




## Leadership Commitment: A Key Factor in Implementation of Event-Based Cybersecurity Risk Assessment

Wan Azlena Wan Mohamad<sup>1</sup> , Noor Hayani Abd Rahim<sup>2\*</sup>   
Nurul Nuha Abdul Molok<sup>3</sup> 

<sup>1</sup>Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Jalan Gombak, 53100 Kuala Lumpur, Selangor, Malaysia

Email: wannazlena@gmail.com

<sup>2</sup>Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Jalan Gombak, 53100 Kuala Lumpur, Selangor, Malaysia

Email: noorhayani@iium.edu.my

<sup>3</sup>Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Jalan Gombak, 53100 Kuala Lumpur, Selangor, Malaysia

Email: nurulnuha@iium.edu.my

### ABSTRACT

#### CORRESPONDING

#### AUTHOR (\*):

Noor Hayani Abd Rahim  
(noorhayani@iium.edu.my)

#### KEYWORDS:

Leadership commitment  
Cybersecurity risk assessment  
Event-based approach

#### CITATION:

Wan Azlena Wan Mohamad, Noor Hayani Abd Rahim, & Nurul Nuha Abdul Molok. (2025). Leadership Commitment: A Key Factor in Implementation of Event-Based Cybersecurity Risk Assessment. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, 10(4), e003365. <https://doi.org/10.47405/mjssh.v10i4.3365>

Implementing event-based cybersecurity risk assessment offers organisations a proactive approach to managing cyber threats in real-time. Unlike the asset-based approach, the event-based approach focuses on identifying and analysing potential cyber-attacks or events, rather than relying on static asset inventories. However, successful cybersecurity implementation relies not only on technical expertise but also on managerial expertise, such as strong leadership commitment. Leadership plays an important role in prioritising cybersecurity initiatives. It secures the necessary resources and ensures strategic integration into the organisation's overall risk management framework. Despite its importance, limited research explores the impact of leadership commitment on implementing event-based cybersecurity risk assessment in organisations. This study uses a qualitative research approach to address this gap through semi-structured interviews with ten cybersecurity experts across multiple public sector organisations in Malaysia. Thematic analysis revealed three key leadership factors: (i) top management buy-in, which embeds cybersecurity into organisational priorities; (ii) resource allocation, which ensures adequate funding and support; and (iii) leadership advocacy, which maintains cybersecurity as a strategic agenda. These findings highlight that without strong leadership support, organisations may struggle to successfully implement event-based cybersecurity risk assessment. This study contributes to cybersecurity governance research by highlighting the critical role of leadership in adopting event-based cybersecurity risk assessment. It highlights the need for strategic leadership engagement in shaping cybersecurity policy, allocating resources and fostering a cyber risk-aware

culture. The findings also provide practical insights for policymakers, cybersecurity professionals and organisational leaders in developing risk management frameworks to strengthen cybersecurity resilience.

**Contribution/Originality:** This study contributes original insights by highlighting the role of leadership commitment in implementing event-based cybersecurity risk assessment in the Malaysian public sector. It also offers practical guidance for public sector organisations to enhance cybersecurity resilience and governance.

## 1. Introduction

In today's interconnected world, the advancement of technology changes business operations, the way governments function, the way we work, and even the way we live. Nonetheless, this digital transformation amplifies organisations' exposure to cyber risks (Krishtanov & Brovko, 2023). As organisations rely on digital infrastructure, exposure to cyber-attacks is on the rise, interrupting services, disclosing sensitive information and eroding customer confidence (National Cybersecurity Agency, 2020). These growing trends and changes in the current cyber threat landscape highlight the importance of cybersecurity risk management in organisations.

Leadership in cybersecurity can be defined as the ability to guide, influence, and motivate individuals or teams within an organisation to prioritise and effectively manage cybersecurity practices. This includes establishing a culture of awareness, fostering engagement with security policies, and ensuring that the organisation's defensive strategies are aligned with its overall goals. As noted by Ujah et al. (2024), strong leadership fosters a culture of awareness and responsible technology use, which is crucial for mitigating risks in cybersecurity.

Leadership commitment is one of the key factors influencing successful cybersecurity risk management practices in organisations. This is due to top management having a crucial role in prioritising cybersecurity efforts, securing funds, and facilitating a business culture around risk assessment practices (Nurwanah, 2024). The work of Finkelstein et al. (2009) on Strategic Leadership Theory suggests leaders articulate organisational vision, allocate scarce resources, and have an impact on longer-term outcomes via the setting of strategic direction. In the cybersecurity domain, leaders help drive policy alignment, make sure the workforce is prepared, and integrate cybersecurity into a larger strategy for their organisation. Without leadership support, cybersecurity initiatives are often thwarted due to financial constraints, resistance to change and misalignment with organisational priorities.

Despite this acknowledged importance, limited research has specifically explored the role of leadership commitment in the context of event-based cybersecurity risk assessment. This study addresses this gap by investigating how leadership commitment influences the successful implementation of event-based cybersecurity risk assessment across public sector organisations. Adopting a qualitative research design, the study draws on in-depth interviews with ten cybersecurity experts to gather rich insights into leadership's influence on policy development, resource allocation, and strategic decision-making in cybersecurity governance. Accordingly, the primary objective of this study is to examine the role of leadership commitment in shaping the implementation of event-based cybersecurity risk assessment within organisations.

This article begins with an introduction, followed by a review of the literature on cybersecurity risk assessment and leadership commitment. The methodology section explains the qualitative research design and thematic analysis approach used to interpret expert perspectives. The findings section presents key themes and sub-themes that emerged from the data, highlighting leadership's role in driving cybersecurity initiatives. Finally, the discussion and conclusion provide theoretical implications, practical recommendations, and policy considerations for strengthening leadership engagement in event-based cybersecurity risk assessment.

## 2. Literature Review

This section presents a review of the literature on cybersecurity risk assessment and the role of leadership commitment in cybersecurity governance.

### 2.1. Cybersecurity Risk Assessment

According to the [International Organization for Standardization \(ISO\) \(2020\)](#), cybersecurity refers to safeguarding people, society, organisations and nations from cyber risks. Cybersecurity focuses on managing risks within cyberspace, an interconnected digital environment that often extends beyond organisational boundaries. In this space, entities share information, interact digitally, and are responsible for responding to cybersecurity incidents ([ISO, 2020](#)).

Cybersecurity risk management encompasses a comprehensive process of identifying, assessing, and mitigating threats to protect individuals, organisations, and nations from cyber risks ([Chen et al., 2021](#); [Lau et al., 2021](#); [Sukumar et al., 2023](#)). According to the [National Institute of Standards and Technology \(NIST\) \(2024\)](#), cybersecurity risk management is essential for addressing risks related to the loss of the confidentiality, integrity, and availability of an organisation's data. The importance of cybersecurity risk management is to ensure that organisations can face cyber threats proactively, reduce the risks that may arise, and increase resistance to cyber-attacks ([Ahmad et al., 2020](#)).

Cybersecurity risk assessment is one of the fundamental components of an organisational cybersecurity risk management process ([NIST, 2012](#)). A robust risk assessment process is essential for devising effective strategies to protect against cyber-attacks and ensure the resilience of public sector operations. A cybersecurity risk assessment framework is a structured methodology designed to help organisations identify, analyse and evaluate cybersecurity risks in line with their overall business objectives ([Mumtaz Awan & Riaz Pitafi, 2024](#)). These frameworks typically integrate various components to effectively assess cybersecurity risks ([Elmarady & Rahouma, 2021](#)).

### 2.2. Approaches in Cybersecurity Risk Assessment

There are two primary approaches to risk assessment: the event-based approach and the asset-based approach ([ISO, 2022](#)). In an asset-based approach, the underlying concept is that risks can be identified and assessed through an inspection of assets, threats and vulnerabilities. An asset is anything that has value to the organisation and, therefore, requires protection ([ISO, 2022](#)).

According to [ISO \(2022\)](#), an event-based approach to cybersecurity risk assessment focuses on analysing potential cyber events or incidents that could affect the



confidentiality, integrity and availability of digital data. In this context, an “event” refers to any occurrence or change in circumstances that may affect security (ISO, 2022). This approach involves identifying specific threats, understanding their potential impact and developing strategies to mitigate those threats (ISO, 2022). By focusing on events, this method aims to provide a more dynamic and responsive framework for managing cyber risk. This is particularly important given the rapidly evolving nature of cyber threats.

### 2.3. Leadership

Leadership can be understood as a multifaceted process that involves guiding, influencing, and motivating individuals or groups to achieve specific goals. At its core, leadership is often defined as the ability to influence others toward a common objective.

Muna (2022) argues that leadership involves individual traits, behaviours, interaction patterns, and role relationships, emphasising that it is fundamentally a process rather than just a position held by a certain individual. This notion underscores the dynamic nature of leadership, where the relationship between leaders and their followers plays a crucial role in achieving shared outcomes.

Strategic leadership plays a crucial role in ensuring the successful implementation of event-based cybersecurity risk assessment, particularly through effective resource allocation and policy-making. These two elements are essential for translating strategic plans into tangible outcomes, as they determine how financial, human, and technological resources are distributed and governed within an organization (Finkelstein et al., 2009). Without strategic oversight in these areas, even the most well-formulated strategies may fail to achieve their intended objectives. By ensuring that financial, human, and technological resources are optimally distributed and by establishing a strong governance framework, leaders can drive organisational success (Finkelstein et al., 2009).

### 2.3. Leadership in Cybersecurity

Cybersecurity leadership can be defined as the ability to guide, influence, and motivate individuals or teams within an organisation to prioritise, implement, and sustain cybersecurity practices. It involves more than technical oversight. It encompasses strategic vision, risk-informed decision-making, and the capacity to foster a security-conscious culture.

Cybersecurity leaders are responsible for shaping and executing strategies that safeguard organisational assets, ensure regulatory compliance, and respond to evolving threats. As noted by Goli et al. (2023), cybersecurity leaders must possess a deep understanding of emerging technologies and threat landscapes to make informed decisions and drive proactive security measures across the organisation.

A critical component of effective cybersecurity leadership is establishing a robust cybersecurity culture, characterised by collective behaviours shaped by beliefs, values, and attitudes regarding cybersecurity within an organisation (Aksoy, 2024). The success of such a culture largely depends on the knowledge and skills of the leadership, along with proactive communication strategies that promote continuous learning (Aksoy, 2024).

Leaders who emphasise the importance of cultivating cybersecurity awareness throughout the organisation encourage employees to adopt safer online behaviours driven by a genuine understanding of potential risks (He et al., 2019). The adoption of cybersecurity policies and the implementation of training programs are markedly enhanced in environments where leadership actively champions these efforts (Abrahams et al., 2024). As such, top management must understand not only the technical aspects of cybersecurity but also the social and behavioural dimensions that contribute to a secure organisational environment (Triplett, 2022).

#### 2.4. Leadership Commitment

Leadership commitment includes a strong alignment with the organisational vision and goals. Leaders who demonstrate a high level of commitment are actively involved in setting and communicating strategic objectives, ensuring that these align with the organisation's mission. This aligns with the results of Khaw et al. (2024), indicating that top management support is crucial for complying with overarching strategies in cybersecurity contexts.

Committed leaders foster a culture that emphasises core values, ethical standards, and acceptable practices. Nurwanah (2024) emphasises that effective leadership in cybersecurity transcends technical challenges and requires a strategic shift that incorporates corporate culture and leadership commitments in shaping practices. This cultural dedication cultivates an environment where employees feel valued and engaged, fostering loyalty and organisational cohesion.

The extent of leadership commitment directly impacts organizational performance. When leaders actively demonstrate their commitment, it encourages employees to adopt similar attitudes, leading to greater engagement and motivation. Research indicates that strong leadership commitment is crucial for effective cybersecurity culture, as employees are more likely to adhere to security protocols and be proactive in reporting incidents (Safitra et al., 2023).

Furthermore, leadership commitment enhances collaboration and communication within teams. As identified by Shaikh and Siponen (2023), committed leadership fosters an environment in which individuals are more willing to share information and collaborate on risk management. This collaboration is particularly critical in cybersecurity, where swift communication and coordinated efforts can significantly mitigate risks and reduce the impact of potential incidents.

Additionally, the role of dedicated leaders, such as the Chief Information Security Officer (CISO), cannot be overlooked. The presence of such figures is crucial in fostering a cybersecurity culture and strategic investment in ensuring preparedness for potential threats (Neri et al., 2024). Through strategic investment in cybersecurity resources driven by leadership commitments, organisations can reduce the likelihood of security incidents and fortify their defenses against cyber-attacks (Benjamin et al., 2024).

The impacts of successful leadership commitment to cybersecurity initiatives extend beyond mere compliance with regulations. They enhance employee engagement, foster a proactive culture, improve organisational performance, and increase resilience to cyber threats. This multifaceted influence underscores the importance of leadership in

cultivating an environment where cybersecurity is prioritised and actively championed across all levels of the organisation.

This study contributes to the existing body of knowledge by providing empirical insights into how leadership commitment shapes event-based cybersecurity risk assessment implementation in organisations. The findings offer practical recommendations for policymakers, cybersecurity professionals, and organisational leaders in enhancing cybersecurity governance.

### 3. Research Methods

This section outlines the research methodology employed in this study. It details the research design, sampling strategy, data collection methods, and data analysis approach. These elements provide a clear framework for how the study was conducted.

#### 3.1. Research Design

This study employs a qualitative research approach to examine the role of leadership commitment in the successful implementation of event-based cybersecurity risk assessment within organisations. Qualitative research allows researchers to dig deeper into understanding these issues and how participants understand them (Creswell & Poth, 2016). In an interdisciplinary field of research like cybersecurity, qualitative methodologies play a crucial role in guaranteeing the diversity of knowledge gained (Fujs et al., 2019).

#### 3.2. Data Sampling and Collection

To ensure that the study involved participants with relevant expertise, purposive sampling was used. This sampling technique allowed for the selection of individuals with in-depth knowledge and experience in cybersecurity risk assessment. Appropriate participant selection was important as it enabled the study objectives to be achieved (Etikan, 2016).

Expert interviews are a widely used qualitative interview method often aiming at gaining information about or exploring a specific field of action (Döringer, 2021). Experts are considered knowledgeable of a particular subject and are identified by their specific knowledge, community position, or status (Döringer, 2021). For this study, A total of ten cybersecurity experts from various public sector organisations participated in the study as presented in Table 1.

Table 1: Participants

Participants	Organisation Specialisation	Gender	Portfolio	Total Years of Service
Participant 1	Specializes in national cybersecurity policies, strategies, and incident management	Female	Officer, Expert, Consultant	20
Participant 2	Focuses on construction, public works, and infrastructure development	Male	Officer, Expert	17



Participants	Organisation Specialisation	Gender	Portfolio	Total Years of Service
Participant 3	Responsible for coordinating national policies, strategic planning, and high-level governance	Female	Officer, Expert	15
Participant 4	Specializes in public sector training and professional development	Female	Officer, Expert, Consultant	16
Participant 5	Oversees human resources, policies, and operations for the Malaysian civil service	Male	Officer, Expert, Consultant	17
Participant 6	Manages cross-ministerial coordination, national projects, and strategic initiatives	Male	Officer, Expert, Consultant	21
Participant 7	Focuses on immigration management, passport services, and border control.	Female	Officer, Expert	15
Participant 8	Responsible for driving national digitalization and ICT development	Female	Officer, Expert, Consultant	24
Participant 9	Manages national finances, budgeting, and economic policy	Female	Officer, Expert, Consultant	21
Participant 10	Oversees national security, law enforcement, and internal affairs.	Female	Officer, Expert	18

Participants were selected based on specific criteria. They were required to have at least 10 years of experience and be actively involved in their organisation's cybersecurity strategy. Additionally, they needed to be part of the management or professional team. These selection criteria ensured that participants provided valuable insights into the role of leadership in event-based cybersecurity risk assessment.

### 3.3. Research Instrument

This study collected data through semi-structured interviews. It allowed for both guided discussions and open-ended responses. Interview questions were designed in line with the research questions. The interview questions aimed to understand the influence of leadership commitment on event-based cybersecurity risk assessment. Each interview lasted between 45 and 60 minutes and was conducted in person. All interviews were audio-recorded with the participants' consent and transcribed verbatim for accuracy and reliability in data analysis.

### 3.4. Data Analysis

Thematic analysis was employed to analyse the interview data. This method was chosen for its ability to systematically identify, organise, and interpret patterns (themes) within qualitative data. The data in this study were analysed using the following steps based on [Abdul Molok et al. \(2013\)](#), [Braun and Clarke \(2022\)](#), and [Matthew et al. \(2018\)](#):

- i. Preparing the transcriptions: The recorded interviews were transcribed verbatim to ensure the accuracy of the data. Every spoken word and relevant expression was captured exactly as stated by the participants. This step was crucial to ensure the accuracy, authenticity, and completeness of the data.
- ii. Reading, understanding and translating the transcripts: The transcriptions were carefully reviewed to gain a comprehensive understanding of the responses, and translations were made where necessary.
- iii. Highlighting the key statements that are relevant to research objectives: Important excerpts related to leadership commitment and cybersecurity risk assessment were identified and marked for further analysis.
- iv. Grouping and coding the key statements: The highlighted statements were categorised into initial codes based on recurring concepts and patterns in the data
- v. Deriving the themes and sub-themes: The themes and sub-themes were directly aligned with the research objective and question. It provides a structured and meaningful interpretation of the data.
- vi. Finalising and writing the results: The identified themes and sub-themes were refined and structured into a coherent findings section, supported by participant quotes and interpretations.

The analysis of the interview data provided a structured and insightful interpretation of how leadership commitment influences the successful implementation of event-based cybersecurity risk assessment. It revealed that leadership commitment is not only a facilitator but a driving force behind the integration of cybersecurity into organisational strategy. These insights offer a deeper understanding of the practical and strategic roles that leadership plays in shaping cybersecurity resilience within public sector organisations.

### 3.5. Themes and Subthemes

The thematic analysis of the interview data revealed three overarching themes that illustrate the critical role of leadership commitment in the successful implementation of event-based cybersecurity risk assessment. These themes provide valuable insights into how leadership influences the implementation of cybersecurity risk assessment within organisations. The identified themes and subthemes are presented in [Table 2](#).

The first theme, top-level management buy-in, highlights the importance of securing executive endorsement and leadership alignment. Participants emphasised that leadership commitment is essential for embedding cybersecurity into the organisation's broader risk management framework. Leadership not only signals the importance of cybersecurity but also drives the development and enforcement of policies that align with organisational goals.

The second theme, resource allocation and strategic investment, focuses on the need for sustained financial commitment to ensure the effective implementation of cybersecurity initiatives. Leadership plays a central role in allocating budgets for cybersecurity tools, training, and skilled personnel. Participants noted that resource constraints often stem from leadership's failure to view cybersecurity as a strategic priority, resulting in competing demands diverting funding elsewhere.



Table 2: Themes and Subthemes

Theme	Subtheme	Key Insights
Top-Level Management Buy-In	Executive Endorsement for Cybersecurity Integration Leadership's Role in Driving Cybersecurity Policy Organisational Resistance to Cybersecurity Change	Leadership commitment is essential for embedding cybersecurity into broader risk management frameworks. Without leadership alignment, cybersecurity initiatives face resistance and fragmentation.
Resource Allocation and Strategic Investment	Budgetary Commitment to Cybersecurity Tools Funding Challenges and Competing Priorities Impact of Resource Constraints on Cybersecurity Readiness	Without strategic investment, cybersecurity teams are underfunded and ill-equipped, reducing the organisation's ability to respond to cyber threats.
Leadership's Role in Organisational Prioritisation	Cybersecurity as an Organisational Priority Workplace Cybersecurity Culture and Awareness Leadership-Driven Risk Governance and Compliance	Strong leadership ensures cybersecurity remains a top organisational priority. Leadership fosters a security-conscious culture and drives policy enforcement.

The third theme, leadership's role in organisational prioritisation, underscores the influence of leadership in maintaining cybersecurity as a central concern across all levels of the organisation. Strong leadership ensures that cybersecurity is not treated merely as a technical or IT issue, but rather as an integral part of the organisational strategy. When leaders actively champion cybersecurity, it is more likely to be supported, resourced, and effectively implemented.

These three themes demonstrate that leadership commitment is not only influential but foundational to the success of event-based cybersecurity risk assessment adoption. The presence or absence of leadership support significantly affects the organisation's ability to prioritise, fund, and integrate cybersecurity measures within its strategic and operational landscape.

#### 4. Findings and Discussion

This section presents the findings derived from interviews with ten cybersecurity experts, focusing on the role of leadership commitment in the successful implementation of event-based cybersecurity risk assessment.

The findings indicate that while technical expertise is essential, leadership commitment is the key enabler for ensuring that event-based cybersecurity risk assessment is prioritised, properly resourced, and effectively integrated into an organisation's risk management strategy. All participants unanimously emphasised that without strong leadership support, the implementation of an event-based approach faces significant challenges, including organisational resistance, insufficient funding, and a lack of clear cybersecurity policies.

Through thematic analysis of the interview data, three key themes emerged as critical leadership factors influencing the adoption of event-based cybersecurity risk assessment:

top-level management buy-in, resource allocation, and organisational prioritisation of cybersecurity.

#### 4.1. Top-Level Management Buy-In as a Strategic Driver

This theme refers to the necessity of securing executive approval and leadership alignment to successfully implement event-based cybersecurity risk assessment. Leadership buy-in ensures that cybersecurity is treated as a strategic priority rather than a standalone technical concern. Without active endorsement from top management, the implementation of an event-based approach faces significant organisational resistance and lacks the necessary integration into broader risk management frameworks. All participants agreed that top-level management buy-in is needed to successfully implement an event-based cybersecurity risk assessment.

Participant 1 underscored the critical role of leadership buy-in, stating: *"To implement the event-based approach, there needs to be buy-in from top management. Top management must understand why we want to use this approach and provide their approval"*. Without this endorsement, cybersecurity initiatives risk being deprioritised, making implementation efforts inconsistent and ineffective.

Echoing this sentiment, Participant 3 highlighted the consequences of weak leadership support: *"Without top-level support, cybersecurity remains a secondary priority, and agencies will not be fully committed to its implementation"*. This statement reflects the reality that when cybersecurity lacks executive backing, it struggles to gain organisational traction, leading to fragmented adoption and inadequate risk management.

Moreover, participants emphasised that leadership commitment is essential for embedding cybersecurity within the organisation's broader risk management strategy rather than treating it as a standalone technical issue. Participant 5 reinforced this point, warning: *"If leadership does not drive the change, cybersecurity will always take a backseat to other operational concerns"*. This insight suggests that without leadership advocacy, cybersecurity will continue to be overshadowed by other organisational priorities, limiting its effectiveness in protecting against evolving cyber threats.

Findings suggest that without leadership alignment, the implementation of event-based risk assessment approaches will face significant obstacles. Effective leadership serves as the foundation for cybersecurity success. This is because it drives the establishment of clear policies, ensures strategic resource allocation, and strengthens governance structures that support accountability and regulatory compliance (Safitra et al., 2023). Without this commitment, cybersecurity initiatives risk being de-prioritized, leading to fragmented risk management practices. This may reduce organisational resilience. Research has shown that organisations with strong management support tend to exhibit stronger cybersecurity readiness. This is because leadership advocacy fosters a proactive security culture and strengthens the risk assessment framework (Neri et al., 2024). Therefore, ongoing leadership engagement is essential. It is to ensure that event-based risk assessment is properly integrated into the organisation's broader cybersecurity strategy.

In conclusion, without leadership alignment, event-based risk assessment faces resistance, leading to fragmented cybersecurity implementation. Strong leadership

advocacy drives policy development, ensures accountability, and strengthens governance to enhance cybersecurity resilience.

#### 4.2. Resource Allocation and Strategic Investment in Cybersecurity

This theme focuses on the importance of financial commitment and resource allocation for successfully implementing event-based cybersecurity risk assessment. Cybersecurity initiatives require investments in personnel, tools, and continuous monitoring, which depend on leadership's willingness to prioritise cybersecurity funding. Without strategic leadership commitment, funding for cybersecurity can be diverted to other priorities, leaving cybersecurity teams understaffed and underequipped. All participants agreed that leadership commitment is important to get the financial commitment and resource allocation for successfully implementing an event-based cybersecurity risk assessment.

Participant 5 highlighted the significant challenge of resource constraints, stating: *"Without the support of top management, implementing an event-based approach will be difficult because we need resources and alignment from the leadership level"*. This underscores the dependence of cybersecurity initiatives on executive leadership for securing the necessary financial and operational support.

Expanding on this point, Participant 2 emphasised the importance of budget allocation, stating: *"Cybersecurity investment is not a luxury, it is a necessity. Leaders must allocate sufficient budgets to ensure that organisations are equipped with the right tools and personnel"*. This perspective reinforces that without a sustained financial commitment from leadership, cybersecurity programs risk becoming underfunded, limiting their effectiveness in mitigating evolving cyber threats.

Participant 7 further explained how leadership perceptions influence funding priorities, noting: *"When leadership does not see cybersecurity as a business priority, budgets get diverted elsewhere, leaving cybersecurity teams underfunded and understaffed"*. This reflects a common organisational challenge where cybersecurity is often seen as an operational rather than strategic necessity, leading to insufficient financial support.

These insights collectively highlight the critical role of leadership in sustaining cybersecurity funding. The findings underscore that without strategic investment and strong leadership prioritisation, the implementation of an event-based cybersecurity risk assessment approach will face significant challenges. Sustained financial commitment is crucial to equipping organisations with advanced cybersecurity tools, hiring skilled personnel, and maintaining continuous threat monitoring capabilities. Without dedicated leadership support, cybersecurity initiatives risk being deprioritised, leading to weakened defences and heightened exposure to cyber threats (Al-Kumaim & Alshamsi, 2023). This lack of commitment not only leaves cybersecurity teams understaffed but also deprives them of the necessary tools, training, and resources required to detect, prevent, and respond to cyber incidents, further risking the organisation to vulnerabilities (Al-Hawamleh, 2024). Therefore, fostering a cybersecurity-conscious leadership culture is essential to ensuring a proper implementation of an event-based risk assessment approach.

In conclusion, leadership plays a pivotal role in securing sustained financial investment for cybersecurity. Without strategic investment, organisations lack the tools, personnel,



and infrastructure needed for event-based cybersecurity risk assessment, increasing their vulnerability to cyber threats.

#### 4.3. Leadership's Role in Organisational Prioritisation of Cybersecurity

This theme highlights the role of executive leadership in ensuring cybersecurity remains an organisational priority. Leadership commitment influences risk management strategies, security culture, and policy enforcement. It ensures that cybersecurity is not overlooked in favour of other operational demands. All participants agreed that leadership commitment is important to ensuring cybersecurity remains an organisational priority.

Participant 7 underscored the pivotal role of leadership in ensuring cybersecurity remains a top organisational priority, stating: *"The role of management is crucial. They need to ensure cybersecurity is prioritised and allocate enough resources for proper implementation"*. This highlights the responsibility of leadership in driving cybersecurity initiatives, ensuring they receive the necessary attention and resources for effective execution.

Similarly, Participant 3 warned that cybersecurity is often misclassified as a purely technical issue rather than a strategic imperative, which can result in limited investment and organisational neglect. They cautioned: *"If leadership does not actively drive cybersecurity efforts, it will always take a backseat to other operational concerns"*. This perspective reflects a common challenge where cybersecurity struggles to compete with other business priorities, leading to gaps in risk management and security preparedness.

Reinforcing the need for leadership integration in cybersecurity governance, Participant 10 stated: *"Cybersecurity should be part of the organisation's broader risk strategy, not a standalone strategy"*. This insight highlights the necessity of embedding cybersecurity within the overall risk management framework, ensuring it is not treated as an isolated concern but as a core component of organisational resilience.

Collectively, these perspectives emphasise that strong leadership advocacy is essential for developing structured cybersecurity frameworks. In contrast, a lack of leadership commitment results in delays, resistance, and ineffective implementation, ultimately weakening an organisation's ability to defend against cyber threats. According to [Layapan et al. \(2022\)](#), strong leadership enables organisations to thrive and prosper, fostering growth, stability, and resilience. When organisations succeed, they achieve financial sustainability and create a more motivated and productive workforce ([Layapan et al., 2022](#)). When leadership demonstrates a strong commitment to cybersecurity, it not only drives investment in critical resources but also builds a workplace culture. A culture where employees understand and adhere to security protocols and best practices ([Sallos et al., 2019](#)). Leadership sets the tone for how cybersecurity will be prioritised within an organisation. Without clear guidance and support from top management, cybersecurity efforts risk being overshadowed by more immediate business objectives. This situation leaves the organisation vulnerable to evolving threats ([Mumtaz Awan & Riaz Pitafi, 2024](#)).

In conclusion, leadership advocacy ensures that cybersecurity remains a strategic focus rather than being deprioritised. Strong leadership promotes a cybersecurity-conscious culture, drives risk governance, and ensures compliance with cybersecurity best practices.

#### 4.4. Summary of Findings

The thematic analysis highlights that leadership commitment is a fundamental enabler of event-based cybersecurity risk assessment. The findings indicate that without executive buy-in, adequate resource allocation, and strong leadership advocacy, cybersecurity risk assessment initiatives may face implementation barriers, resource shortages, and lack of strategic alignment.

The study suggests that organisations should focus on encouraging executive leadership engagement in cybersecurity decision-making. Leadership engagement ensures sustainable financial investment in cybersecurity tools, personnel, and infrastructure. Leadership commitments foster a cybersecurity-aware culture that integrates security practices into daily operations.

These findings align with strategic leadership theory, which highlights the role of leadership in shaping organisational policies, risk management strategies, and long-term cybersecurity resilience. Strengthening leadership commitment will enable organisations to effectively adopt and sustain event-based cybersecurity risk assessment frameworks.

#### 5. Conclusions

This study examines the critical role of leadership commitment in the successful implementation of event-based cybersecurity risk assessment within organisations. The implementation of an event-based cybersecurity risk assessment demands not only technical expertise but also managerial expertise such as strong leadership engagement. Top management plays a pivotal role in ensuring that cybersecurity is prioritised, adequately resourced, and strategically integrated into an organisation's overall risk management framework.

The impact of leadership commitment on the implementation of event-based cybersecurity risk assessments is profound and multifaceted. Leadership commitment shapes how cybersecurity is viewed, prioritised, and managed within an organisation. The findings underscore that leadership commitment is not just an administrative necessity but a strategic imperative in cybersecurity governance. Without executive support, adequate resource allocation, and leadership advocacy, event-based cybersecurity risk assessment faces significant implementation barriers. These results align with Strategic Leadership Theory ([Finkelstein et al., 2009](#)), which emphasises that effective leaders influence organisational outcomes through vision-setting, policy development, and long-term strategic planning.

This study contributes to the growing body of research on cybersecurity governance and leadership in risk management by highlighting the essential role of strategic leadership in ensuring cybersecurity resilience. The findings provide valuable insights for policy makers, cybersecurity professionals, and organisational leaders in organisations. While this study provides valuable insights, it has limitations due to a limited sample size. The study focuses on ten experts, which may not fully represent all sectors of organisations. Future research could expand on these insights by exploring the role of leadership commitment in event-based cybersecurity risk assessment in different sectors of organisations, with a larger sample size.

## Ethics Approval and Consent to Participate

The researchers adhered to the ethical guidelines established by the International Islamic University Malaysia (IIUM) Research Ethics Committee (IREC). All procedures involving human participants were conducted in accordance with the ethical standards of the institutional research committee.

Informed consent was obtained from all participants prior to their involvement in the study. Each participant was provided with a clear and comprehensive explanation of the study's objectives, procedures, potential risks, and their rights as participants. Participation was strictly voluntary, and written consent was obtained to confirm their agreement.

To uphold ethical integrity, all data collected during the study were treated with strict confidentiality, and participant anonymity was maintained throughout. No personal identifiers were disclosed at any stage of the research process. This aligns with the ethical principle of confidentiality, which obliges researchers to safeguard the privacy and identity of all participants (Nifakos et al., 2021). The researchers ensured that ethical considerations remained central to the study's design, data collection, and reporting processes.

## Acknowledgement

We greatly appreciate the Public Service Department of Malaysia for sponsoring this study.

## Funding

The Ministry of Higher Education Malaysia supported this work under the Fundamental Research Grant Scheme - Early Career (FRGS/1/2024/ICT07/UIAM/02/1). The authors would like to express their sincere gratitude for the financial support for the project entitled "A Framework on Cyber Resilience for Malaysian SMEs Using Event-Based Risk Management Approach". The support has been instrumental in facilitating the successful completion of this research.

## Conflict of Interest

The authors declare no conflicts of interest for this work and declare that there is no potential conflict of interest with respect to the research, authorship, or publication of this article.

## References

- Abdul Molok, N. N., Chang, S., & Ahmad, A. (2013). Disclosure of Organizational Information on Social Media: Perspectives from Security Managers. *Pacific Asia Conference on Information Systems (PACIS)*. <http://aisel.aisnet.org/pacis2013/108>
- Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity Awareness and Education Programs: A Review of Employee Engagement and Accountability. *Computer Science & IT Research Journal*, 5(1), 100–119. <https://doi.org/10.51594/csitrj.v5i1.708>



- Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, 71(8), 939–953. <https://doi.org/10.1002/asi.24311>
- Aksoy, C. (2024). Building a Cyber Security Culture for Resilient Organizations Against Cyber Attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, 7(1), 96–110. <https://doi.org/10.33416/baybem.1374001>
- Al-Hawamleh, A. M. (2024). Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA. *Digital Policy, Regulation and Governance*, 26(3), 317–336. <https://doi.org/10.1108/DPRG-11-2023-0168>
- Al-Kumaim, N. H., & Alshamsi, S. K. (2023). Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership. *Applied Sciences*, 13(10), 5839. <https://doi.org/10.3390/app13105839>
- Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, 19(2), 134–153. <https://doi.org/10.30574/gjeta.2024.19.2.0084>
- Braun, V., & Clarke, V. (2022). *Thematic Analysis - A practical guide*. SAGE publications.
- Chen, J., Zhu, Q., & Başar, T. (2021). Dynamic Contract Design for Systemic Cyber Risk Management of Interdependent Enterprise Networks. *Dynamic Games and Applications*, 11(2), 294–325. <https://doi.org/10.1007/s13235-020-00363-y>
- Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. (4th Edition). SAGE Publication.
- Döringer, S. (2021). 'The problem-centred expert interview'. Combining qualitative interviewing approaches for investigating implicit expert knowledge. *International Journal of Social Research Methodology*, 24(3), 265–278.
- Elmarady, A. A., & Rahouma, K. (2021). *Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment*. IEEE Access, 9, 143997–144016. <https://doi.org/10.1109/ACCESS.2021.3121230>
- Etikan, I. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1. <https://doi.org/10.11648/j.ajtas.20160501.11>
- Finkelstein, S., Hambrick, D. C., & Cannella, A. A. (2009). *Strategic leadership: Theory and research on executives, top management teams, and boards*. Oxford University Press.
- Fujs, D., Mihelič, A., & Vrhovec, S. L. R. (2019, August 26). The power of interpretation: Qualitative methods in cybersecurity research. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3339252.3341479>
- Goli, D., Al-Mohannadi, H., & Shah, M. (2023). Plan, Prepare and Respond: A Holistic Cyber Security Risk Management Platform. *2023 10th International Conference on Future Internet of Things and Cloud (FiCloud)*, 367–374. <https://doi.org/10.1109/FiCloud58648.2023.00060>
- He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, 21(2), 203–213. <https://doi.org/10.1108/JIC-05-2019-0112>
- International Organization for Standardization (ISO). (2022). *ISO/IEC 27005: Information Security, Cybersecurity and Privacy Protection - Guidance on Managing Information Security Risks*. International Organization for Standardization (ISO). <https://www.iso.org/standard/80585.html>

- International Organization for Standardization (ISO). (2020). *ISO/IEC TS 27100: Information Technology — Cybersecurity — Overview and Concepts*. International Organization for Standardization (ISO). <https://www.iso.org/standard/72434.html>
- Khaw, T. Y., Amran, A., & Teoh, A. P. (2024). Building a thematic framework of cybersecurity: a systematic literature review approach. *Journal of Systems and Information Technology*, 26(2), 234–256. <https://doi.org/10.1108/JSIT-07-2023-0132>
- Krishtanosov, V. B., & Brovko, N. A. (2023). Conceptual-Analytical Approaches to Threats in the Digital Economy. *AlterEconomics*, 20(1), 216–245. <https://doi.org/10.31063/AlterEconomics/2023.20-1.11>
- Lau, P., Wang, L., Liu, Z., Wei, W., & Ten, C.-W. (2021). A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability. *IEEE Transactions on Power Systems*, 36(6), 5512–5524. <https://doi.org/10.1109/TPWRS.2021.3078730>
- Layapan, M., Esa, Mohd. S., & Ationg, R. (2022). The Significance of Leadership Ethics in Youth Voluntary Organization Development in Malaysia. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, 7(6), e001556. <https://doi.org/10.47405/mjssh.v7i6.1556>
- Matthew B., M., A. Michael, H., & Johnny, S. (2018). *Qualitative Data Analysis: A Methods Sourcebook* (4th Edition). SAGE Publications.
- Mumtaz Awan, T., & Riaz Pitafi, Z. (2024). Perspective Chapter: Cybersecurity and Risk Management—New Frontiers in Corporate Governance. In *Corporate Governance - Evolving Practices and Emerging Challenges [Working Title]*. IntechOpen. <https://doi.org/10.5772/intechopen.1005153>
- Muna, A. N. (2022). Examining The Importance of Leadership Skills in Today's Life. *International Journal of Social Service and Research*, 2(10), 977–982. <https://doi.org/10.46799/ijssr.v2i10.185>
- National Cybersecurity Agency of Malaysia (NACSA). (2020). *Malaysia Cyber Security Strategy 2020-2024*. <https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf>
- Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information & Computer Security*, 32(1), 38–52. <https://doi.org/10.1108/ICS-05-2023-0084>
- Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, 21(15), 5119. <https://doi.org/10.3390/s21155119>
- National Institute of Standards and Technology (NIST). (2012). NIST SP 800-30: Guide for Conducting Risk Assessments. *U.S. Department of Commerce*. <https://doi.org/10.6028/NIST.SP.800-30r1>
- National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework (CSF) 2.0. *U.S. Department of Commerce*. <https://doi.org/https://doi.org/10.6028/NIST.CSWP.29>
- Nurwanah, A. (2024). Cybersecurity in Accounting Information Systems: Challenges and Solutions. *Advances in Applied Accounting Research*, 2(3), 157–168. <https://doi.org/10.60079/aaar.v2i3.336>
- Safitra, M. F., Lubis, M., & Fakhurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, 15(18), 13369. <https://doi.org/10.3390/su151813369>

- Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*, 20(4), 581–597. <https://doi.org/10.1108/JIC-03-2019-0041>
- Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974. <https://doi.org/10.1016/j.cose.2022.102974>
- Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*, 43(10), 2082–2098. <https://doi.org/10.1111/risa.14092>
- Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*, 2(3), 573–586. <https://doi.org/10.3390/jcp2030029>
- Ujah, O., Duru, M., & Akinola, S. (2024). Cybersecurity Strategic Plan Part 2. *International Journal of Latest Technology in Engineering Management & Applied Science*, 13(7), 197–207. <https://doi.org/10.51583/IJLTEMAS.2024.130724>