© JUN 2019 | IRE Journals | Volume 2 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV2I12-1713779

Risk-Based Cybersecurity Assurance and Data Availability Limitations, Advances and Future Research Opportunities

OLADAPO FADAYOMI[1], TOYOSI O ABOLAJI[2], JOSEPH EDIVRI[3], JOLLY I. OGBOLE[4], PRECIOUS OSOBHALENEWIE OKORUWA[5], BISOLA AKEJU[6]

[1]ND Western Limited, Lagos, Nigeria
[2]Independent Researcher
[3]Microsoft Canada
[4]University of California, Berkeley, USA
[5]Independent Researcher
[6]Independent Researcher

Abstract:** Ensuring cybersecurity assurance in complex digital environments increasingly requires a risk-based approach, where resource allocation, control implementation, and monitoring are guided by the potential impact of threats and system vulnerabilities rather than prescriptive compliance checklists. Risk-based cybersecurity assurance prioritizes the protection of critical assets, balances security investments against operational requirements, and incorporates probabilistic assessments of threat likelihood and severity. A key dimension of this approach is data availability, which directly influences decision-making, operational continuity, and the reliability of automated risk assessments. Despite advances in cybersecurity frameworks and monitoring technologies, organizations continue to face limitations in data completeness, timeliness, and quality. Inadequate or fragmented data can impede accurate risk modeling, delay detection of emerging threats, and reduce the effectiveness of control strategies, particularly in distributed, cloud-enabled, and high-velocity digital ecosystems. Recent advances address some of these challenges through the integration of real-time telemetry, behavioral analytics, and AI-driven anomaly detection. These technologies enable continuous assessment of system state and user activity, improving the granularity and predictive power of risk models. Additionally, the adoption of probabilistic and scenario-based methodologies allows organizations to quantify uncertainty, model cascading effects, and anticipate potential disruptions even under incomplete information. However, gaps remain in standardizing data collection, ensuring data integrity across multi-source environments, and integrating data-driven insights into actionable governance and policy frameworks. Future research opportunities include the development of autonomous, adaptive cybersecurity assurance systems that leverage AI-native risk assessment, cross-domain data integration, and continuous feedback loops. There is also a need for empirical validation of risk-based models in diverse operational contexts, exploration of data availability trade-offs, and methods for resilient decision-making under uncertainty. Advancing these areas will enhance the effectiveness of risk-based cybersecurity assurance, improve organizational resilience, and support sustained operational continuity in increasingly complex and interconnected digital systems.

***Keywords:** Risk-Based Cybersecurity, Data Availability, Assurance, Threat Modeling, Probabilistic Risk Assessment, Anomaly Detection, Operational Resilience, AI-Driven Security*

I. INTRODUCTION

Cybersecurity has undergone a profound evolution over the past decades, transitioning from compliance-driven control frameworks to dynamic, risk-based assurance models (Onovo et al., 2015; Nwankwo, C.O. and Ihueze, 2018). Early approaches were largely prescriptive, emphasizing adherence to standards, policies, and regulatory mandates rather than the real-time management of emergent threats. Organizations relied on checklists, audits, and procedural compliance to demonstrate security readiness, often prioritizing documentation over actual resilience (Mehan, 2016; Boyd and Holton, 2018). While these methods ensured a baseline of accountability, they were limited in addressing sophisticated, adaptive cyber threats that exploit system complexity, insider vulnerabilities, and interconnected digital infrastructures. The increasing frequency and severity of cyber incidents have highlighted the inadequacy of compliance-centric paradigms, creating a shift toward risk-based cybersecurity assurance, which integrates probabilistic threat assessments, continuous monitoring, and scenario-based evaluation to provide actionable intelligence for decision-makers (Romanosky, 2016; Tsakalidiset al., 2018).

The reliance of contemporary digital ecosystems on high-quality, timely, and trustworthy data has intensified the stakes for cybersecurity assurance. Critical operations across cloud computing, enterprise platforms, and industrial control systems depend on the integrity, availability, and confidentiality of data flows (Chenet al., 2016; Aniet al., 2017). Disruptions to data availability or quality can compromise operational continuity, decision-making, and strategic initiatives, making data itself a critical asset requiring protection. Consequently, cybersecurity assurance is no longer solely about protecting networks or endpoints; it is inseparable from ensuring data reliability and operational trustworthiness, which underpins analytics, artificial intelligence, and automated decision systems across sectors (Borkyand Bradley, 2018; Bhattacharjee, 2018). This interdependence underscores the need for frameworks that simultaneously address system security, data fidelity, and risk exposure, recognizing that vulnerabilities in one domain can cascade into broader operational and strategic consequences.

The interrelationship between cybersecurity assurance, risk modeling, and data availability forms a central concern for organizations seeking resilient digital architectures. Risk-based assurance models leverage probabilistic assessments, threat modeling, and scenario analysis to quantify potential impacts of cyber events, while also factoring in data availability constraints (Ciapessoniet al., 2016; Hibshiand Breaux, 2018). For example, decisions regarding access controls, backup strategies, or anomaly detection mechanisms must consider the timeliness and completeness of the underlying data streams. Failure to integrate these dimensions can result in misaligned risk prioritization, ineffective mitigation strategies, and over- or under-allocation of resources (Fini, 2017; Bennettet al., 2017). This convergence of technical, analytical, and operational considerations highlights the importance of holistic, evidence-based assurance approaches that link cybersecurity, data governance, and risk management in a coherent framework.

The motivation for examining limitations, recent advances, and future research directions arises from the persistent challenges posed by rapidly evolving threats and technological innovation. Despite progress in machine-assisted threat detection, AI-driven analytics, and real-time monitoring, significant gaps remain in modeling complex threat behaviors, quantifying uncertainty, and ensuring that assurance measures are adaptive and scalable. Emerging technologies, such as cloud-native architectures, IoT networks, and distributed ledger systems, introduce novel data availability constraints and risk vectors, demanding continued investigation (Laszewskiet al., 2018; NETTOet al., 2018). Understanding these limitations and evaluating recent advances is crucial for guiding the development of next-generation assurance mechanisms and informing best practices in cybersecurity governance.

The research objectives of this study are to develop a structured understanding of risk-based cybersecurity assurance under data availability constraints, synthesize current technological and methodological advances, and identify actionable directions for future research. By articulating the interplay between system security, data quality, and risk assessment, this work contributes to the cybersecurity governance literature by providing a conceptual foundation for evidence-driven assurance (Carr, 2016; Katinaand Keating, 2018). This aims to inform practitioners, policymakers, and researchers on designing resilient architectures that integrate technical controls, data reliability measures, and analytical frameworks, ultimately enhancing organizational preparedness against evolving cyber threats and fostering sustainable trust in digital ecosystems.

II. METHODOLOGY

A systematic review following the PRISMA methodology was conducted to examine the literature on risk-based cybersecurity assurance and the associated challenges of data availability, recent advances, and emerging research opportunities. The objective was to provide a structured and transparent synthesis of empirical, conceptual, and methodological contributions while identifying gaps and directions for future investigation. Multiple academic databases, including Scopus, Web of Science, IEEE Xplore, ACM Digital Library, SpringerLink, and ScienceDirect, were searched to capture a comprehensive and interdisciplinary view spanning cybersecurity, information systems, risk management, and organizational studies. Search terms included combinations of keywords such as "cybersecurity assurance," "risk-based security," "data availability," "cyber risk modeling," "continuous monitoring," "regulatory compliance," and "threat intelligence." Boolean operators and truncation were applied to maximize coverage and ensure retrieval of relevant studies. The search was restricted to peer-reviewed journal articles, conference proceedings, and authoritative review papers published in English to maintain methodological rigor.

Eligibility criteria were defined to focus on studies that addressed risk-based approaches to cybersecurity assurance, the role of data availability in risk assessment and decision-making, advances in monitoring, modeling, or analytic techniques, and the integration of assurance processes with organizational risk management. Both qualitative and quantitative studies were considered if they contributed to conceptual frameworks, empirical validation, or methodological innovations in cybersecurity risk assessment. Excluded were studies that focused solely on external threat management without reference to internal risk assurance, purely opinion-based articles lacking analytical or methodological grounding, and works limited to technical descriptions of tools without connection to risk-informed assurance practices. Duplicate records were identified and removed prior to screening.

The screening process followed the PRISMA framework, beginning with title and abstract review to assess topical relevance. Records meeting preliminary criteria were subjected to full-text review to confirm alignment with inclusion and exclusion standards. Discrepancies in study selection were resolved through iterative assessment and consensus, ensuring consistent application of eligibility criteria and minimizing selection bias. The final corpus comprised studies addressing technical, organizational, and socio-technical aspects of risk-based cybersecurity assurance, with explicit attention to the challenges and strategies related to data availability.

Data extraction focused on capturing elements critical to understanding the interplay between cybersecurity assurance and data limitations. Key attributes included definitions and conceptualizations of risk-based assurance, data sources and quality metrics used in risk assessments, monitoring and analytic methodologies, organizational and regulatory integration, identified challenges and limitations, and proposed solutions or innovations. Particular attention was paid to how studies addressed dynamic, distributed, and cloud-based environments, as well as complex interdependencies that affect data integrity, timeliness, and completeness. Extracted information also included insights on continuous monitoring, feedback mechanisms, and the evolution of assurance frameworks in response to emerging threats and regulatory expectations.

The synthesis phase employed a qualitative thematic analysis approach. Extracted data were coded and grouped to identify recurring patterns, methodological innovations, limitations, and research gaps. Emphasis was placed on integrating insights from technical, organizational, and governance perspectives to inform a comprehensive understanding of risk-based cybersecurity assurance. Emerging themes included the constraints imposed by incomplete or fragmented data, advances in real-time monitoring and analytic frameworks, probabilistic and scenario-based risk modeling, and the role of automation and AI in enhancing assurance. Synthesis also highlighted cross-cutting considerations such as regulatory compliance, auditability, and the need for adaptive, continuous approaches in high-velocity digital environments.

Quality assessment of the included studies considered methodological transparency, robustness of analytic approaches, empirical validation, and relevance to complex and distributed digital systems. This assessment informed the weighting of findings during synthesis, ensuring that conclusions were grounded in evidence with clear applicability to practice. By following the PRISMA methodology, this review establishes a systematic and defensible foundation for understanding the limitations, advances, and future research directions in risk-based cybersecurity assurance. The approach highlights persistent data availability challenges, emerging technological and methodological solutions, and critical areas where future research can advance both theoretical understanding and practical resilience in organizational cybersecurity.

2.1 Conceptual Foundations of Risk-Based Cybersecurity Assurance

Cybersecurity assurance represents a fundamental objective of modern enterprise security governance, aiming to ensure that information systems, critical data, and digital operations remain protected, reliable, and resilient in the face of evolving threats (Noand Vasarhelyi, 2017; Nicho, 2018). Traditionally, cybersecurity assurance focused on compliance-driven or control-centric paradigms, emphasizing adherence to standards, policies, and predefined security controls. While effective in establishing baseline defenses, these approaches often fail to account for the dynamic, complex, and interconnected nature of contemporary digital ecosystems. In contrast, risk-based cybersecurity assurance shifts the focus from mere compliance to a holistic understanding of threats, vulnerabilities, and their potential impact on organizational objectives. Within this paradigm, assurance is defined as the degree of confidence that cybersecurity risks are effectively identified, assessed, mitigated, and monitored in alignment with enterprise goals, risk appetite, and operational priorities. This approach not only evaluates the adequacy of controls but also emphasizes the probabilistic likelihood and severity of potential incidents, enabling organizations to prioritize security investments and interventions based on their relative contribution to risk reduction.

A critical conceptual foundation of risk-based cybersecurity assurance lies in distinguishing it from control-based and maturity-based assurance approaches. Control-based assurance emphasizes verifying the presence, functionality, and effectiveness of specific technical or procedural safeguards. While this approach ensures compliance with standards such as ISO/IEC 27001 or NIST Cybersecurity Framework, it often provides a static snapshot and may overlook residual risks or evolving threat dynamics. Maturity-based assurance, on the other hand, evaluates organizational capabilities, processes, and governance practices against defined maturity models, offering insights into long-term security evolution but lacking quantitative measures of threat likelihood or potential impact. In contrast, risk-based assurance integrates probabilistic risk assessment, contextual analysis, and dynamic prioritization, providing actionable insights into where resources and attention should be focused to reduce exposure to the most significant threats (Thompsonet al., 2016; Leviet al., 2017). By situating assurance decisions within a risk-centric framework, organizations can move beyond reactive compliance toward strategically informed, proactive security management.

The concepts of risk appetite, risk tolerance, and prioritization are central to effective risk-based assurance. Risk appetite defines the level of risk an organization is willing to accept in pursuit of its objectives, reflecting strategic priorities and stakeholder expectations. Risk tolerance specifies acceptable deviations from established thresholds, guiding operational decision-making and contingency planning. By combining these constructs with systematic risk identification and assessment, organizations can prioritize cybersecurity initiatives according to the likelihood and impact of potential threats, aligning resource allocation with enterprise objectives (Tupaet al., 2017; Kureet al., 2018). This prioritization ensures that high-impact riskssuch as insider threats, critical system compromises, or regulatory violationsreceive greater attention and mitigation effort, while lower-priority risks are monitored efficiently without overextending organizational resources.

Risk-based cybersecurity assurance also necessitates integration with enterprise risk management (ERM) and digital resilience strategies. Modern organizations face complex interdependencies across business units, technology platforms, supply chains, and regulatory environments. Cybersecurity risk cannot be managed in isolation; it must be contextualized within broader organizational risk exposure, including operational, financial, reputational, and strategic dimensions. Integrating assurance activities with ERM frameworks enables a holistic view of risk interdependencies, facilitating coordinated decision-making, scenario planning, and crisis response. Furthermore, risk-based assurance directly supports digital resilience by identifying vulnerabilities that could disrupt critical operations and enabling proactive controls and contingency planning, thereby enhancing the organization's capacity to withstand, recover, and adapt in the face of cyber incidents (Nissenet al., 2018; Ugwu-Ojuet al., 2018).

Finally, risk-based cybersecurity assurance must account for diverse stakeholder perspectives. Regulators and auditors seek assurance that organizations meet legal, contractual, and industry obligations, emphasizing transparency and accountability (Heald, 2018; Nikolakiset al., 2018). Boards of directors focus on strategic alignment and enterprise risk exposure, evaluating whether cybersecurity investments appropriately reduce material risk. Chief Information Security Officers (CISOs) and security leaders are concerned with operational effectiveness, threat detection, and incident response capabilities. System owners and operational managers require assurance that critical business processes and technology services remain available and secure. Risk-based assurance provides a common framework that balances these perspectives, translating technical and procedural findings into strategic, probabilistic insights that support informed decision-making across all organizational levels.

The conceptual foundations of risk-based cybersecurity assurance are grounded in a shift from compliance-centric verification to risk-aware, context-sensitive, and strategically prioritized security management. By integrating probabilistic risk assessment, risk appetite and tolerance frameworks, enterprise-wide risk management, and stakeholder-centric perspectives, risk-based assurance enables organizations to achieve a higher degree of confidence in their cybersecurity posture. This paradigm not only strengthens operational resilience but also aligns cybersecurity objectives with enterprise strategy, resource optimization, and sustainable digital trust in complex, interconnected technological environments.

2.2 Data Availability and Quality Requirements for Risk-Based Assurance

Data availability and quality are foundational to the effectiveness of risk-based cybersecurity assurance. Accurate risk assessment relies on comprehensive, timely, and trustworthy data to quantify the likelihood and potential impact of threats, evaluate the effectiveness of controls, and prioritize mitigation strategies. Without reliable data, risk-based assurance frameworks cannot provide meaningful insights, leaving organizations exposed to unanticipated incidents and misaligned security investments. In modern enterprises, the increasing complexity of digital ecosystemsspanning cloud, hybrid, and distributed architecturesamplifies the importance of ensuring both the availability and integrity of critical cybersecurity data.

A comprehensive risk assessment requires several types of data, each serving a distinct purpose. Threat intelligence provides contextual information on emerging attack patterns, indicators of compromise, adversary tactics, and vulnerabilities actively exploited in the wild. Incorporating threat intelligence into risk models allows organizations to anticipate attacks and assess exposure to relevant threat actors. Vulnerability data, including patch status, known system weaknesses, and misconfigurations, informs the likelihood of exploitation and the prioritization of remediation efforts. Incident and loss data, drawn from historical security events, operational disruptions, and financial impacts, supports probabilistic modeling of potential consequences, enabling organizations to estimate both severity and frequency of insider or external attacks (Paté-Cornellet al., 2018; Sunet al., 2018).

Equally critical are asset inventories, dependency mappings, and configuration states, which provide a structural understanding of the enterprise digital environment. Accurate asset inventories catalog hardware, software, and digital services, ensuring that all critical systems are included in risk assessments. Dependency mappings reveal how applications, data repositories, and infrastructure components interact, enabling the identification of cascading risks where the compromise of one asset affects others. Configuration states capture the operational status of systems, including network settings, privilege assignments, and security controls, offering insights into exposure points that influence both the likelihood and impact of threats.

The characteristics of data directly influence the accuracy and reliability of risk-based assurance. Completeness ensures that all relevant assets, vulnerabilities, and threat vectors are represented, preventing blind spots in risk calculations. Timeliness is essential, as stale data may underestimate current exposure, particularly in fast-moving environments where patches, configurations, and threat landscapes evolve rapidly. Granularity determines the level of detail available for analysis; fine-grained data allows more precise modeling of risk at the asset or process level, while coarse data may obscure critical nuances. Consistency ensures that data collected from multiple sources adhere to standard definitions, formats, and taxonomies, enabling coherent integration (Ugwu-Ojuet al., 2018). Provenance, or the traceability of data sources, supports trust in data integrity, a crucial factor when integrating third-party or external intelligence feeds into enterprise risk models.

In dynamic, cloud-native environments, the continuous availability of data flows is particularly important. Automated provisioning, ephemeral workloads, containerized applications, and API-driven services create highly transient conditions, where asset states and security postures change rapidly. Continuous monitoring and real-time telemetry provide the necessary visibility for accurate, up-to-date risk assessments, enabling proactive mitigation and adaptive control measures (Fraga-Lamaset al., 2016; Jarviset al., 2018). Without continuous data flows, organizations risk basing decisions on incomplete or outdated information, undermining the efficacy of risk-based assurance.

Despite advances in monitoring and data collection technologies, data fragmentation remains a significant challenge. Large enterprises often maintain disparate data repositories across business units, cloud providers, and partner ecosystems, with varying access controls, data formats, and update cycles. Fragmentation can result in gaps, overlaps, or inconsistencies that reduce confidence in risk evaluations. Cross-organizational and supply chain environments exacerbate this problem, as external partners may provide incomplete or delayed data, limiting the ability to model enterprise-wide risks effectively. Addressing these challenges requires robust data governance, integration platforms, and standardization protocols to ensure that critical cybersecurity data is consolidated, validated, and accessible for real-time risk-based assurance processes.

Data availability and quality are critical enablers of effective risk-based cybersecurity assurance. The integration of threat intelligence, vulnerability and incident data, asset inventories, and configuration states provides a foundation for comprehensive risk assessment. Data must be complete, timely, granular, consistent, and traceable to support accurate modeling and informed decision-making. Continuous monitoring is essential in dynamic digital environments, while data fragmentation across organizational and ecosystem boundaries presents ongoing challenges that require structured governance and integration strategies (Palominoet al., 2017; Pappaset al., 2018). By prioritizing the availability and quality of cybersecurity data, organizations can ensure that risk-based assurance frameworks deliver actionable insights, enhance resilience, and optimize resource allocation in complex, high-velocity digital systems.

2.3 Limitations in Current Risk-Based Cybersecurity Assurance Practices

Risk-based cybersecurity assurance has emerged as a critical framework for organizations seeking to manage and mitigate cyber threats in increasingly complex digital environments. By linking security controls and monitoring processes to organizational risk priorities, risk-based assurance aims to allocate resources efficiently, enhance decision-making, and improve resilience. However, despite its theoretical and operational appeal, current practices exhibit significant limitations across data, measurement, organizational, and technological dimensions (McAdamet al., 2017; Lucianoet al., 2018). These limitations constrain the effectiveness, accuracy, and strategic value of risk-based assurance programs, particularly in high-velocity, distributed, and adaptive systems.

A fundamental limitation in current risk-based cybersecurity assurance practices is the scarcity and incompleteness of data required to generate accurate risk assessments. High-quality, longitudinal datasets documenting cyber incidents, system vulnerabilities, and realized losses are often limited, fragmented, or proprietary. Without such datasets, organizations struggle to develop statistically robust models of threat likelihood, exposure, and potential impact. Furthermore, underreporting of breaches exacerbates this scarcity. Organizations may withhold information on cyber incidents due to reputational concerns, potential legal liabilities, or regulatory obligations (Romanosky, 2016; Reetzet al., 2017). This underreporting not only reduces the volume of available data but introduces systematic bias, as high-impact or high-profile breaches are more likely to be publicly documented, while minor or internal incidents remain unreported.

Biases are also prevalent in vendor-provided and open-source threat intelligence feeds, which are frequently used to supplement internal data. Vendors may emphasize specific types of threats aligned with their commercial offerings, or datasets may be skewed toward particular sectors, geographies, or attack vectors. Open-source feeds, while valuable for situational awareness, are often inconsistent in quality, completeness, and timeliness. These limitations collectively constrain the ability of risk-based assurance frameworks to produce accurate, representative, and actionable risk scores, particularly when predictive analytics or modeling is required for strategic decision-making.

Measurement and modeling challenges represent a second major limitation in risk-based cybersecurity assurance. Quantifying cyber risk—defined as the likelihood and impact of a given threat—is inherently difficult due to the stochastic nature of attacks, the evolving threat landscape, and limited historical data. Many organizations continue to rely on qualitative or ordinal risk scoring methods, such as low/medium/high ratings, which are inherently subjective and lack statistical rigor. These approaches can obscure nuances in threat probability, interdependencies among assets, or cumulative exposure across systems. Even when quantitative approaches are employed, models are often constrained by uncertainty in parameter estimation, sensitivity to input assumptions, and opacity in underlying algorithms. Probabilistic risk models, Monte Carlo simulations, or Bayesian networks require careful calibration to reflect realistic scenarios, yet parameter values are frequently approximated due to insufficient empirical evidence. Model outputs may thus convey a false sense of precision, leading to overconfidence in risk assessments or misallocation of mitigation resources. Furthermore, the opaque nature of many modeling techniques complicates validation and stakeholder understanding, limiting executive confidence and the ability to integrate findings into strategic decision-making (Falconi and Palmer, 2017; Ekeret al., 2018).

Organizational and governance issues further limit the effectiveness of risk-based cybersecurity assurance. One prominent challenge is the misalignment between technical security metrics and executive-level risk narratives. While security operations teams often monitor detailed indicators such as intrusion attempts, vulnerability patching rates, or endpoint anomalies, executives require high-level risk summaries that align with business impact, regulatory exposure, and strategic priorities. Failure to bridge this gap can result in miscommunication, delayed decisions, or insufficient allocation of resources to high-risk areas.

Siloed data ownership and restricted data sharing exacerbate these challenges. Security, IT, and operational units frequently maintain independent datasets, often with inconsistent formats and limited interoperability. Restrictions on sharing sensitive data, whether due to internal policies or regulatory constraints, impede the creation of comprehensive risk assessments that integrate multiple system domains (Ugwu-Ojuet al., 2018). Limited assurance coverage also extends to third-party and supply-chain risks, which are increasingly critical in multi-vendor environments. Many organizations have partial visibility into vendor security practices, subcontracted systems, or cloud dependencies, leaving gaps in the risk-based assurance framework.

The final dimension of limitation arises from the nature of modern complex and adaptive systems.

Contemporary infrastructures incorporate dynamic and distributed architectures, DevSecOps pipelines, cloud-native deployments, and AI-enabled systems. While these designs enhance operational agility and scalability, they introduce challenges for risk-based assurance. Continuous change in configurations, code deployments, and network topologies complicates monitoring and modeling, as risk profiles can shift rapidly. Automated security controls, while efficient, often suffer from limited observability and explainability, making it difficult to validate whether controls are performing as intended or to interpret anomalies accurately.

Furthermore, the rapid evolution of emerging threats creates a temporal lag between threat identification and integration into assurance models. New attack techniques, AI-driven malware, and previously unknown vulnerabilities may remain unaccounted for, resulting in incomplete or outdated risk assessments (Mooreand Rid, 2016; Scholzet al., 2018). This lag undermines the real-time relevance of assurance outputs and limits the system's ability to proactively guide mitigation strategies.

In combination, these limitations highlight the gap between the conceptual promise of risk-based cybersecurity assurance and its operational execution. Addressing these gaps requires concerted effort across multiple fronts, including the development of richer, longitudinal datasets, the adoption of rigorous yet interpretable quantitative modeling techniques, improved alignment between technical metrics and strategic risk narratives, and the creation of adaptive assurance mechanisms suitable for complex and dynamic digital environments. Recognizing these constraints is critical for advancing both the practice and the research of risk-based cybersecurity assurance, ultimately enhancing organizational resilience against insider and external threats alike.

2.4 Recent Advances in Risk-Based Cybersecurity Assurance

The field of cybersecurity assurance has witnessed transformative advancements in recent years, driven by the increasing complexity of digital and cloud computing ecosystems, the proliferation of threat vectors, and the growing dependence on data integrity and availability. Modern approaches increasingly move beyond static, compliance-driven paradigms toward dynamic, risk-based assurance models that integrate real-time monitoring, quantitative risk assessment, and automation. These innovations enable organizations to anticipate, quantify, and mitigate cyber risks more effectively, ensuring resilience across both operational and strategic dimensions. Key developments can be categorized into four major areas: data and analytics innovations, quantitative and probabilistic risk modeling, automation and continuous assurance, and regulatory and standards evolution.

A foundational driver of risk-based cybersecurity assurance is the advancement of data collection and analytics capabilities. Cloud-native architectures have enabled improved telemetry through integrated logging mechanisms, endpoint detection, and extended detection and response (XDR) platforms. These tools aggregate large volumes of system and network data in near real-time, providing unprecedented visibility into both normal operations and anomalous activities. Complementing these capabilities are big data architectures and real-time risk dashboards, which allow organizations to process, visualize, and analyze complex datasets across distributed environments, supporting timely decision-making and proactive threat mitigation (Bendreand Thool, 2016; Nandigama, 2016). Moreover, data normalization, correlation, and enrichment techniques enhance the interpretability and contextual relevance of collected data. By consolidating heterogeneous data sources—ranging from security logs to cloud API activity—organizations can generate coherent risk signals, detect subtle attack patterns, and prioritize mitigation efforts based on actionable intelligence.

Parallel to advances in data collection, quantitative and probabilistic risk modeling has emerged as a critical component of modern cybersecurity assurance. Organizations increasingly leverage probabilistic risk assessment methods, including Bayesian networks and Monte Carlo simulations, to evaluate the likelihood and impact of potential cyber events under varying conditions. Such models enable the estimation of systemic vulnerabilities and the propagation of risk across interconnected systems, providing a more nuanced understanding than deterministic approaches.

Integration of loss modeling and cyber value-at-risk (CyVaR) concepts allows organizations to quantify potential financial and operational impacts, facilitating informed capital allocation and insurance decisions. In addition, scenario-based stress testing and resilience analytics support the evaluation of organizational response capabilities under extreme or compound threat conditions. These approaches allow assurance programs to move from reactive checklists toward proactive, data-driven planning that explicitly considers uncertainty and system interdependencies.

Another significant advance lies in automation and continuous assurance mechanisms, which embed security controls and monitoring directly into operational workflows. Continuous control monitoring and automated evidence collection enable real-time verification of control effectiveness, reducing the latency between detection and remediation (Sans and Cronin, 2016; Rahmaniet al., 2018). The adoption of policy-as-code frameworks and integration into continuous integration/continuous deployment (CI/CD) pipelines ensures that compliance and risk management are operationalized alongside software development, enabling immediate detection of deviations from approved configurations or standards. AI-assisted anomaly detection further enhances these systems by identifying unusual patterns of activity, adapting risk scores dynamically, and flagging potential insider or external threats before significant damage occurs. Together, these capabilities support a shift from episodic audit-based assurance toward a persistent, evidence-driven model aligned with the operational tempo of modern enterprises.

Finally, recent developments in regulatory frameworks and standards reflect the growing emphasis on risk-based cybersecurity assurance. Updates to frameworks such as NIST CSF 2.0 and ISO/IEC 27001 increasingly prioritize demonstrable risk management over purely prescriptive controls, emphasizing the need for organizations to assess, quantify, and respond to threats systematically. Regulators now focus on measurable effectiveness of security programs, encouraging reporting that links controls to risk outcomes rather than mere policy compliance. This evolution has also driven convergence between cybersecurity assurance, audit, and resilience reporting, enabling organizations to integrate operational, financial, and regulatory perspectives into a unified framework. By aligning governance structures with quantitative risk assessments, organizations can demonstrate accountability, maintain stakeholder trust, and improve strategic decision-making in the face of complex cyber threats.

Recent advances in risk-based cybersecurity assurance reflect a paradigm shift from reactive compliance to proactive, data-driven risk management. Innovations in telemetry, analytics, probabilistic modeling, and automation have enhanced the granularity, timeliness, and reliability of threat detection and risk quantification. Simultaneously, evolving regulatory expectations reinforce the integration of these technical capabilities into governance and assurance structures. Collectively, these developments enable organizations to manage cyber risks with greater precision, adaptability, and transparency, establishing a foundation for resilient, secure, and trustworthy digital ecosystems.

2.5 Data Availability Gaps and Emerging Challenges

In risk-based cybersecurity assurance, data availability is a foundational requirement, yet significant gaps persist that limit the effectiveness of threat detection, risk assessment, and mitigation strategies. These gaps emerge from both technical and organizational constraints, reflecting an ongoing asymmetry between the sophistication and adaptability of attackers and the visibility available to defenders. Attackers often operate across distributed systems, exploit zero-day vulnerabilities, and adapt quickly to defensive measures, whereas defenders rely on data streams that may be incomplete, delayed, or fragmented (Nespoliet al., 2017; Ibitoye, 2018). This persistent asymmetry creates an inherent disadvantage for organizations attempting to maintain situational awareness and proactively manage risk, particularly in complex digital environments characterized by cloud-native infrastructure, ephemeral workloads, and highly interconnected networks.

Data privacy, sovereignty, and ethical constraints further limit access to comprehensive information for cybersecurity purposes. Regulations such as the

General Data Protection Regulation (GDPR), sector-specific data protection laws, and corporate privacy policies restrict the collection, storage, and sharing of personally identifiable information (PII) and sensitive operational data. While these constraints are necessary for legal compliance and ethical stewardship, they create tension between the need for rich, high-fidelity datasets to drive risk-based modeling and the obligation to protect user privacy and respect national or organizational boundaries. Ethical considerations also extend to the use of behavioral and psychometric data for insider threat detection, where excessive monitoring may conflict with principles of fairness, consent, and transparency.

Cross-sector and cross-border data integration introduces additional challenges. Modern enterprises often operate in global, multi-supplier ecosystems where threat intelligence, vulnerability data, and incident reports must be aggregated from diverse sources. Differences in data formats, standards, reporting practices, and security controls complicate integration, often resulting in incomplete or inconsistent datasets. Geopolitical factors, regulatory discrepancies, and contractual limitations can further restrict access to critical data, leaving defenders with blind spots that attackers may exploit. Effective risk-based assurance therefore requires both technical interoperability and governance frameworks to harmonize and validate multi-source data.

Emerging threats to data integrity also pose significant challenges. Data poisoning, manipulation, and adversarial inputs represent deliberate attempts to degrade the quality of information relied upon for cybersecurity decision-making. Attackers may inject misleading or maliciously crafted data into telemetry feeds, anomaly detection systems, or machine learning models, producing false negatives, misclassifications, or inappropriate prioritization of security controls (Lambaet al., 2018; Ugwu-Ojuet al., 2018). Such attacks exploit overreliance on automated or algorithmic analyses and can undermine the confidence in risk-based assurance frameworks. Defenders must therefore implement validation, redundancy, and anomaly-checking mechanisms to maintain data reliability in adversarial environments.

Finally, the growing dependence on proprietary data sources and opaque algorithms introduces further constraints. Many organizations rely on commercial threat intelligence feeds, cloud monitoring services, and machine learning models with limited transparency regarding data provenance, modeling assumptions, and inference mechanisms. While these solutions offer scalability and convenience, their opacity can impede the verification of data quality, the explanation of risk assessments, and the alignment with organizational risk policies. Overreliance on proprietary tools also creates systemic vulnerabilities if providers experience outages, delays, or compromised data feeds.

Data availability gaps in risk-based cybersecurity assurance arise from a combination of adversarial asymmetries, regulatory and ethical constraints, integration challenges, integrity threats, and reliance on opaque sources. These gaps reduce situational awareness, hinder accurate risk modeling, and increase organizational exposure to both insider and external threats. Addressing these challenges requires a multi-faceted approach: enhancing real-time telemetry and cross-domain data sharing, implementing strong governance and ethical oversight, validating data integrity, and promoting transparency in algorithms and data sources. Only by mitigating these limitations can organizations achieve robust, adaptive, and credible risk-based cybersecurity assurance in complex, interconnected digital ecosystems.

2.6 Future Research Opportunities

The rapidly evolving landscape of cybersecurity, characterized by increasingly complex digital environments and dynamic threat actors, underscores the necessity for advancing research in risk-based cybersecurity assurance. While existing frameworks provide valuable foundations for linking security controls to organizational risk, several persistent gaps limit their effectiveness (Cramet al., 2017; Force, 2018). Future research opportunities span data availability, methodological innovations, emerging technologies, and empirical validation, and addressing these areas is critical for improving resilience, operational decision-making, and strategic risk management.

A primary area for future investigation is improving data availability and sharing mechanisms. Risk-based cybersecurity assurance depends heavily on high-quality, representative, and timely data to inform threat models, quantify exposure, and validate controls. Current limitations in internal data collection and underreporting of incidents constrain predictive and diagnostic capabilities. Research should explore the development of trusted data-sharing consortia and federated intelligence models, enabling organizations to collaborate without compromising confidentiality or competitive advantage. Federated approaches allow for the aggregation of threat intelligence, vulnerability data, and incident reports across multiple entities while maintaining local control over sensitive information. Complementary research should investigate privacy-preserving analytics, secure multiparty computation, and differential privacy, which offer mechanisms to analyze sensitive data collectively without disclosing identifiable information. Standardization efforts also represent a critical avenue, particularly through the creation of consistent taxonomies for cyber incidents, losses, and exposure metrics, which would facilitate cross-organization benchmarking, longitudinal studies, and meta-analytic insights. Collectively, these data innovations can reduce scarcity, improve completeness, and enhance the fidelity of risk-based assurance models.

A second research direction involves advancing risk modeling and assurance methodologies. Current risk models often rely on qualitative scoring or static quantitative metrics, which can limit their predictive accuracy and responsiveness in dynamic environments. Future studies should explore hybrid qualitative–quantitative assurance frameworks that combine the interpretability of qualitative risk narratives with the rigor of probabilistic or statistical modeling. This approach allows decision-makers to assess both the operational impact and the likelihood of threats in a nuanced manner. Additionally, the incorporation of explainable and auditable AI into cybersecurity risk assessment is an emergent priority. AI-driven models can enhance anomaly detection, predictive scoring, and scenario analysis, but their utility depends on transparency, traceability, and the ability to satisfy regulatory and audit requirements. Another promising line of inquiry is the design of dynamic, self-updating risk models capable of adapting to high-velocity digital environments. By continuously ingesting telemetry, threat intelligence, and behavioral data, such models can provide near-real-time risk assessments, enabling proactive mitigation and resource prioritization in complex systems (Houser, 2016; Jarviset al., 2018).

Assurance of emerging technologies and architectures represents a third critical research frontier. As organizations adopt AI systems, autonomous agents, and cyber-physical integrations, the scope and nature of risks evolve. Future research should develop risk-based assurance frameworks tailored to AI systems and autonomous agents, including mechanisms for verifying algorithmic behavior, detecting unintended emergent outcomes, and ensuring alignment with ethical and operational objectives. Similarly, the increasing adoption of zero-trust, serverless, and edge computing environments introduces unique challenges for continuous monitoring, access verification, and control enforcement. Research is needed to establish methodologies for evaluating assurance effectiveness in these distributed, adaptive, and ephemeral environments. Moreover, emerging systems often incorporate self-healing and adaptive mechanisms, which necessitate new metrics and approaches for measuring assurance efficacy, understanding system behavior under stress, and quantifying residual risk.

Finally, the field requires robust empirical validation and longitudinal studies. Many current risk-based assurance frameworks remain conceptual or validated only in limited operational contexts. Future research should prioritize large-scale empirical studies linking assurance practices to actual incident outcomes, providing evidence for the efficacy and ROI of specific controls or monitoring strategies. Validation of risk-based metrics against real-world loss events will also improve confidence in predictive models and support decision-making under uncertainty. Comparative studies across sectors, geographies, and regulatory environments can reveal patterns in assurance maturity, highlight best practices, and identify contextual factors that influence effectiveness. Longitudinal analyses can further capture trends over time, elucidate the impact of evolving threats, and inform adaptive updates to frameworks and models.

Future research in risk-based cybersecurity assurance must address the intertwined challenges of data availability, methodological rigor, emerging technology adoption, and empirical validation. By developing federated, privacy-preserving data infrastructures, advancing hybrid and self-updating risk models, extending assurance to novel architectures, and conducting large-scale longitudinal studies, the field can move beyond static or reactive approaches (Jowet al., 2017; Vaidya and Li, 2018). These initiatives will enable organizations to implement proactive, adaptive, and evidence-based cybersecurity assurance practices, enhancing resilience against both known and emergent threats while providing a robust foundation for strategic decision-making in complex digital ecosystems.

2.7 Implications for Practice and Policy

The evolution toward risk-based cybersecurity assurance presents significant practical and policy implications for organizations, boards, regulators, and the broader ecosystem of stakeholders involved in digital security governance. Unlike traditional compliance-oriented approaches, risk-based models require active engagement with probabilistic threat assessments, continuous monitoring, and evidence-driven decision-making. Consequently, organizations must not only adopt new technologies and analytical methods but also realign governance structures, cultural norms, and reporting mechanisms to fully realize the benefits of this paradigm.

For organizations transitioning to risk-based cybersecurity assurance, practical guidance emphasizes systematic capability building, process integration, and continuous improvement. First, enterprises should invest in advanced telemetry and analytics platforms that support near-real-time visibility into network, endpoint, and cloud activity. The integration of machine learning and AI-driven anomaly detection can enhance predictive risk modeling, enabling proactive mitigation strategies. Second, organizations should embed risk-based practices into operational workflows through policy-as-code frameworks and integration with CI/CD pipelines, ensuring that security controls are applied consistently across dynamic digital environments. Third, enterprises should prioritize the development of cross-functional teams combining security, data, and business expertise, thereby enabling risk assessment to inform strategic decision-making rather than remaining siloed within IT functions. Training programs and awareness campaigns further cultivate a risk-conscious culture, fostering alignment between technical controls, organizational priorities, and ethical standards (Bughinet al., 2017; Cantatore and James, 2017).

For boards, regulators, and auditors, the shift toward risk-based assurance necessitates a focus on oversight that goes beyond compliance checklists to include evaluation of the effectiveness and resilience of cybersecurity programs. Boards are increasingly expected to understand probabilistic risk assessments, scenario analysis outputs, and cyber value-at-risk metrics, integrating these insights into strategic decision-making and investment allocation. Regulators and auditors, in turn, must adopt evaluation frameworks that emphasize evidence of risk management effectiveness, encouraging organizations to demonstrate how controls mitigate real-world threats rather than simply conforming to prescriptive standards. This approach promotes accountability and incentivizes organizations to maintain up-to-date, adaptive risk management practices aligned with evolving threat landscapes.

Public–private partnerships play a crucial role in enhancing the reliability and availability of data underpinning risk-based assurance. Information sharing initiatives between government agencies, industry consortia, and cybersecurity intelligence providers improve access to threat intelligence, anomaly baselines, and best practice methodologies. Such collaborations enable organizations to benchmark their risk profiles against broader datasets, refine predictive models, and enhance situational awareness of emerging threats. Moreover, partnerships can facilitate coordinated responses to large-scale incidents and supply chain risks, reinforcing collective resilience in interconnected digital ecosystems.

Balancing transparency, accountability, and security is a critical consideration in risk-based assurance reporting. Transparency demands that organizations communicate their risk management practices, methodologies, and outcomes clearly to stakeholders, including boards, regulators, and customers. However, full disclosure of operational details or control configurations could inadvertently expose vulnerabilities to malicious actors. Therefore, organizations must design reporting frameworks that provide sufficient visibility for governance and compliance purposes while protecting sensitive operational data (Layton, 2016; Rezaee, 2017). Explainable risk metrics, anonymized analytics, and tiered reporting mechanisms can support this balance, enabling stakeholders to evaluate program effectiveness without compromising system security.

The transition to risk-based cybersecurity assurance carries profound implications for organizational practice and public policy. Organizations must integrate advanced analytics, continuous monitoring, and cross-functional governance into operational routines, while boards, auditors, and regulators must recalibrate oversight to emphasize risk effectiveness and resilience. Public–private partnerships enhance data availability and collective situational awareness, further strengthening assurance capabilities. Finally, transparent and accountable reporting frameworks that safeguard sensitive information are essential for maintaining stakeholder trust. Collectively, these measures position organizations to manage cyber risk more proactively, ensuring that digital and cloud ecosystems remain secure, resilient, and aligned with regulatory, ethical, and societal expectations.

III. CONCLUSION

Risk-based cybersecurity assurance represents a significant evolution in the management of digital security, moving beyond static compliance and control-based approaches toward a dynamic, context-aware, and strategically prioritized paradigm. Throughout this discussion, several key limitations and advances have emerged. Traditional control-centric and maturity-oriented frameworks provide baseline safeguards and process visibility but are limited in their capacity to adapt to rapidly evolving threat landscapes. Advances in probabilistic risk modeling, scenario-based assessment, and AI-driven analytics have enhanced the ability to quantify, anticipate, and prioritize risks. Nevertheless, these advances remain contingent on the availability, quality, and integrity of underlying data, highlighting persistent gaps that constrain the practical effectiveness of risk-based assurance.

The centrality of data cannot be overstated. High-fidelity threat intelligence, asset inventories, vulnerability and incident data, and system configuration information collectively form the backbone of accurate risk assessment. Attributes such as completeness, timeliness, granularity, consistency, and provenance directly influence the precision and reliability of risk calculations. In dynamic, cloud-native, and interconnected environments, continuous data flows are essential to maintain situational awareness and support adaptive responses. Gaps arising from regulatory constraints, cross-organizational fragmentation, adversarial manipulation, and dependence on opaque proprietary sources underscore the systemic vulnerabilities that organizations must address to achieve credible assurance outcomes.

These limitations emphasize the strategic importance of ongoing research and innovation. Developing robust mechanisms for secure, ethical, and standardized data sharing, enhancing real-time telemetry and anomaly detection, and integrating probabilistic modeling with operational decision-making are critical areas for both academic inquiry and practical implementation. Research that bridges technical, organizational, and governance perspectives is essential for designing assurance frameworks capable of operating in complex, high-velocity digital systems.

Ultimately, the evolution of cybersecurity assurance is trending toward continuous, data-driven models. By integrating advanced risk modeling with high-quality, continuously updated data, organizations can move from reactive, episodic assessments to proactive, adaptive, and predictive security governance. This transformation promises enhanced resilience, more informed decision-making, and a foundation for sustained digital trust in increasingly complex and interconnected operational environments.

REFERENCES

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

[2] Bendre, M.R. and Thool, V.R., 2016. Analytics, challenges and applications in big data environment: a survey. Journal of Management Analytics, 3(3), pp.206-239.

[3] Bennett, J.C., Bettencourt, M.T., Clay, R.L., Edwards, H.C., Glass, M.W., Hollman, D.S., Kolla, H., Lifflander, J.J., Littlewood, D.J., Markosyan, A.H. and Moore, S.G., 2017. ASC ATDM Level 2 Milestone# 6015: Asynchronous Many-Task Software Stack Demonstration (No. SAND-2017-9980). Sandia National Lab.(SNL-CA), Livermore, CA (United States); Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

[4] Bhattacharjee, S., 2018. Practical Industrial Internet of Things security: A practitioner's guide to securing connected industries. Packt Publishing Ltd.

[5] Borky, J.M. and Bradley, T.H., 2018. Protecting information with cybersecurity. In Effective model-based systems engineering (pp. 345-404). Cham: Springer International Publishing.

[6] Boyd, R. and Holton, R.J., 2018. Technology, innovation, employment and power: Does robotics and artificial intelligence really mean social transformation?. Journal of Sociology, 54(3), pp.331-345.

[7] Bughin, J., Hazan, E., Sree Ramaswamy, P., DC, W. and Chu, M., 2017. Artificial intelligence the next digital frontier.

[8] Cantatore, F. and James, N.J., 2017. Heroism science offers a new framework for cultivating civic virtue within clinical law programs. Australian Journal of Clinical Education, 2(1), pp.1-19.

[9] Carr, M., 2016. Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), pp.43-62.

[10] Chen, Z., Xu, G., Mahalingam, V., Ge, L., Nguyen, J., Yu, W. and Lu, C., 2016. A cloud computing based network monitoring and threat detection system for critical infrastructures. Big Data Research, 3, pp.10-23.

[11] Ciapessoni, E., Cirio, D., Kjølle, G., Massucco, S., Pitto, A. and Sforna, M., 2016. Probabilistic risk-based security assessment of power systems considering incumbent threats and uncertainties. IEEE Transactions on Smart Grid, 7(6), pp.2890-2903.

[12] Cram, W.A., Proudfoot, J.G. and D'arcy, J., 2017. Organizational information security policies: a review and research framework. European Journal of Information Systems, 26(6), pp.605-641.

[13] Eker, S., Rovenskaya, E., Obersteiner, M. and Langan, S., 2018. Practice and perspectives in the validation of resource management models. Nature communications, 9(1), p.5359.

[14] Falconi, S.M. and Palmer, R.N., 2017. An interdisciplinary framework for participatory modeling design and evaluation—What makes models effective participatory decision tools?. Water Resources Research, 53(2), pp.1625-1645.

[15] Fini, A.A.F., 2017. Optimizing Crew Performance through Integration of Human Resource Strategies into Planning of Construction Activities.

[16] Force, J.T., 2018. Risk management framework for information systems and organizations. NIST Special Publication, 800, p.37.

[17] Fraga-Lamas, P., Fernández-Caramés, T.M., Suárez-Albela, M., Castedo, L. and González-López, M., 2016. A review on internet of things for defense and public safety. Sensors, 16(10), p.1644.

[18] Heald, D., 2018. Transparency-generated trust: The problematic theorization of public audit. Financial Accountability & Management, 34(4), pp.317-335.

[19] Hibshi, H. and Breaux, T.D., 2018. Risk management and information assurance decision support. Acquisition Research Program.

[20] Houser, B.M., 2016. A model for real-time data reputation via cyber telemetry.

[21] Ibitoye, J.S., 2018. Securing smart grid and critical infrastructure through AI-enhanced

cloud networking. International Journal of Computer Applications Technology and Research, 7(12), pp.517-529.

[22] Jarvis, A., Morales, L. and Jose, J., 2018. Quality Experience Telemetry. Quality Press..

[23] Jow, J., Xiao, Y. and Han, W., 2017. A survey of intrusion detection systems in smart grid. International Journal of Sensor Networks, 23(3), pp.170-186.

[24] Katina, P.F. and Keating, C.B., 2018. Cyber-physical systems governance: a framework for (meta) cybersecurity design. In Security by design: innovative perspectives on complex problems (pp. 137-169). Cham: Springer International Publishing.

[25] Kure, H.I., Islam, S. and Razzaque, M.A., 2018. An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences, 8(6), p.898.

[26] Lamba, A., Singh, S., Balvinder, S., Dutta, N. and Rela, S., 2018. Embedding machine & deep learning for mitigating security & privacy issues in iot enabled devices & networks. International Journal For Technological Research In Engineering.

[27] Laszewski, T., Arora, K., Farr, E. and Zonooz, P., 2018. Cloud Native Architectures: Design high-availability and cost-effective applications for the cloud. Packt Publishing Ltd.

[28] Layton, T.P., 2016. Information Security: Design, implementation, measurement, and compliance. Auerbach Publications.

[29] Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M., 2017. Cyberfraud and the implications for effective risk-based responses: themes from UK research. Crime, Law and Social Change, 67(1), pp.77-96.

[30] Luciano, M.M., Mathieu, J.E., Park, S. and Tannenbaum, S.I., 2018. A fitting approach to construct and measurement alignment: The role of big data in advancing dynamic theories. Organizational Research Methods, 21(3), pp.592-632.

[31] McAdam, R., Bititci, U. and Galbraith, B., 2017. Technology alignment and business strategy: A performance measurement and dynamic capability perspective. International Journal of Production Research, 55(23), pp.7168-7186.

[32] Mehan, J., 2016. Insider threat: A guide to understanding, detecting, and defending against the enemy from within. IT Governance Ltd.

[33] Moore, D. and Rid, T., 2016. Cryptopolitik and the Darknet. Survival, 58(1), pp.7-38.

[34] Nandigama, N.C., 2016. Teradata-driven big data analytics for suspicious activity detection with real-time Tableau dashboards. International Journal For Innovative Engineering and Management Research, 5(1), pp.73-78.

[35] Nespoli, P., Papamartzivanos, D., Mármol, F.G. and Kambourakis, G., 2017. Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks. IEEE Communications Surveys & Tutorials, 20(2), pp.1361-1396.

[36] NETTO, M.A., TOOSI, A.N., RODRIGUEZ, M.A., LLORENTE, I.M., DI VIMERCATI, S.D.C., SAMARATI, P., MILOJICIC, D., VARELA, C., BAHSOON, R., DE ASSUNCAO, M.D. and RANA, O., 2018. A Manifesto for Future Generation Cloud Computing: Research Directions for the Next Decade.

[37] Nicho, M., 2018. A process model for implementing information systems security governance. Information & Computer Security, 26(1), pp.10-38.

[38] Nikolakis, W., John, L. and Krishnan, H., 2018. How blockchain can shape sustainable global value chains: An evidence, verifiability, and enforceability (EVE) framework. Sustainability, 10(11), p.3926.

[39] Nissen, C., Gronager, J.E., Metzger, R.S. and Rishikof, H., 2018. Deliver uncompromised: A strategy for supply chain security and resilience in response to the changing character of war.

[40] No, W.G. and Vasarhelyi, M.A., 2017. Cybersecurity and continuous assurance. Journal of Emerging Technologies in Accounting, 14(1), pp.1-12.

[41] Nwankwo, C.O. and Ihueze, C.C., 2018. Corrosion rate models for oil and gas pipeline systems a numerical approach. International Journal of Engineering Research and Technology.

[42] Onovo, A.A., Nta, I.E., Onah, A.A., Okolo, C.A., Aliyu, A., Dakum, P., Atobatele, A.O. and Gado, P., 2015. Partner HIV serostatus disclosure and determinants of serodiscordance among prevention of mother to child transmission clients in Nigeria. BMC public health, 15(1), p.827.

[43] Palomino, J., Muellerklein, O.C. and Kelly, M., 2017. A review of the emergent ecosystem of collaborative geospatial tools for addressing environmental challenges. Computers, Environment and Urban Systems, 65, pp.79-92.

[44] Pappas, I.O., Mikalef, P., Giannakos, M.N., Krogstie, J. and Lekakos, G., 2018. Big data and business analytics ecosystems: paving the way towards digital transformation and sustainable societies. Information systems and e-business management, 16(3), pp.479-491.

[45] Paté-Cornell, M.E., Kuypers, M., Smith, M. and Keller, P., 2018. Cyber risk management for critical infrastructure: a risk analysis model and three case studies. Risk Analysis, 38(2), pp.226-241.

[46] Rahmani, A.M., Gia, T.N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M. and Liljeberg, P., 2018. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 78, pp.641-658.

[47] Reetz, M.A., Prunty, L.B., Mantych, G.S. and Hommel, D.J., 2017. Cyber risks: Evolving threats, emerging coverages, and ensuing case law. Penn St. L. Rev., 122, p.727.

[48] Rezaee, Z., 2017. Business sustainability: Performance, compliance, accountability and integrated reporting. Routledge.

[49] Romanosky, S., 2016. Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), pp.121-135.

[50] Sans, V. and Cronin, L., 2016. Towards dial-a-molecule by integrating continuous flow, analytics and self-optimisation. Chemical Society Reviews, 45(8), pp.2032-2043.

[51] Scholz, R.W., Bartelsman, E.J., Diefenbach, S., Franke, L., Grunwald, A., Helbing, D., Hill, R., Hilty, L., Höjer, M., Klauser, S. and Montag, C., 2018. Unintended side effects of the digital transition: European scientists' messages from a proposition-based expert round table. Sustainability, 10(6), p.2001.

[52] Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L.Y. and Xiang, Y., 2018. Data-driven cybersecurity incident prediction: A survey. IEEE communications surveys & tutorials, 21(2), pp.1744-1772.

[53] Thompson, M.P., MacGregor, D.G. and Calkin, D., 2016. Risk management: core principles and practices, and their relevance to wildland fire. Gen. Tech. Rep. RMRS-GTR-350. Fort Collins, CO: US Department of Agriculture, Forest Service, Rocky Mountain Research Station. 29 p., 350.

[54] Tsakalidis, G., Vergidis, K., Madas, M. and Vlachopoulou, M., 2018. Cybersecurity threats: a proposed system for assessing threat severity. In Proceedings of the the forth international conference on decision support system technology–ICDSST 2018.

[55] Tupa, J., Simota, J. and Steiner, F., 2017. Aspects of risk management implementation for Industry 4.0. Procedia manufacturing, 11, pp.1223-1230.

[56] Ugwu-Oju, U. M., Okeke, O. T., & Nwankwo, C. O. (2018). Advances in cybersecurity protection for sensitive business digital infrastructure. IRE Journals, 1(11), 127–135.

[57] Ugwu-Oju, U. M., Okeke, O. T., & Nwankwo, C. O. (2018). Conceptual model improving encryption strategies for organizational information protection. IRE Journals, 2(2), 139–147.

[58] Ugwu-Oju, U. M., Okeke, O. T., & Nwankwo, C. O. (2018). Conceptual model improving digital workflows within organizational information

[59] Ugwu-Oju, U. M., Okeke, O. T., & Nwankwo, C. O. (2018). Review of network protocol stability techniques for enterprise information systems. IRE Journals, 1(8), 196–204.

[60] Vaidya, J. and Li, J. eds., 2018. Algorithms and Architectures for Parallel Processing: 18th International Conference, ICA3PP 2018, Guangzhou, China, November 15-17, 2018, Proceedings, Part IV (Vol. 11337). Springer.