconfirms that organisational risk oversight is under-researched and the alignment of CsM with ERM is a justified joint effort that contributes to the holistic control of risks.

Moreover, exploration of empirical findings demonstrate that further work needs to be done in order to manage risk and effectively sustain organisations in the long-term. The challenges encountered by organisations and the way they respond to cyber threats serve as a starting point to justify the value of CsM alignment with ERM. Additionally, the scarceness of literature focusing specifically on the topic demonstrates confusion and unclear direction. Overall, the results of this exploratory paper support an understanding of risk oversight development whilst articulating gaps in theory and practice associated with misalignment. This research can be used to evidence that strategic alignment can enact integrated capabilities to renew and redeploy an aligned risk oversight of CsM with ERM. Furthermore, this research was restricted to 26 interviews. Thus, additional exploration of the phenomenon may be extended to a larger sample to identify additional insights.

REFERENCES

[1] Goode, J., Levy, Y., Hovav, A., and Smith, J. (2018) 'Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness', Online Journal of Applied Knowledge Management (OJAKM), 6(1), 67-80.

[2] Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019) 'Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior', International Journal of Information Management, 45, pp.13-24.

[3] de Bruijn, H. and Janssen, M. (2017) 'Building Cybersecurity Awareness: The need for evidence-based framing strategies', Government Information Quarterly, 34(1), pp. 1-7. doi: /10.1016/j.giq.2017.02.007.

[4] Fibikova, L. and Mueller, R. (2012) 'Threats, Risks and the Derived Information Security Strategy', In ISSE 2012 Securing Electronic Business Processes, pp. 11-20.

[5] Craig, J. (2018) 'Cybersecurity Research—Essential to a Successful Digital Future', Engineering, 4(1), pp. 9-10.

[6] Webb, J., Ahmad, A., Maynard, S. and Shanks, G. (2016) 'Foundations for an Intelligence-driven Information Security Risk-management System', Journal of Information Technology Theory and Application (JITTA), 17(3).

[7] Kauspadiene, L., Cenys, A, Goranin, N., Tjoa, S. and Ramanauskaite, S. (2017) 'High-level self-sustaining Information Security management framework', Baltic J. Modern Computing, 5(1), pp. 107-123.

[8] Soomro, Z. A., Shah, M. H. and Ahmed, J. (2016) 'Information security management needs more holistic approach: A literature review', International Journal of Information Management, 36(2), pp. 215–225. doi: 10.1016/j.ijinfomgt.2015.11.009.

[9] Ahmad, A., Maynard, S. and Park, S. (2012) Information security strategies: towards an organisational multi-strategy perspective', Journal of Intelligent Manufacturing, 25(2), pp. 357-370.

[10] Rebollo, O., Mellado, D. and Fernández-Medina, E. (2012), 'A systematic review of information security governance frameworks in the cloud computing environment', J. Ucs, Vol. 18 No. 6, pp. 798-815.

[11] Nicho, M. (2018) 'A process model for implementing information systems security governance', Information & Computer Security, Vol. 26 Issue: 1, pp.10-38, https://doi.org/10.1108/ICS-07-2016-0061.

[12] Preston, D. S. and Karahanna, E. (2009) 'Antecedents of IS strategic alignment: A Nomological network', Information Systems Research, 20(2), pp. 159–179. doi: 10.1287/isre.1070.0159.

[13] Wu, S., Straub, D. and Liang, T. (2015) 'How information technology governance mechanisms and strategic alignment influence, organisational performance: insights from a matched survey of business and IT managers', MIS Quarterly, 39(2), pp. 497-518.

[14] Farrell, M. and Gallagher, R. (2014) 'The valuation implications of enterprise risk management maturity', Journal of Risk and Insurance, 82(3), pp. 625–657. doi: 10.1111/jori.12035

[15] Servaes, H., Tamayo, A. and Tufano, P. (2009) 'The theory and practice of corporate risk Management', Journal of Applied Corporate Finance, 21(4), pp. 60–78. doi: 10.1111/j.1745-6622.2009.00250.x.

[16] Atoum, I., Otoom, A. and Abu Ali, A. (2014) 'A holistic cyber security implementation framework', Information Management and Computer Security, 22(3), pp. 251–264. doi: 10.1108/imcs-02-2013-0014.

[17] Atoum, I., Otoom, A. and Abu Ali, A. (2017) 'Holistic cyber security implementation framework: a case study of Jordan International Journal of Information', Business and Management, 9 (1), pp. 108-119.

[18] Bayuk, J. L., Healey, J., Schmidt, J., Weiss, J., Sachs, M. H., and Rohmeyer, P. (2012) Cyber security policy guidebook. United States: Wiley.

[19] Kaplan, J., Bailey, T. and Rezek, C. (2015) Beyond cybersecurity: protecting your digital business. United States: Wiley.

[20] Humphreys, E. (2008) 'Information security management standards: Compliance, governance and risk management', Information Security Technical Report, 13(4), pp. 247–255. doi: 10.1016/j.istr.2008.10.010.

[21] Gerber, M. and Von Solms, R. (2005) 'Management of risk in the information age', Computers and Security, 24(1), pp. 16–30. doi: 10.1016/j.cose.2004.11.002.

[22] Posthumus, S. and Von Solms, R. von (2004) 'A framework for the governance of information security', Computers and Security, 23(8), pp. 638–646. doi: 10.1016/j.cose.2004.10.006.

[23] Von Solms, R. and Van Niekerk, J. (2013) 'From information security to cyber security', Computers & Security, 38, pp. 97–102. doi: 10.1016/j.cose.2013.04.004.

[24] Althonayan, A. and Andronache, A. (2018) 'Shifting from Information Security towards a Cybersecurity Paradigm'. In: ICIME 2018. Manchester: Association for Computing Machinery.

[25] Calder, A. and Watkins, S. (2012) IT Governance: an international guide to data security and ISO27001/ ISO27002. London: Kogan Page Limited.

[26] Nazareth, D. L. and Choi, J. (2015) 'A system dynamics model for information security management', Information and Management, 52(1), pp. 123–134. doi: 10.1016/j.im.2014.10.009.

[27] Chartered Institute of Internal Auditors (2018) 'Risk in focus 2019: hot topics for internal auditors'. Available at: https://www.iia.org.uk/media/1689824/risk-in-focus-2019.pdf (Accessed: 10 November 2019).

[28] Tianfield, H. (2016) 'Cyber Security Situational Awareness', 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, 2016, pp. 782-787.doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.165

[29] Cragg, P., King, M. and Hussin, H. (2002) 'IT alignment and firm performance in small manufacturing firms', The Journal of Strategic Information Systems, 11(2), pp. 109–132. doi: 10.1016/s0963-8687(02)00007-0.

[30] Rahman, S. and Donahue, S. (2010) 'Convergence of corporate and information security', International Journal of Computer and Information Security, 7(1), pp. 63-68.

[31] Avison, D., Jones, J., Powell, P. and Wilson, D. (2004) 'Using and validating the strategic alignment model', The Journal of Strategic Information Systems, 13(3), pp. 223–246. doi: 10.1016/j.jsis.2004.08.002.

[32] Johnson, A. M. and Lederer, A. L. (2010) 'CEO/CIO mutual understanding, strategic alignment, and the contribution of IS to the organisation', Information & Management, 47(3), pp. 138–149. doi: 10.1016/j.im.2010.01.002.

[33] Chen, L. (2010) 'Business–IT alignment maturity of companies in China', Information & Management, 47(1), pp. 9–16. doi: 10.1016/j.im.2009.09.003.

[34] Althonayan, A., Keith, J. and Misiura, A. (2011) 'Aligning enterprise risk management with business strategy and information systems', In European, Mediterranean & Middle Eastern Conference on Information Systems 2011 (EMCIS2011).30-31 May 2011, Athens, Greece, pp. 109-129.

[35] Reynolds, P. and Yetton, P. (2015) 'Aligning business and IT strategies in multi-business organisations', Journal of Information Technology, 30(2), pp. 101–118. doi: 10.1057/jit.2015.1.

[36] Hampton, J. J. (2015) Fundamentals of Enterprise risk management: how top companies assess risk, manage exposure, and seize opportunity, 2nd edn. New York: American Management Association.

[37] Chang, H., C. (2016) 'The synergy of scientometric analysis and knowledge mapping with topic models: modelling the development trajectories of information security and cyber-security research', Journal of Information & Knowledge Management, 15 (4), pp. 1650044-1-1650044-33. doi: 10.1142/S0219649216500441.

[38] Ramirez, R. and Choucri, N. (2016) 'Improving interdisciplinary communication with standardised cyber security terminology: a literature review', IEEE Access, 4, pp. 2216-2243.

[39] Alexander, R.D. and Panguluri, S. (2017) in Clark, R. M and Hakim, S. (eds), Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level, Volume 3 in Protecting Critical Infrastructure, pp. 19-47.

[40] Luftman, J. and Kempaiah, R. (2007) 'An update on IT: business alignment: "a line" has been drawn', MIS Quarterly Executive, 6(3), pp. 165–177.

[41] Iden, J., Methlie, L. and Christensen, G. (2016) 'The nature of strategic foresight research: A systematic literature review', Technological Forecasting and Social Change, 116, pp.87-97.

[42] Raban, Y. and Hauptman, A. (2018) 'Foresight of cyber security threat drivers and affecting technologies'. Foresight. doi:10.1108/FS-02-2018-0020.

[43] Kitchenham, B. and Charters, S. (2007) 'Guidelines for performing systematic literature reviews in software engineering', Evidence-Based Software Engineering (EBSE) Technical Report Engineering. Available at: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf (Accessed: 17 September 2017).

[44] Boland, A., Cherry, G. and Dickson, R.(ed.) (2014) Doing a systematic review: a student's guide. London: Sage Publications Ltd.

[45] El-Talbany, O. and Elragal, A. (2014) 'Business-Information Systems Strategies: A Focus on Misalignment', CENTERIS 2014 - Conference on Enterprise Information Systems, Cairo.

[46] Luftman, J. (2000) 'Assessing business-IT alignment maturity', Communication of the Association for Information Systems, 4(14), pp. 1-50.

[47] Campbell, B., Kay, R. and Avison, D. (2005) 'Strategic alignment: a practitioner's perspective', Journal of Enterprise Information Management, 18(6), pp. 653–664. doi: 10.1108/17410390510628364.

[48] Luftman, J., Lyytinen, K. and Zvi, T. J (2017) 'Enhancing the measurement of information technology (IT) business alignment and its influence on company performance', Journal of Information, 32(26).

[49] Bergeron, F., Raymond, L. and Rivard, S. (2004) 'Ideal patterns of strategic alignment and business performance', Information and Management, 41(8), pp. 1003–1020. doi: 10.1016/j.im.2003.10.004.

[50] Tallon, P. (2008) 'Inside the adaptive enterprise: an information technology capabilities perspective on business process agility', Information Technology and Management, 9(1), pp. 21-36.

[51] Tallon, P. Ramirez, R. and Short, J. (2013) 'The Information Artifact in IT Governance: Toward a Theory of Information Governance', Journal of Management Information Systems, 30:3, 141-178.

[52] Islam, Md., S. and Stafford, T. (2017) 'Information Technology (IT) Integration and Cybersecurity/Security: The Security Savviness of Board of Directors', Twenty-third Americas Conference on Information Systems, Boston.

[53] Henderson, J. C. and Venkatraman, H. (1993) 'Strategic alignment: leveraging information technology for transforming organizations', IBM Systems Journal, 32(1), pp. 472–484. doi: 10.1147/sj.382.0472.

[54] Burn, J. M. and Szeto, C. (2000) 'A comparison of the views of business and IT management on success factors for strategic alignment', Information & Management, 37(4), pp. 197–216. doi: 10.1016/s0378-7206(99)00048-8.

[55] Yaokumah, W. and 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(2).

[56] Baets, W. R. J. (1996) 'Some empirical evidence on IS strategy alignment in banking', Information and Management, 30(4), pp. 155–177. doi: 10.1016/0378-7206(95)00056-9.

[57] Saleh, M. S. and Alfantookh, A. (2011) 'A new comprehensive framework for enterprise information security risk management', Applied Computing and Informatics, 9(2), pp. 107–118. doi: 10.1016/j.aci.2011.05.002.

[58] Fakhri, B., Fahimah, N. and Ibrahim, J. (2015) 'Information security aligned to enterprise management', Middle East Journal of Business, 10(1), pp. 62-66.

[59] Webb, J., Ahmad, A., Maynard, S. B. and Shanks, G. (2014) 'A situation awareness model for information security risk management', Computers & Security, 44, pp. 1–15. doi: 10.1016/j.cose.2014.04.005.

[60] Le, N. and Hoang, D. (2016) 'Can maturity models support cyber security?', 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC). doi: 10.1109/pccc.2016.7820663.

[61] Zhang, M., Chen, H. and Luo, A. (2018) 'A systematic review of business-IT Alignment research with enterprise architecture', IEEE Access, 6, pp. 18933-18944.

[62] Walter, J., Kellermanns, F. W., Floyd, S. W., Veiga, J. F. and Matherne, C. (2013) 'Strategic alignment: a missing link in the relationship between strategic consensus and organizational performance', Strategic Organization, 11(3), pp. 304–328. doi: 10.1177/1476127013481155.

[63] Siponen, M. and Willison, R. (2009) 'Information security management standards: Problems and solutions', Information and Management, 46(5), pp. 267–270. doi: 10.1016/j.im.2008.12.007.

[64] Huang, C. D. and Hu, Q. (2007) 'Achieving IT-business strategic alignment via enterprise-wide implementation of Balanced Scorecards', Information Systems Management, 24(2), pp. 173–184. doi: 10.1080/10580530701239314.

[65] Marsh (2015) 'UK 2015 Cyber risk survey report'. Available at: http://uk.marsh.com/Portals/18/Documents/UK%202015%20Cyber%20Risk%20Survey%20Report-06-2015.pdf (Accessed: 22 June 2015).

[66] Nasir, A., Arshah, R., Hamid, M. and Fahmy, S. (2019) 'An analysis on the dimensions of information security culture concept: A review', Journal of Information Security and Applications, 44, pp. 12-22.

[67] European Union Agency for Network and Information Security (ENISA) (2017) Cyber Security Culture in organisations. Available at: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport (Accessed: 12 September 2018).

[68] Korovessis, P., Furnell, S., Papadaki, M. and Haskell-Dowland, P. (2017) 'A toolkit approach to information security awareness and education', Journal of Cybersecurity Education, Research and Practice, 5(2), p. 1-32.

[69] Cambridge Centre for Risk Studies (2018) Risk management perspectives of global corporations.Available at: https://www.theirm.org/media/4043222/IRM-Cambridge-RM-PERSPECTIVES-OF-GLOBAL-CORPORATIONS_correct-covers_final.pdf (Accessed: 20 February 2019).

[70] World Economic Forum (2017) 'Advancing cyber resilience principles and tools for boards'. Available at: https://www.google.co.uk/search?q=Advancing+Cyber+Resilience+Principles+and+Tools+for+Boards&oq=Advancing+Cyber+Resilience+Principles+and+Tools+for+Boards&aqs=chrome..69i57.12321j0j7&sourceid=chrome&ie=UTF-8# (Accessed: 17 March 2018).

[71] Gordon, L., Loeb, M., Lucyshyn, W. and Zhou, L. (2018) 'Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms', Journal of Information Security, 9(2), p. 133-153.

[72] Talabis, M. and Martin, J. (2012) Information security risk assessment toolkit: Practical Assessments through Data Collection and Data Analysis. Waltham, Mass.: Syngress.

[73] Hagen, J. M., Albrechtsen, E. and Hovden, J. (2008) 'Implementation and effectiveness of organizational information security measures', Information Management & Computer Security, 16 (4), pp. 337-397. doi: 10.1108/09685220810908796.

[74] McAfee (2013) 'The economic impact of cybercrime and cyber espionage'. Available at: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf (Accessed: 14 November 2016).

[75] Websense Security Labs (2015) '2015 Industry drill-down report, financial services'. Available at: http://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf?mkt_tok=3RkMMJWWfF9wsRokv6vAde%2FhmjTEU5z14uopXKawhokz2EFye%2BLIHETpodcMRcNjPa%2BTFAwTG5toziV8R7DEJM1u0dMQWxHq (Accessed: 24 June 2015).

[76] McAfee (2014) 'Net losses: estimating the global cost of cybercrime, economic impact of cybercrime II'. Available at: http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf (Accessed: 28 April 2015).

[77] McAfea (2018) 'The economic impact of cybercrime—no slowing down'. Available at: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf (Accessed: 29 November 2018).

[78] Julisch, K. (2013) 'Understanding and overcoming cyber security anti-patterns', Computer Networks, 57(10), pp. 2206–2211. doi: 10.1016/j.comnet.2012.11.023.