EFFECT OF INFORMATION SECURITY SYSTEMS ON COMPETITIVE ADVANTAGE IN PRIVATE FIRMS IN KENYA

MIKE KAMAU (149018)

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT FOR THE AWARD OF THE DEGREE, MASTER OF BUSINESS ADMINISTRATION OF STRATHMORE UNIVERSITY.

STRATHMORE BUSINESS SCHOOL

STRATHMORE UNIVERSITY

NAIROBI, KENYA

December 2024

DECLARATION

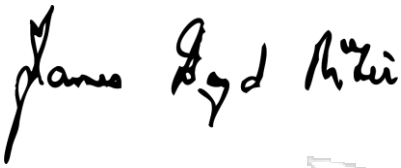
I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the thesis itself.

STUDENT NAME: Mike Kamau **REG NO:** 149018

07/05/2025

Sign: _____ Date: _____

APPROVAL



7 May 2025

Lecturer, Strathmore University Business School,

Strathmore University.

ABSTRACT

This study evaluated the effect of information security systems on competitive advantage in private firms in Kenya. Although studies emphasise that organisations should adopt holistic information security management standards (ISMSs), such as ISO/IEC 27001, a concern remains that there is a lack of empirical inquiry on how these systems contribute to a private firm's competitive advantage. Considering the dearth of studies on the association between these two in Kenya, this study assessed the influence of information security systems on competitive advantage in private firms in Kenya. The study was anchored on the dynamic capability theory and the Information Security Policy Framework. To attain the study's aim and objectives, the positivism philosophy was adopted. This study also adopted the descriptive research design where quantitative research methods were used to collect and analyse data. The target population comprised all private sector firms in Kenya. Further, 247 questionnaires out of a target sample of 400 were returned from the online survey. Inferential and descriptive analysis were employed to address the research objectives. Findings indicate that deterrence mechanism has a positive significant effect on the competitive advantage of private firms in Kenya. This is by building a security-conscious culture and operational resilience in private organisations in Kenya, increasing stakeholder confidence in the process. Visible disincentives, proactive policies, and continuous training directly support the Dynamic Capability Theory's emphasis on adaptability. However, defence and detection have non-significant results. This suggests that other dimensions not addressed in this study could explain this association. The inclusion of firm size and firm age as control variables has no significant effect on the interaction between Information Security Systems (ISSs) and competitive advantage in private firms in Kenya. These findings challenge the assumption that older or larger firms potentially leverage ISSs differently to their advantage possibly because of their established market positions or greater resources. This study recommends that private firms and other ICT stakeholders in Kenya should enhance regulatory standards for deterrence-oriented ISSs. It also recommends that private firms should embed security awareness in organisational culture. Finally, the management of private firms in Kenya should balance ISS components while emphasising strategic deterrence.

Keywords: Information security, information security system, competitive advantage, dynamic capabilities, and information security management system.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
ICT	Information and Communications Technology
ISMS	Information Security Management System
ISO	International Organisation for Standardization
ISS	Information Security Systems
PAM	Process Assessment Model
SMEs	Small and Medium Enterprises

ACKNOWLEDGEMENTS

I express my sincere gratitude to my supervisor for all of the help and support during this challenging research journey. I would also like to thank my family and friends for their unmeasured support towards working on this dissertation. Finally, I would like to express my gratitude to my Strathmore Business School community for providing the impetus and creating a cooperative atmosphere that enabled this investigation.

DEDICATION

I dedicate this thesis to my family, whose unfailing support and understanding have helped me persevere through the difficulties of this academic pursuit. My appreciation goes to my mentors and colleagues. Their encouragement and wisdom have greatly influenced the direction that this project has taken. Lastly, the ISMS community in Kenya, your dedication to information security excellence served as a source of inspiration and motivation for the research that went into this thesis.

CHAPTER ONE

INTRODUCTION TO THE STUDY

1.1 Background

In today's dynamic business landscape, private enterprises wanting long-term success must prioritise gaining a competitive advantage. According to Farida and Setiawan (2022), private organisations should possess two attributes to claim to have a competitive advantage. First, they must generate returns that exceed the cost of capital. Second, these organisations must earn economic returns that are higher than the average returns of their peers. Traditionally, rivalry among organisations was addressed by examining how fierce peers compete against one another along dimensions such as product promotion, price, services, advertising, and new product introductions. In nearly every industry, the firm that was able to tacitly coordinate these areas improved its collective economic profit (Farida and Setiawan, 2022).

However, Naanani (2021) indicates that, with the arrival of the Fourth Industrial Revolution (Industry 4.0), which is marked by the extensive integration of digital technology, a new dimension has developed: that of how better a firm can protect its information and cyber-physical assets through data privacy measures, robust cybersecurity protocols, information security, and resilience to cyber threats (Naanani, 2021). As organisations rely more on digital infrastructure and data-driven processes, defending information threats has become critical to sustaining a competitive advantage (Fast et al., 2023).

Kenya, being one of Africa's leading technologically advanced economies and a magnet for innovation and entrepreneurship (Haqqi, 2023), provided a unique setting for studying the relationship between information security and competitive dynamics. Kenya is experiencing rapid digitisation and increased reliance on digital infrastructure (Mwaura, 2024). This means that Kenyan private enterprises confront both opportunities and challenges in exploiting information security systems to achieve a competitive advantage and maintain long-term success (Communication Authority of Kenya, 2023).

From a theoretical perspective, the study of Information Security Systems (ISS) and competitive advantage draws on a variety of disciplines (Da Veiga et al., 2020). This includes strategic management, information technology, and cybersecurity. Theoretical frameworks such as Information Security Policy Framework and dynamic capabilities theory offer useful insights into how private organisations in Kenya might strategically employ Information

Security System to gain and maintain competitive advantage. Against this backdrop, this research explored the influence of Information Security Systems on competitive advantage within private firms in Kenya. This was to shed light on how effective information security measures contribute to outperforming industry peers. This is in addition to fostering long-term sustainability in the dynamic Kenyan business landscape.

1.1.1 Information Security Systems

The goal of information security systems is to safeguard the Confidentiality, Integrity, and Availability (CIA) of information assets through a variety of technologies, procedures, and practices (Unigwe, 2022). These systems provide the cornerstone of an organisation's resilience against evolving cyberthreats and vulnerabilities. ISO/IEC 27001 is a globally recognised benchmark for creating, implementing, maintaining, and continually improving an information security management system, according to Hamdani et al. (2021), one of the major frameworks and standards utilised in contemporary information security practices. The NIST Cybersecurity Framework offers a comprehensive approach to risk management in addition to ISO/IEC 27001 (Hamdani et al., 2021). Enterprise IT governance and management can also be approached methodically with the help of Control Objectives for Information and Related Technologies. Enterprises handling sensitive payment card data must adhere to the Payment Card Industry Data Security Standard. What's more, the Information Technology Infrastructure Library provides a set of best practices for managing IT services, including information security considerations for support and service delivery. Lastly, a prioritised list of cyber defence measures is provided by the Center for Internet Security's Controls (Wanyonyi, 2020; Winarno et al., 2020). These standards and recommendations, when taken as a whole, offer an all-encompassing approach to information security. In an increasingly linked digital world, they help organisations to proactively manage risks, safeguard critical assets, and maintain stakeholder trust and confidence.

There are three basic assumptions of an information security system. According to Rhodes-Ousley (2013), the first assumption is that an organisation wants to protect its assets. Second, there are threats to an organisation's assets. Finally, the organisation wants to mitigate these threats. As such, three dimensions of information security can be applied to an organisation. These three include defence, detection, and deterrence, also referred to as the three Ds of information security. Defence is conceptualised as measures implemented by an organisation to minimise the probability of a successful security compromise to valuable information assets.

The successful deployment of defence lowers the risk of incidents while saving on incident-related costs (Rhodes-Ousley, 2013). Defensive controls range from firewalls, web content filtering, network access control, change control processes, spam and malware filtering, and web content filtering. These controls offer protection from attack scripts, software vulnerabilities, ethical violations, policy violations, bugs, and accidental damage to data. Alanezi and Brooks (2014) operationalise defence using firewalls, procedures, physical obstacles, and authentication devices.

Detection is conceptualised as an Information Security System's ability to track data access, thereby detecting inappropriate or unauthorised access attempts (Cohen, Freilich, & Siboni, 2017; Rhodes-Ousley, 2013). The early warning of impending attacks is crucial to the security of information systems. Besides, prevention of security incidents is only possible if an organisation has sufficient early warning (Cohen et al., 2017). Detective controls range from motion sensors, video surveillance cameras, alarm systems used to detect violations of a security perimeter, network controls such as audit trails and log files, dashboards, system and network intrusion detection prevention systems, and reports, to Security Information and Event Management (SIEM) alerts. Alanezi and Brooks (2014) operationalise detection using security breach detection, internal system control, and audit trail.

Deterrence is conceptualised by Alanezi and Brooks (2014) as methods employed by an organisation aimed at affecting an adversary's behaviour, deterring them from engaging in undesirable information system activities. Deterrence is an effective way to reduce security compromises and associated losses. Globally, organisations often use deterrent measures, such as disciplinary action and termination, to discourage employees from violating policies (Kosutic, 2021). Deterrent controls include communicating acceptable usage and security policies to employees, requiring employee signatures on agreements to ensure compliance with security policies, providing training, and monitoring web browsing behaviour. Deterrence is operationalised by Alanezi and Brooks (2014) using disincentives, policies, awareness, training, and physical security.

Based on dynamic capacity theory, which states that businesses should constantly adapt and innovate to maintain a competitive edge, ISS serves as a foundation for developing dynamic capabilities within private firms (Goel et al., 2023, Lee & Yoo, 2019). By investing in comprehensive ISS, Kenyan private enterprises can improve their ability to predict and respond to the growing cyber threat scenario. This can boost operational resilience and agility.

Organisations that adopt ISS can build a proactive risk management strategy. They can successfully reduce possible security breaches and minimise disruptions to their business processes. Additionally, ISS allow organisations to use emerging technology and best practices in information security. This helps in increasing their ability to innovate and differentiate themselves in the market. Establishing a culture of security awareness and knowledge sharing through ISS enables organisations to leverage new possibilities and stay ahead of the competition (Goel et al., 2023, Lee & Yoo, 2019).

There was a significant opportunity to objectively investigate the relationship between ISS and competitive advantage in the context of Kenyan private organisations. Despite the rising understanding of the relevance of ISS in protecting organisational assets and minimising cyber threats, limited research has been performed to investigate how ISS, through its defence, deterrence, and detection dimensions, translate into an actual competitive edge for private organisations in Kenya (Wanyonyi, 2020). Given the increasingly digitised business world and the increased frequency of cyber risks, understanding the influence of ISS on competitive advantage is critical for organisations attempting to negotiate the complexity of the modern marketplace (Breda and Kiss, 2020). By exploring this link, this study has filled a significant gap in the existing literature and provided actionable insights for Kenyan private organisations wishing to use ISS to acquire a competitive advantage.

More importantly, the choice of defence, detection, and deterrence was driven by the research's strategic emphasis on how private firms in Kenya employ ISS proactively to gain competitive advantage. While models like the NIST framework- which comprises dimensions such as identify, protect, detect, respond, and recover, it is broader and more operational in scope for assessing cybersecurity risk management. This makes it a sorely a reactive risk management tool often aimed at driving resilience and compliance. In contrast, the defence, detection, and deterrence were deliberately selected as they capture the dynamic firm level strategies directly aligned with pre-empting threats (defence), promptly identifying incidents (detection), and shaping adversary behaviour (deterrence). All these clearly translate into firm level strategic capabilities. Private firms can leverage these capabilities for minimisation of disruptions, differentiation, and building trust and confidence in digital business environments. More importantly, defence, detection, and deterrence resonate with the dynamic capabilities theory. This is because they reflect a private firm's ability to continuously sense, seize, and transform in the wake of cyber threats. As such, these capacities are crucial for agility and innovation in a volatility, uncertainty, complexity, and ambiguity environment that private firms in Kenya.

Lastly, defence, detection, and deterrence are actionable dimensions of ISS that private entities in Kenya can intentionally shape, measure, and optimise to create an edge over rivals.

The scope of information security in this study extends beyond systems. It covers policies, standards, people, and technologies. The study paradigm, based on the dimensions of defence, detection, and deterrence, captures the breadth of information security as a socio-technical system. Defence accounts for the technological and procedural safeguards embedded in systems. On the other hand, detection bridges both technological and human capabilities to monitor and respond to ISS threats. The deterrence pillar takes into account policies, norms, and people's roles, notably in establishing security culture and compliance behaviour. This holistic approach reflects the study's alignment with dynamic capabilities theory.

1.1.2 Competitive Advantage in the Organisational Context

Abbasi et al. (2022) indicate that in the age of Industry 4.0, organisations increasingly face the challenge of creating a competitive advantage. Deszczyński and Deszczyński (2021) conceptualise competitive advantage as a company's above-average manifested exploitation of existing opportunities in the market while neutralising competitive threats. Organisations that deliberately identify unique resources and competencies in their environment, deploy them and protect what is wanted, scarce, and valued by the market can achieve a competitive edge over others (Farida & Setiawan, 2022). Bal and Erkan (2019) note that the complex operational environment organisations find themselves in during the fourth industrial revolution is shrinking the margin of competitiveness. This is considering the central role that information technology and data are taking in combination with smart networked systems, knowledge management, and engineering in the value chain of different organisations (Szymańska, 2020). For enterprises to remain competitive in the fast-paced world of the fourth industrial revolution, they should strategically navigate and leverage these technological breakthroughs.

Kosutic and Pigni (2022) indicate that, globally, upper organisational executives view information security as one of their top priorities, and this is reflected in the steady growth in investment in cybersecurity and budgetary allocations towards the protection of most valuable systems and data from cyberattacks. It transpires that some of the top executives consider cybersecurity investment as strategic and capable of generating higher business value and a competitive edge (Lee, 2021). Research indicates that it is possible to create a long-term competitive advantage from satisfactory information security management, and this is through developing a distinct set of competencies that are harder for rivals to imitate originating from

cybersecurity dynamic capabilities (De Arroyabe et al., 2023; Kosutic & Pigni, 2022; Xu, 2019).

Lee and Yoo (2019) conceptualise cybersecurity dynamic capability as an organisation's combined abilities and processes to implement information security strategies and create new value in a rapidly changing environment, using both internal and external resources. Cybersecurity dynamic capability anticipates prospective technological changes and adapts through new techniques to remain competitive in a changing business context (Goel et al., 2023, Lee & Yoo, 2019). It enables businesses to detect information security opportunities and risks, explore new information and skills, and seek market opportunities proactively (Goel et al., 2023, Lee & Yoo, 2019).

In the era of Industry 4.0, ISS transcend their protective function to become strategic assets that actively shape organisations' competitive edge. This is by reducing threat exposure, enhancing resilience, and building stakeholder trust. According to literature, these are core to sustaining organisational competitiveness (Farida & Setiawan, 2022; Naanani, 2021; Fast et al., 2023). Through dynamic capabilities embedded in ISS- such as defence, detection, and deterrence- private firms can mitigate costly incidents. They can also maintain continuity while signal institutional integrity to stakeholders (Rhodes-Ousley, 2013; Alanezi & Brooks, 2014; Kosutic, 2021). Essentially, this can enhance customer and investor confidence. Kenya's high-risk digitised environments- where cyber exposure escalates alongside innovation (Mwaura, 2024; Haqqi, 2023), effective ISS not only defend assets but serve as differentiators that are difficult to replicate (Goel et al., 2023; Lee & Yoo, 2019; De Arroyabe et al., 2023). They collectively generate sustained competitive advantages for organisations that employ them. Additionally, this positioning aligns cybersecurity investments with value creation. It turns ISS into a dynamic, value-based capability that enables strategic adaptability. It also extends to strategic innovation and stakeholder assurance (Kosutic & Pigni, 2022; Lee, 2021).

1.1.3 Private Firms in Kenya

As per the Kenya Institute for Public Policy Research and Analysis (KIPPRA, 2020), private firms in Kenya are defined as those entities operating within the private sector. Kenya's private sector is well-developed and substantial compared to sub-Saharan and regional standards. This has allowed private firms to contribute significantly to the country's economy. Private firms' health directly impacts the economy's health and the advantages it provides to citizens directly through employment and indirectly through the contribution to the GDP. While the number of

private organisations in Kenya continues to grow, this growth remains below the private sector's full potential. Infrastructure, regulatory, security, and political issues are hurdles that these firms continue to face. Kenya's private firms fall under a thriving and productive formal sector and a vast informal small business sector that employs nearly 90% (KIPPRA, 2020).

According to the Kenya Private Sector Alliance (KEPSA) (2023), private firms in Kenya are present in primary, secondary, and tertiary activities. Interestingly, Kenya has a particularly strong tertiary sector for a developing country. The private sector firms contribute more than 80% of the overall GDP through agriculture, manufacturing, trade, tourism, transportation, communication, and financial services. Trade, transportation, information and communications technology (ICT), and financial services are key drivers of private sector growth (KEPSA, 2023).

Despite the considerable contributions of private enterprises to Kenya's economy, these entities must build competitive advantages to fully achieve their potential and prosper in an increasingly competitive global environment. The well-developed nature of Kenya's private sector, together with its significant contribution to the country's GDP, emphasises the role of private enterprises in promoting innovation, productivity, and efficiency across many sectors (KEPSA, 2023; KIPPRA, 2020). Private companies must prioritise the development of competitive advantages that allow them to distinguish themselves from competitors. This is besides improving operational efficiency and capitalising on market opportunities. Creating competitive advantages increases the resilience and sustainability of individual enterprises (Aidara et al., 2021). It also helps the general health and vibrancy of Kenya's private sector. This is crucial in promoting greater economic growth and social welfare.

Private firms were chosen as the focus of this study because they are central to Kenya's economic engine (KEPSA, 2023; KIPPRA, 2020). These firms operate across all sectors-agriculture, manufacturing, trade, tourism, transport, ICT, and financial services. They also include a wide spectrum of sizes, from start-ups and SMEs to large corporations. In today's increasingly digitised and competitive business environment, private firms face mounting pressure to secure their operations while also innovating to stay ahead (Šikman et al., 2019). ISS are no longer just protective tools. As such, they are strategic enablers of trust, efficiency, and differentiation in the marketplace (Mirtsch et al., 2020). Thus, investigating how ISS contributes to competitive advantage within this private firms was both timely and economically relevant.

The scope of private firms in this study was deliberately broad to reflect the diversity of Kenya's private sector. Using a representative sample of 400 enterprises chosen at random from a projected population of 1,000,000 (KEPSA, 2024), the study captured firms of diverse sizes, sectors, and geographic locations in Kenya. This inclusion meant that the findings were applicable across the private sector. The study acknowledges the increasing pressure firms in the private sector are under to maintain competitive advantage in a rapidly digitising market. This is in line with Kosutic's (2021) assertion that ISS represent a strategic investment key to bolster a firm's operational resilience, stakeholder trust, and innovation. The sampling approach ensured inclusivity and generalisability. This was key to making the findings relevant across the private sector and providing practical recommendations for Kenyan private firms looking to leverage ISS for competitive advantage.

1.2 Problem Statement

Murphy (2022) holds that an organisation will derive a competitive advantage from an ISS if it implements it with variation such that it obviates industry-wide homogeneity. ISS gives firms a competitive edge since they may customise their Information Security Management Systems to meet specific requirements. Organisations can maintain a sustainable competitive advantage by proactively navigating changing environments and meeting requirements using agility, strategic alignment, and operational efficiency (Murphy, 2022).

Studies by Šikman et al. (2019) (global), Kosutic (2021) (global), and Saeidi et al. (2019) (Iran) highlight the significance of ISS implementation in enhancing strategic value in organisations. Although these studies emphasise that organisations should adopt holistic ISS, a concern remains that there is a lack of empirical inquiry on the relationship between Information Security Systems and competitive advantage (Mirtsch et al., 2020; Mirtsch et al., 2021; Mirtsch, Pohlisch, & Blind, 2020). While studies by Alanezi and Brooks (2014) (Saudi Arabia), Cohen et al. (2017) (global), Kakucha and Buya (2018) (global), Safa et al. (2019), and Gundu and Modiba (2020) (South Africa) offer insights into specific aspects of ISS management and its implications for security and innovation, there is a lack of comprehensive research examining the direct link between ISS and competitive advantage in the Kenyan context. Geographical confinement is a restriction in some studies. More importantly, most of the studies conducted on ISS are either qualitative or based on a systematic review. According to Nickels et al. (2024), in the digital economy, information/knowledge is now the fifth critical resource for production, alongside land, labour, capital, and entrepreneurship. As firms invest

heavily in ISS to protect this vital asset, the strategic return on these investments remains under-examined.

Investigating the ISS- competitive advantage link in Kenyan private firms is critical because this sector operates in a uniquely digitised yet under-researched environment (Wanyonyi, 2020). Similarly, the environment is marked by rapid innovation, informal structures, and regulatory gaps. Unlike public entities, private firms often lack mandated cybersecurity frameworks (Mirtsch et al., 2020; Saeidi et al., 2019). It forces them to strategically tailor ISS to mitigate rising cyber threats. This is while unlocking agility, operational resilience, and stakeholder trust and confidence, core enablers of developing competitive edge. Further, a Kenyan context captured the dynamics of a fast-emerging digital economy in the Global South (Maleh et al., 2022; Murphy, 2022; Wanyonyi, 2020). It offers empirical insights beyond the commonly studied Global North (Murphy, 2022; Šikman et al., 2019). This justified a context-specific, quantitative inquiry that moved past generic reviews and untested assumptions to reveal actionable, locally relevant ISS strategies that drive sustainable advantage in high-velocity markets such as Kenya (Maleh et al., 2022; Murphy, 2022).

1.3 Research Objectives

The general objective for this study was to establish the effects of Information Security Systems on competitive advantage in private firms in Kenya.

1.3.1 Specific Research Objective

I. To assess the influence of Information Security Systems on competitive advantage in private firms in Kenya.
II. To assess the influence of defence, detection, and deterrence on competitive advantage in private firms in Kenya.
III. To assess the controlling effect of firm size and firm age on the influence of information security systems on competitive advantage in private firms in Kenya.

1.4 Research Questions

I. What is the influence of Information Security Systems on competitive advantage in private firms in Kenya?
II. What is the controlling effect of firm size and firm age on the influence of information security systems on competitive advantage in private firms in Kenya?

1.5 Scope of the Study

The concluded research quantitatively investigated the effects of Information Security Systems on competitive advantage in private firms in Kenya. The study population were 1,000,000 (KEPSA, 2024) private organisations operating in various sectors and industries in Kenya. This population consisted of organisations of different sizes, ranging from small and medium-sized enterprises (SMEs) to large organisations. The organisations were represented by the senior managers because of their extensive understanding of their ISS and how competitive their firms are.

1.6 Significance of the Study

This study has important implications for practitioners in information security management and strategic decision-making in private firms in Kenya. By examining the influence of Information Security Systems on competitive advantage, practitioners, including IT managers, executives, and business owners, can gain valuable insights into the strategic importance of investing in robust ISS infrastructure. Understanding how ISS effectiveness impacts organisational capabilities and competitive advantage can help in strategic planning. It guides resource allocation and investment decisions, enhancing organisational resilience and competitiveness in the marketplace. Practitioners can leverage the findings of this study to justify investments in ISS implementation and optimisation, prioritise security initiatives, and develop tailored strategies to leverage ISS as a source of competitive advantage within their respective firms.

Moreover, the study contributes to theoretical knowledge in the fields of information security management and strategic management by advancing the understanding of the mechanisms through which ISS influences competitive advantage in private firms. By empirically testing theoretical frameworks and models, the study enhances theoretical insights into the role of ISS in shaping organisational capabilities and competitive positioning. The findings shed light on new theoretical linkages and stimulate further scholarly inquiry into the strategic implications of ISS for firm performance and competitiveness. Moreover, by bridging the gap between theory and practice, the study facilitates the application of theoretical insights to real-world contexts, fostering knowledge transfer and informing evidence-based decision-making among scholars and practitioners alike.

Private firms in Kenya stand to benefit from the findings of this study by gaining actionable

insights into the strategic value of Information Security Systems. By understanding how ISS can enhance organisational capabilities and competitive advantage, firms can make informed decisions about investments in security infrastructure, technology adoption, and risk management strategies. This knowledge empowers firms to proactively mitigate security risks. It also helps improve operational efficiency and capitalise on opportunities for market differentiation and growth.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter scrutinises existing research to shed light on the relationship between ISS and competitive advantage. This is guided by the research objective outlined in Chapter 1. The chapter begins with a review of theoretical literature. This is followed by the empirical review of academic sources, utilising both Google Scholar and Scopus databases to discover and extract the scholarly materials for scrutiny in this study. The chapter concludes with a gap analysis, a presentation of the conceptual framework, and the operationalisation of the study variables, respectively.

2.2 Theoretical Review

Two theories – Dynamic capability and Information Security Policy Framework- anchored this study. Each of these theories is examined and their relevance to the study is provided.

2.2.1 Dynamic Capability Theory

In recent years, dynamic capacity theory has become one of the most influential theories in strategic management (Tran, Zahra, & Hughes, 2019). According to Nayal, Pandey, and Paul (2022), the resource-based theory's shortcomings led to the development of the dynamic capabilities theory. This stemmed from multiple authors voicing reservations over the resource-based theory's insufficiency in elucidating the strategies employed to attain a competitive edge. This critique arises from the fact that resource-based theory fails to consider the dynamic external business environment. Researchers have developed resource-based theory into what is known as dynamic capability theory in response to these constraints. According to this idea, organisations should continuously assess the business environment and adaptably purchase and deploy resources in accordance with it, rather than depending only on their current resources to gain a competitive edge (Nayal et al., 2022).

This study adopts a working definition advanced by Nayal et al. (2022) that the dynamic capability theory is a strategic management framework that highlights an organisation's continuous revitalisation of processes and operational capacities to adaptively realign resources with the evolving business landscape, aiming to secure a competitive edge. This theory

underscores the significance of integrating, constructing, and adapting internal and external capabilities in response to the dynamic environment, and in the case of this study, with a particular emphasis on effectively managing information security.

The dynamic capability theory provides an important lens for examining the multidimensional environment of private enterprises' ISS and competitiveness in Kenya. The essence of the theory is found in its emphasis on the continuous adaptation and realignment of resources to match the changing business environment - a concept that resonates well with the issues outlined in the study objective. The dynamic capability theory unveils a lens to analyse the effect of ISS on private organisations in Kenya in the realm of competitive advantage. This perspective delves into how the dynamic capability theory's emphasis on adaptability and innovation can illuminate the degree to which private organisations in Kenya can capitalise on continuous improvement in the adoption of ISS to develop a robust information security foundation, enhancing their competitive edge. In this regard, dynamic capability theory reveals a critical dimension through which to dissect the intricate interplay between adaptive resource alignment and continuous improvement and the realisation of a tangible competitive advantage in the unique context of ISS in Kenyan private organisations.

2.2.2 Information Security Policy Framework

The information security policy framework is one of the most frequently used to explain information security systems (Bhaharin et al., 2019). The policy formulation process, often described through frameworks such as Anderson's policy cycle or the stages heuristic model (Jann & Wegrich, 2017; Laswell, 1956), offers a structured lens to understand how information security objectives are translated into actionable ISS policies within organisations (Niemimaa & Niemimaa, 2017). According to Edwards (2024), security policies are strategic tools shape behaviour, enable controls, and align security governance with corporate objectives. However, despite significant investments, organisations often struggle to implement policies that are contextually relevant, measurable, and enforceable (Kamaziwe, 2023). This highlights a governance problem, not just a technical one.

An information systems security policy framework includes goals and priorities for securing information systems, often known as security objectives. The establishment of an information systems security strategy is a key mechanism in IS security management (Rostami et al., 2020). It also gives a thorough review of the tactics and approaches used to achieve these goals. Creating a security strategy is a difficult and critical activity that requires integrating technical

and organisational measures to meet security needs (Bhaharin et al., 2019). This policy should protect not only the components of the information system but also its overall functionality. Although the development and implementation of a security policy is a widely adopted practice and organisations allocate substantial resources to security management endeavours, it is frequently observed that the execution of a security policy often falls short of achieving its intended objectives (Nasirpouri Shadbad & Biros, 2021). The development of a robust security policy can be a highly challenging and intricate endeavour.

The information security policy framework was key for this research as it draws attention to the institutional processes of policy design, implementation, and compliance as integral to the effectiveness of ISS (Bhaharin et al., 2019; Rostami et al., 2020). When private firms align ISS policies with operational agility, their needs, and contextual risks, they increase the likelihood of realizing competitive outcomes (Yoshikuni et al. 2024). This is through enhanced trust, resilience, and reduced disruption (Jann & Wegrich, 2017; Kamaziwe, 2023). Thus, information security policy frameworks, which is grounded in policy formulation models and strategic IS governance literature, served as an explanatory lens to understand how formalised security structures in private firms interact with adaptive capabilities to influence the competitive advantage of these entities.

Further, this study information selected the security policy framework because it emphasises the significant role of developing, implementing, and effectiveness of security policies in safeguarding the information security of organisations. It also outlines the priorities and goals critical to effective security management. This can inform the selection and implementation of ISS critical to protecting valuable assets. Coupled with mitigating security threats, this could lead to an ultimate enhancement of a firm's overall security posture. Protecting organisational assets contributes to competitive advantage.

Overall, this study integrates Dynamic Capability Theory and the Information Security Policy Framework to holistically investigate the relationship between ISS and competitive advantage in private firms in Kenya. Dynamic capability explains how the firms in dynamic markets reconfigure resources to sustain competitiveness (Nayal et al., 2022). These resources including digital assets and human expertise. In parallel, the information security policy framework guides the design and implementation of context-sensitive, governance-driven ISS. Together, they underpin the study's conceptual framework (Yoshikuni et al. 2024). As such, dynamic capabilities enable adaptive resource alignment while policy structures ensure that

security interventions are embedded, strategic, and enforceable. This dual-theoretical anchoring allowed the study to investigate the effect of ISS in competitiveness of private firms in the agile Kenyan market.

2.3 Empirical Review

2.3.1 The Influence of Information Security Systems on Competitive Advantage

Previous research examines the link between successfully implementing an Information Security Management System and competitive advantage. For instance, Šikman, Latinović, and Paspalj (2019) suggest that organisations strive to preserve a competitive advantage by meeting client demands and adapting to changing market conditions. Internal benefits of successfully implementing an ISMS include increased staff knowledge, enhanced operational efficiency, and improved communication, all of which coincide with the concept of dynamic capabilities. These qualities enable businesses to adapt to changing challenges, adopt new information security policies, and foster a culture of continuous improvement (Šikman et al., 2019). As a result, an organisation is better positioned to respond to market changes, improve operational effectiveness, and strengthen its competitive position. However, there are potential research gaps in this area. The focus placed by Šikman et al. (2019) on the connections between competitive advantage, dynamic capacities, and successful ISMS implementation raises the possibility that more research is necessary to clarify the specific strategies and processes businesses use to improve their dynamic capabilities.

Kosutic (2021) looked into the components necessary for cybersecurity deployment and management within an organisation, as well as the influence of cybersecurity on a company's competitive edge. The researcher employed a qualitative approach, interviewing security officials, executives, consultants, and information technology (IT) managers from firms in ten countries. The companies came from diverse industries, including aircraft, bioscience, chemical manufacturing, finance, food processing, information technology, and security. Kosutic (2021) observed that creating certain cybersecurity dynamic capabilities can help businesses achieve strategic value. This value will be difficult for competitors to replicate, granting enterprises a competitive advantage.

Serrado et al. (2020) carried out a systematic review to investigate the efficiency of current information security frameworks in European banks to comply with the General Data Protection Regulation (GDPR). The study discovered increased ISO/IEC 27001 adoption rates

in industries with high information density and regulation. It is crucial to highlight, however, that the study's unique focus on the European banking sector may limit its relevance to industries and geographic regions. As a result, the context of developing countries was captured using this study in Kenya.

In a study that employed systematic review to find out the key success factors of ISS, Arbanas & Žajdela Hrustek, (2019) suggest that organisations strive to preserve a competitive advantage by meeting client demands and adapting to changing market conditions. Internal benefits of successfully implementing ISS include increased staff knowledge, improved operational efficiency, and improved communication, all of which coincide with the concept of dynamic capabilities (Nagata, 2023). These qualities enable businesses to adapt to changing challenges, adopt new information security policies, and foster a culture of continuous improvement. As a result, an organisation is better positioned to respond to market changes, improve operational effectiveness, and strengthen its competitive position (Azeem et al., 2021). However, there are potential research gaps in this area. The connections between competitive advantage, dynamic capacities, and successful information security system implementation raised the possibility that more research was necessary to clarify specific strategies and processes that businesses use to improve their dynamic capabilities (Baptista et al., 2020).

Saeidi et al. (2019) examined the impact of enterprise risk management on competitive advantage in Iran, moderating the relationship with information technology strategy and structure. They used a quantitative survey to gather information from 84 participants. They found that enterprise risk management is a good predictor of a firm's competitive advantage. Furthermore, the study discovered that IT strategy and IT structure have a direct impact on competitive advantage while also mitigating the association between enterprise risk management and competitive advantage. This study provides valuable insights into the methods by which risk management measures help firms maintain their competitiveness. However, there is a significant gap in the literature regarding the specific impact of ISS on competitive advantage in private enterprises in Kenya. This is despite Saeidi et al.'s (2019) focus on enterprise risk management and its relationship to competitive advantage regulated by IT considerations in Iran. By investigating this gap, the research has provided unique perspectives on how ISS practices affect competitive advantage in Kenyan contexts.

Gundu and Modiba (2020) conducted a study in South Africa to advance and validate a model for IS awareness and compliance geared towards building an Ubuntu-inspired competitive

advantage. The study used both primary (quantitative surveys) and secondary data (systematic review). As such, 31 questionnaires were collected from employees of a South African organisation. The study concluded that African information security awareness and compliance initiatives can only be properly addressed if an African employee is viewed as a member of a larger community rather than a solo individual. This is considering that IS threats originate from human elements. Besides, these threats continue to be aggravated by firms investing in technical controls such as firewalls and antiviruses to protect information and cyber assets (Gundu & Modiba, 2020). In line with deterrence, a well-planned information security awareness campaign has the potential to change employees' attitudes regarding security.

Alanezi and Brooks (2014) explored the organisation and management of online fraud prevention mechanisms in Saudi Arabian financial institutions. The study addressed the growing problem of online fraud in an area with high Internet penetration and significant online financial activity. The study, which was conducted through qualitative interviews with specialists in Saudi Arabia, investigated the multidimensional impact of people's perceptions, which are influenced by moral, social, cultural, and religious backgrounds, on awareness and fraud prevention efforts. The findings imply that technology measures alone may not help combat online fraud. Instead, the study calls for a complete approach that incorporates deterrence, defensive, detection, and remediation actions.

On their part, Cohen et al. (2017) developed a conceptual model for dealing with ISS threats based on conventional military strategy principles known as the "four Ds". That is detection, deterrence, defence, and defeat. In a systematic review study, the authors argue that, while cyber threats provide new challenges, they are not fundamentally different from existing asymmetric threats. Their model calls for the development of policies that incorporate defence, deterrence, and detection to improve the security of organisational cyber systems. By using this paradigm, businesses can develop thorough strategies and plans to resist a wide range of cyber threats, whether they come from state-based organisations, non-state groups, or people, creating a dynamic cybersecurity capability in the process.

Kakucha and Buya (2018) investigated the security measures used in financial management systems to promote innovation and obtain a competitive edge. The study recognised the growing complexity of security risks faced by enterprises as a result of internal and external attacks. Using a desktop literature review, the study identified the frequency of large-scale network environments in businesses, including multiple devices and sophisticated access

profiles. The strategies shown to be critical to information security include prevention, deterrent, surveillance, detection, response, deception, perimeter defence, and layering, with a particular emphasis on loss prevention to protect important assets.

Safa et al. (2019) study discussed crucial concerns such as information security breaches and privacy violations. The study emphasised the significance of taking into account both technological and human factors to successfully manage risks. It also emphasised the important role that employees play in creating dangers to information assets, whether purposefully or accidentally. The study presents a novel conceptual framework for mitigating insider risks, with a focus on deterrent and preventative measures. Deterrence factors try to deter personnel from engaging in information security malfeasance, whilst situational crime prevention factors encourage them to avoid such behaviour. The findings show that the certainty and severity of perceived consequences have a considerable impact on individuals' views and dissuade them from engaging in wrongdoing. Further, increased work, risk, and decreasing incentives alter employees' attitudes toward preventing information security misbehaviour. However, while deterrent and preventative measures are critical to ISS, the study by Safa et al. (2019) fails to show how this leads to competitive advantage.

2.4 Research Gap

While the existing literature provides useful insights into information security system adoption and implementation, various research gaps highlighted the need for a targeted study on information security system implementation in Kenyan private enterprises to strengthen their competitive edge. Although the studies mentioned above have investigated adoption incentives such as regulatory compliance and information security enhancement, these variables were not explored in the context of Kenya, calling for a study of this nature. Furthermore, the generalisability of findings from studies focusing on specific sectors or areas, such as the European banking industry, raised issues, emphasising the importance of research specialised in the Kenyan private sector. Addressing these gaps through a focused study in Kenya's private sector has provided tailored insights into the motivations for information security system adoption, ultimately guiding strategies for improving competitive advantage.

Table 2. 1 Research gaps as synthesised from the literature review.

Authors	Country	Purpose	Methodology	Findings	Research Gaps
Alanezi and Brooks (2014)	Saudi Arabia	Investigated the multidimensional impact of people's perceptions, which are influenced by moral, social, cultural, and religious backgrounds, on awareness and fraud prevention efforts.	Qualitative	Technology measures alone may not help combat online fraud.	The conceptual gap in that the study does not explicitly examine the association between ISS and competitive advantage in private firms. There is a contextual gap in that the findings cannot be transferred to Kenya.
Gundu and Modiba (2020)	South Africa	Advance and validate a model for IS awareness and compliance geared towards building a Ubuntu-inspired competitive advantage.	Mixed method	African information security awareness and compliance initiatives can only be properly addressed if an African employee is viewed as a member of a larger community rather than a solo individual.	The conceptual gap in that the study does not explicitly examine the association between ISS and competitive advantage in private firms.
Kosutic (2021)	10 countries globally	Factors required for cybersecurity deployment and management inside an organisation, as well as the impact of cybersecurity on the competitive advantage of a company.	Qualitative	Developing specific cybersecurity dynamic capabilities can help organisations attain strategic value. This value will be difficult for rivals to imitate, helping firms attain a competitive advantage.	Mechanisms underlying relationships between ISS and competitive advantage are not well expounded. There is a lack of quantitative insights into the relationship.
Saeidi et al. (2019)	Iran	Assessed the effect of enterprise risk management on competitive advantage.	Quantitative	Enterprise risk management is a positive predictor of the competitive advantage of firms.	There is a noticeable gap in the literature concerning the precise impact of ISS on competitive advantage in private firms in Kenya.
Serrado et al. (2020)	European banking sector	Explored information security frameworks' efficiency in the European banking sector.	Systematic review.	Discovered increased ISO/IEC 27001 adoption in high-information-density industries.	Limited to the European banking sector.
Šikman et al. (2019)	Not confined to any region	Explore links between ISMS, dynamic capabilities, and competitive advantage	Systematic review and conceptual framework analysis.	ISMS enhances adaptation and competitiveness	Mechanisms underlying relationships are not well expounded. There is a lack of quantitative insights into the relationship.

(Author, 2023)

2.5 Conceptual Framework

According to this study's conceptual framework, the independent variable refers to the measures taken by private enterprises in Kenya to protect their digital assets through Information Security Systems. These systems are identified as the independent variable in the study because they are hypothesised to impact the dependent variable, competitive advantage (Li et al., 2021). In this study, the dependent variable, competitive advantage, refers to the strategic edge gained by private enterprises in Kenya through the effective use of Information Security Systems. Competitive advantage, the focal variable in this study, is influenced by the independent variable, Information Security Systems. The control variables include firms' size and age (Cheah, Leong, and Fernando, 2023).

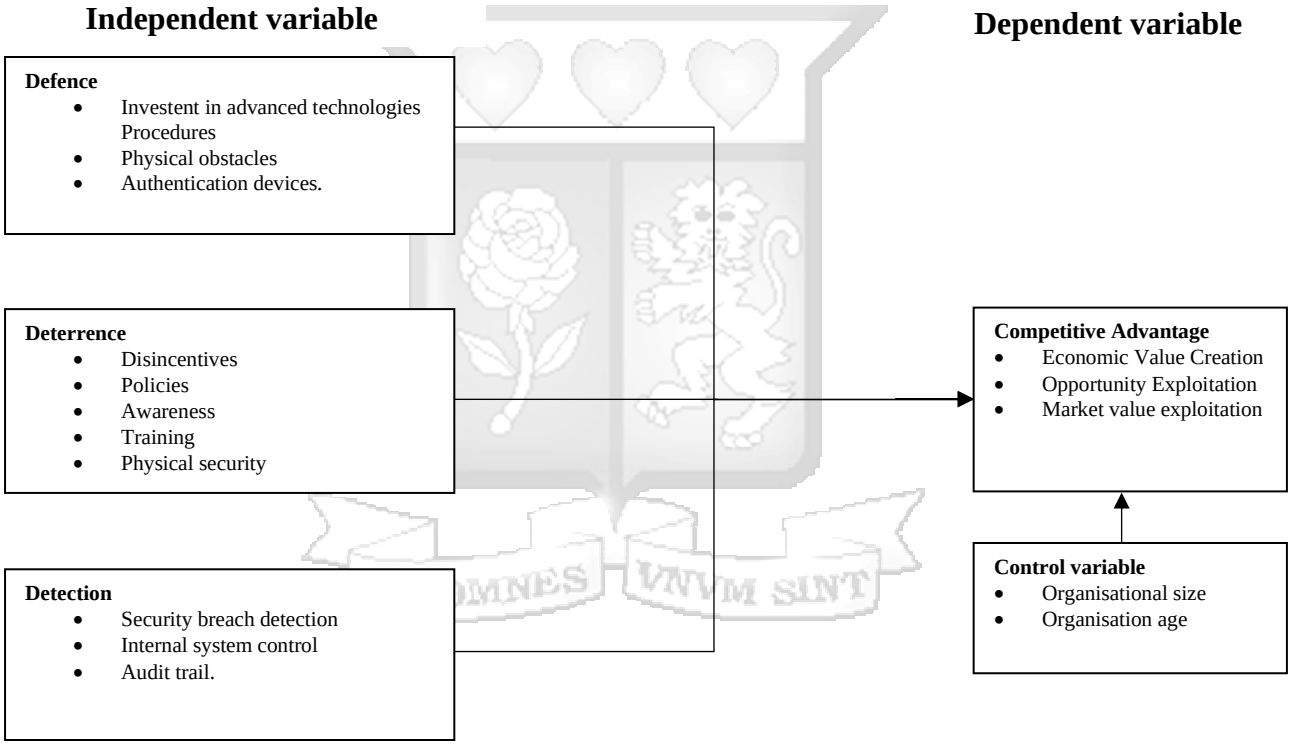


Figure 2. 1 Conceptual framework (Author, 2025).

Table 2. 2 Operationalisation of variables

Variable	Type of Variable	Indicator	Measurement	Data Collection Method	Reference
Defence	Independent	• Level of investment in advanced technologies like firewalls and access control systems • Existence and clarity of procedures for security incidents • Use of defensive controls to mitigate	5-Point Likert scale ordinal	Questionnaire	Alanezi and Brooks (2014); Cohen et al. (2017), Gundu and Modiba (2020) Kakucha and Buya (2018) Safa et al. (2019).

		software vulnerabilities and data damage • Maintenance and update routines to address vulnerabilities			
Deterrence	Independent	• Existence and communication of policies and consequences • Frequency and quality of employee security training and awareness • Monitoring of user activity for compliance • Use of disciplinary actions to enforce policy	5-Point Likert scale ordinal	Questionnaire	Alanezi and Brooks (2014); Cohen et al. (2017), Gundu and Modiba (2020) Kakucha and Buya (2018) Safa et al. (2019).
Detection	Independent	• Use of monitoring tools for detecting suspicious activity • Regular audits and vulnerability scans • Active monitoring of logs/audit trails for unauthorised access • Established incident investigation and response processes	5-Point Likert scale ordinal	Questionnaire	Alanezi and Brooks (2014); Cohen et al. (2017), Gundu and Modiba (2020) Kakucha and Buya (2018) Safa et al. (2019).
Firm characteristics	Control	• Organisation size o Number of employees • Organisation age o Years of existence	Questionnaire	Questionnaire	Cheah, Leong, & Fernando (2023).
Competitive advantage	Dependent	• Ability to create more economic value compared to competitors. • Organisation's above-average exploitation of existing opportunities while neutralising competitive threats. • Protection of what is wanted, scarce, and valued by the market	5-Point Likert scale ordinal	Questionnaire	Saeidi et al. (2019).

(Author, 2025).

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

The current chapter introduces the research methodology employed in this study. To begin with, the chapter outlines the research philosophy that was used to address the research objectives. Further, it provides an overview of the research design, data collection methods, population and sampling, data analysis techniques, research quality, and ethical considerations.

3.2 Research Philosophy

The study adopted a deductive approach which aligns with the positivist philosophy. Positivism is rooted in the belief that the social world operates according to observable laws similar to those found in the natural sciences (Park et al., 2020). Positivists hold an objectivist ontological stance, asserting that there is an objective reality independent of human perception. They also embrace a nomothetic epistemology, seeking to uncover generalisable laws and causal relationships through systematic observation and empirical evidence (Alharahsheh & Pius, 2020). The selection of the deductive approach for this study stems from its alignment with the positivist research philosophy and its appropriateness for addressing the aims of this investigation. The deductive approach involves reaching conclusions derived from existing theories or conceptual frameworks. It starts with the formulation of a theory-based framework, which is then tested using empirical data. Deductive reasoning moves from general principles or theories to specific observations or predictions, following a structured and logical sequence. (Azungah, 2018). The researcher initiated the investigation by utilising established theories that define the connections between variables in this study. Following this, data was gathered and examined to validate or disprove the theoretical assertions.

3.3 The Research Design

The study employed a descriptive research design. Aggarwal and Ranganathan (2019) imply that the descriptive design serves as a research blueprint focused on fact-finding, aiming to describe the current state of the variables being studied, specifically ISS and competitive advantage in private firms in Kenya. Descriptive research was well-suited for analysing and elucidating connections between variables that have not been extensively investigated (Aggarwal & Ranganathan, 2019) as was the case of ISS and competitive advantage in Kenyan private firms.

Further, the methodological framework used in this study was quantitative method. This requires the sole use of quantitative research for both data gathering and analysis. Quantitative methodology involves collecting numerical data and using statistical techniques to examine and interpret the results (Savela, 2018). The utilisation of numerical data helped to get objective findings (Creswell & Creswell, 2018). A variety of factors contributed to the decision to choose a quantitative design. First, it allowed the researcher to investigate the relationship between ISS and competitive advantage in Kenyan private enterprises systematically and objectively. The quantitative method ensured that the data collection instruments were constructed consistently. According to Savela (2018), this uniform strategy improves the replicability of the study's findings. This allowed the researcher to generalises the results to the study population.

3.4 Population and Sampling

The population for the study on the influence of Information Security Systems on competitive advantage in private enterprises in Kenya consisted of private firms operating in Kenya. Each firm functioned as a unit of analysis. Executives or managers in these firms served as units of observation. This was because of their extensive understanding of their ISS and how competitive their firms are. This population included a varied range of enterprises from various industries, sizes, and geographical locations in Kenya. This is to ensure a comprehensive knowledge of the relationship between ISS and competitive advantage in the Kenyan environment.

Based on statistics provided by the Kenya Private Sector Alliance (2024) (KEPSA), which represents private sector associations and corporate bodies throughout all sectors of the economy, including trade associations, KEPSA was projected to have around 1,000,000 members. These members represent a diverse range of private firms, from multinational corporations to small and medium-sized enterprises (SMEs) and start-ups. While this estimate sheds light on the size and diversity of Kenya's private sector, it is crucial to note that KEPSA does not represent all private enterprises in the country. Nonetheless, this data provided a useful approximation for understanding the composition of Kenya's private sector and informed the sampling and generalisation strategies used in this study.

3.4.1 Sampling

Securing an appropriate sample is useful in achieving adequate statistical power for detecting significant associations between variables, while also mitigating the potential errors that may

occur during the analysis stage (Vasileiou et al., 2018). The Slovin formula $n = \frac{N}{1+N(e)^2}$ was utilised to determine the study's sample size. The population was represented by N, the sample size by n, and the sampling error by e. Therefore, $n = \frac{1000000}{1+1000000(0.05)^2}$ resulted in a sample size of 400 respondents.

Further, the sample exhibited sufficient diversity to encompass a wide range of industries, company sizes, and geographical areas within Kenya. With this regard, the simple random sampling technique was employed to select the private firms to participate in the study. One reason for selecting simple random sampling was its ability to allow each private organisation to take part in the study (Saunders et al., 2019). This ensured the generalisability of the findings to the full population of private enterprises in Kenya the sample used is representative of the broader sector. Using a representative sample of private firms in Kenya helped the study extend to a broader range of enterprises that have deployed ISS in their operations.

To ensure diversity and relevance in the study findings, the 400 sampled firms were drawn from various sectors represented by KEPSA. This included agriculture, manufacturing, trade, tourism, transport, ICT, and financial services. Further, the sample included enterprises of different sizes- start-ups, SMEs, and large corporations- capturing a range of operational scales. While specific cities were not detailed, the study ensured regional and sectoral diversity using simple random sampling. Participants included executives and managers knowledgeable in ISS and strategic competitiveness- such as CIOs, IT managers, and business strategists. This respondent profile was selected to ensure informed and enhanced the credibility of the study's results by ensuring the results could be applied to similar settings.

3.5 Data Collection

The study used a cross-sectional survey to collect data. The researcher gathered data at one point in time (Leavy, 2022), enabling the researcher to acquire a momentary representation of the present condition of ISS in private organisations in Kenya and competitive advantage. The cross-sectional survey used a questionnaire to establish connections between the study variables. The study employed an online survey to gather primary data that was utilised to examine the association between the study variables. This approach was deemed appropriate for the study's objective since it allowed the researcher to collect information from respondents via an online questionnaire (Leavy, 2022). This effectively operationalised the study variables. This survey method yielded numerical data, allowing for the use of statistical analytic

techniques to investigate the relationships between ISS and competitive advantage (Leavy, 2022). Further, a survey strategy was effective in minimising bias because the data collected included both inferential and demographic characteristics. This enhanced the findings' generalisability to the larger research population (Saunders et al., 2019).

3.6 Data Analysis

This research relied on both descriptive and inferential analysis. The first section of the questionnaire collected demographic data for the descriptive analysis. This included each respondent's gender, age, and educational level. The inferential data analysis made use of the information gathered from the second part of the questionnaire. Here, questions were led by the research objectives and variables under consideration. After the data was collected, it was evaluated using IBM Statistical Package for the Social Sciences (SPSS), version 29. The regression model $CA = \beta_0 + \beta_1 DF + \beta_2 DT + \beta_3 DTCT + FS + FA + \varepsilon$, was used to carry out the regression analysis.

CA = Competitive advantage.

β_0 = The model intercept.

DF = Defence.

DT = Deterrence.

$DTCT$ = Detection.

FS = Firm size.

FA = Firm age.

ε = the model error term.

Several diagnostic tests were conducted. The first was the normality test to understand which between parametric and non-parametric tests to use. Further, a goodness of fit test and a model fitting test were conducted. The aim is to qualify the ideal regression model for parameter estimation. Further details on the tests are presented in the findings chapter.

3.7 Research Quality

3.7.1 Validity

In this study, validity was ensured through content validity and construct validity (Shrotryia & Dhanda, 2019). For content validity, the researcher developed the questionnaire on the extensive literature review in addition to consulting experts in the field of ISMS at Strathmore University. Content validity ensured that the questions in the questionnaire effectively address the objective set out in Chapter 1.

To enhance the construct validity of the study, the researcher considered a two-fold approach involving expert review and pilot testing. The researcher engaged subject matter experts in ISMS to critically assess the questionnaire. Subsequently, the researcher conducted a pre-test using a sample of 15 respondents, a representative subset of the intended participants (Gani et al., 2020). The aim was to identify issues with the questionnaire such as ambiguous questions or gaps in construct coverage. This iterative process of expert review and pilot testing offered a solid basis for developing the measuring instruments and verifying the study's construct validity.

3.7.2 Reliability

Reliability in research refers to the extent to which a research instrument consistently produces the same results when applied repeatedly (Gani et al., 2020). To ascertain the reliability of the measurement tools, a pilot test was conducted as previously mentioned. To evaluate internal consistency, the investigator analysed the responses collected and assess the extent to which the questions within each construct yielded similar results. Additionally, the test-retest reliability assessment involved administering the questionnaire to 15 respondents on two distinct occasions, allowing for a comparison of responses over time (Gani et al., 2020). The results of the test retest are presented in Table 3.1. Each independent and dependent variable attained a coefficient of more than 0.8. This is in line with Oluwatayo (2012) who holds that, for a measure to guarantee reliability, it should attain a Pearson correlation coefficient of >= 0.80.

Table 3. 1 Test retest reliability

Variable	Coefficient
Defence	0.895
Deterrence	0.871

Detection	0.830
Competitive advantage	0.806

This comprehensive approach aligns with established methodologies and aims to ensure the dependable and consistent nature of the research tools used in the study. When it comes to assessing reliability, incorporating participant engagement strategies becomes essential. The researcher gave participants a sense of direction and significance by giving a summary of the study's objectives and highlighting the value of their participation. This approach not only elucidated the significance of their participation but also inspired them to make substantial contributions towards testing the instrument's reliability.

3.8 Ethical Considerations

This research project followed the ethical principles specified in Strathmore University's code of ethics, ensuring that the study was carried out with integrity and respect for the rights and well-being of all participants. As a first step, the researcher acquired an ethical approval from Strathmore University. This granted the researcher permission to proceed with the study per ethical norms. This approval procedure comprised demonstrating how the research would preserve the privacy of participants, acquire informed consent, and manage any possible risks. Thereafter, the researcher sought approval from the National Commission for Science, Technology, and Innovation to conduct the study in Kenya. This step guaranteed that the research adhered to national regulatory criteria while remaining ethically sound. The researcher strived to respect the dignity and welfare of participants, maintain research transparency and respondent confidentiality and anonymity. This contributed to the credibility of the findings and conclusions drawn therein.

CHAPTER FOUR
DATA ANALYSIS AND PRESENTATION OF FINDINGS

4.1 Introduction

This chapter presents the results guided by the research objectives: to assess the influence of information security systems (defence, deterrence, detection) on competitive advantage in private firms in Kenya and to examine the role of firm characteristics (organisation size and age) in controlling the relationship between each dimension of information security systems and competitive advantage. The chapter begins with an examination of the response rate. This is followed by a presentation of the demographic information, descriptive statistics, and inferential statistics. The inferential statistics are presented under the correlation analysis and multiple regression analysis against each objective.

4.2 Response Rate

The researcher sought a representative response rate to qualify the data for a quantitative analysis. According to Wu et al. (2022), the response rate is one of the yardsticks used by researchers to assess the quality of a survey. Of the 400 questionnaires sent out, 247 were returned, representing 61.75% of the sample. The researcher achieved the response rate through a combination of approaches, from sending follow-up emails to invited respondents, making follow-up phone calls, and talking to contact persons within respondent firms to encourage participation. The 61.75% response rate is within the recommended response rate acceptable for statistical analysis in line with Fincham (2008) who asserts that an online study needs at least 30% for a quantitative analysis to occur. The response rate of 61.75% is also well in line with Wu et al. (2022) who note that 44.1% is the average response rate for online surveys: 61.75% provides adequate data for statistical analysis.

Table 4. 1 Survey response rate

Response	**Frequency**	**Percentage**
Returned	247	61.75
Unreturned	153	38.25
Total Administered	**400**	**100**

(Survey data, 2024).

4.3 Demographic Information

Before conducting the descriptive and inferential analysis, the researcher sought to understand the demographic composition of the study's respondents. To begin with, the researcher examined the gender of the respondents. As indicated in Table 4.2, most of the respondents were male (65.2%) against females (34.8%). The researcher distributed 200 surveys to male respondents and 200 to female respondents. This ensured equal opportunity for participation from both genders. The approach aimed to minimise gender-based sampling bias. This was by providing an equal chance to respond for both male and female leadership in private firms in Kenya. Of the 200 questionnaires distributed to males, 161(80.5%) were returned. On the other hand, 86 (43%) questionnaires were returned from the 200 sent to females. While the response rate was higher for male respondents, this balanced distribution helped mitigate the risk of biased sampling. An independent-samples t-test was conducted to compare responses between male and female participants across four variables (competitive advantage, defence, deterrence, and detection). For competitive advantage, the results indicated a statistically significant difference between males (M = 3.8412, SD = 0.69894) and females (M = 3.6362, SD = 0.71970), with a mean difference of 0.20496, t (245) = 2.173, p = 0.031, and a small effect size (Cohen's d = 0.290). However, for defence, deterrence, and detection, no statistically significant differences were found between males and females. For defence, t (245) = 1.038, p = 0.300; for deterrence, t (245) = 0.410, p = 0.682; and for detection, t(245) = 0.699, p = 0.485. The effect sizes for these variables were very small (Cohen's d ranging from 0.055 to 0.139), suggesting minimal practical differences between male and female responses for defence, deterrence, and detection. Thus, while there is a significant difference for competitive advantage, the practical significance of this difference is relatively small. Similarly, the remaining variables showed no meaningful differences.

Table 4. 2 Respondents' gender

	Frequency	**Percent**
Female	86	34.8
Male	161	65.2
Total	**247**	**100.0**

(Survey data, 2024).

The respondents' educational levels in Table 4.3 indicate a high level of academic accomplishment among managers in Kenyan private firms. The bulk of the 247 participants

(54.3%) have only an undergraduate university degree, a further 33.6% have earned a master's degree, and an additional 2% have earned a doctoral degree. This means that roughly 90% of respondents had at least a university-level education. This implies that higher education is a frequent requirement for leadership positions in private firms in Kenya. Further, a smaller proportion of the sample holds a diploma (8.5%) with an even smaller fraction (1.6%) having only a high school education. This distribution emphasises the importance of formal education among private sector leaders. This may influence how information security systems (ISS) are understood and implemented. The respondents' high educational credentials are likely to influence their understanding and strategic use of ISS to gain a competitive advantage. Besides, this representation implies a well-informed management inside the sampled organisations.

Table 4. 3 Respondents' educational levels

	Number	**Percent**
High School	4	1.6
Diploma	21	8.5
Undergraduate university Degree	134	54.3
Master's Degree	83	33.6
Doctoral Degree	5	2
Total	**247**	**100**

(Survey data, 2024).

The age distribution of the respondents provides insight into the demographic composition of executives and managers in private firms in Kenya. Of the 247 participants, the largest age group were those between 40 and 49 years old, comprising 40.9% of the respondents. Close behind were those aged 30 to 39, who accounted for 39.7% of the respondents. These two age groups accounted for more than 80% of the sample, demonstrating that middle-aged leaders dominate these organisations.

A lower percentage of responders (14.6%) were between the ages of 18 and 29. This shows the existence of younger managers, albeit in smaller numbers. 4.5% of the respondents were between the ages of 50 and 59, with only one (0.4%) older than 60. This distribution indicates that, while there is some representation from younger and older age groups, the majority of leadership roles is held by people in their 30s and 40s. This age variety may indicate varied levels of knowledge and experience with information security systems. Younger managers may be more adaptive and technologically knowledgeable, but older managers may rely more on

established methods, which could influence their attitude to implementing new security technology in private organisations.

Table 4. 4 Respondents' age

	Number	**Percent**
18-29	36	14.6
30-39	98	39.7
40-49	101	40.9
50-59	11	4.4
Over 60	1	.4
Total	**247**	**100.0**

(Survey data, 2024).

The private companies in Kenya in this study exhibit a notable range in firm size distribution, as shown by the number of employees. At 44.1%, businesses with fewer than 50 employees make up the largest group, indicating that small businesses make up a sizable share of the sample. 16.2% of the firms represented had between 50 and 100 employees, while 17% had between 101 and 500 employees. The distribution indicates that small and medium-sized businesses (SMEs) are fairly represented in the sample. According to the Kenya Bankers Association (2021), small businesses in Kenya are defined as those that employ 10 to 49 people, whereas medium-sized businesses employ 50 to 99 people. Further, 8.1% of firms represented in the study had between 501 and 1,000 employees while 14.6% of the firms had more than 1,000 employees. This distribution shows that the respondent firms span a wide variety of sizes. This diversity enables a thorough examination of how information security systems affect competitive advantage at various organisational scales and sheds light on the moderating effect of firm size on this association.

Table 4. 5 Firm size by the number of employees within respondents' firms

	Frequency	**Percent**
Less than 50	109	44.1
50-100	40	16.2
101-500	42	17.0
501-1,000	20	8.1
More than 1,000	36	14.6
Total	**247**	**100**

(Survey data, 2024).

The distribution of firm age, as determined by years of operation in Table 4.6, sheds light on the stability and maturity of the Kenyan private companies that were surveyed. Each of the 247 respondents worked at a different firm, representing 247 firms in Kenya. Out of the 247 firms, 55.5% of firms have been in business for more than ten years. This suggests a stable business environment with experienced enterprises, as there is a substantial representation of well-established firms in the sample. 24.3% of firms have been operational for six to ten years. This suggests that a significant portion of the private businesses represented in the study are beyond their initial startup phase. These firms are in their mid-stage of development characterised by growth and stability. These companies most likely have sufficient experience to have successfully implemented and assessed their information security systems. Further, 20.2% of the firms are those who have been in operation for one to five years. This category consists of young, startup businesses that might be only beginning to get established and hone their competitive strategies, such as having efficient information security systems. It is helpful to understand how the length of operation moderates the effects of information security systems on competitive advantage because this distribution displays a wide range of firm ages. A thorough examination of how a firm's maturity influences its information security procedures and competitive positioning is made possible by the inclusion of both more recent and more established companies.

Table 4. 6 Firms age by years of existence of respondents' firms

	Number	**Percent**
1-5 years	50	20.2
6-10 years	60	24.3
Above 10 years	137	55.5
Total	**247**	**100.0**

(Survey data, 2024).

4.4 Descriptive Analysis

This subsection examines the descriptive statistics of the survey respondents' evaluation of defence, deterrence, detection, and competitive advantage in private sector organisations in Kenya. The analysis computes the averages and standard deviations of each statement. This is to determine the respondents' level of agreement with each statement and the respondents spread around the mean, respectively. Since the average ratings for each variable exceed the midpoint of the Likert scale, it indicates that, on the whole, respondents tend to agree or

strongly agree with the statements related to the effectiveness of defence, deterrence, detection, and competitive advantage in their organisations. Each variable's mean was used to conduct the inferential analysis to address each research objective and question.

4.4.1 Descriptive Analysis of Defence

To address objective one on the influence of information security systems on competitive advantage in private firms in Kenya, the research sought to answer the research question: what is the influence of defence mechanisms on competitive advantage in private firms in Kenya? Each respondent was requested to rate their agreement levels with each statement on information security defence mechanisms. The results of each statement are presented in Table 4.7.

Table 4. 7 Private firm's defence mechanisms descriptive results

Statement	**Mean**	**Std. Dev**
Our organisation prioritizes implementing robust defence mechanisms to protect valuable information assets.	4.23	1.009
We invest in state-of-the-art security technologies, such as firewalls and access control systems, to safeguard our network infrastructure.	4.19	1.086
Our organisation regularly updates and patches software to address vulnerabilities and enhance our defensive capabilities.	4.19	1.004
We have established clear procedures and protocols for handling security incidents to minimize the impact of potential breaches.	4.09	1.040
Our defensive controls are designed to mitigate various threats, including software vulnerabilities, bugs, and accidental data damage.	4.11	.961
Overall Mean	**4.1619**	**.86580**

(Survey data, 2024).

The results in Table 4.7 indicate that private firms prioritised information systems defence mechanisms. The highest-rated statement, with a mean of 4.23 on a five-point scale, demonstrates that the majority of private firms surveyed prioritise building strong defence systems to protect valuable information assets. Similarly, investments in advanced security technology such as firewalls and access control systems are highly valued. This is demonstrated by an average rating of 4.19. Regular software updates and patching, which are critical for resolving vulnerabilities, also received an average of 4.19. Procedures for dealing with security

incidents and defensive controls to mitigate diverse risks both had scores greater than 4. This suggests a comprehensive approach to defence mechanisms. The standard deviations, which range from 0.961 to 1.086, indicate some heterogeneity in responses. However, the scores were generally consistent around the mean. This stability in high means suggests that most private firms in Kenya not only understand the significance of strong defence systems but also actively implement and maintain them.

4.4.2 Descriptive Analysis of Deterrence

The study also sought to understand the influence of deterrence mechanisms on competitive advantage in private firms in Kenya. The statements used to operationalise deterrence are presented in Table 4.8. The analysis of deterrence mechanisms in the private sector in Kenya reveals a high emphasis on deterring unauthorised activity and encouraging adherence to security standards. The averages across the statements reflect a proactive approach to deterrence. The highest-rated statement, with a mean of 4.16, demonstrates that private firms use effective deterrent measures to keep employees from engaging in illegal actions. Communicating clear security regulations and the penalties for infractions had a mean of 4.09. This reinforces the deterrent approach by highlighting the necessity of policy understanding and adherence.

Table 4. 8 Private firm's deterrence mechanisms descriptive results

Statements	**Mean**	**Std. Dev**
Our organisation implements effective deterrence measures to discourage employees from engaging in unauthorized activities.	4.16	.864
We communicate clear security policies and consequences for policy violations to all employees to promote compliance and deter potential threats.	4.09	.950
Our organisation provides regular security training and awareness programs to educate employees on the importance of cybersecurity and their role in maintaining a secure environment.	3.83	1.175
We actively monitor employee web browsing behaviour to identify and address any security policy violations.	3.42	1.193

Our organisation utilises disciplinary actions, such as warnings and termination, to enforce security policies and deter employees from engaging in risky behaviour.	3.62	1.075
Overall Mean	**3.8227**	**.82962**

(Survey data, 2024).

Regular security training and awareness programs had a mean of 3.83. This suggests an above-average commitment to teaching staff about cybersecurity. As such, responses varied with a standard deviation of 1.175. Monitoring employee online browsing behaviour, with a mean of 3.42, and the usage of disciplinary procedures, with a mean of 3.62, demonstrate that private firms use an above average direct control and enforcement to maintain security policies. These results suggest that monitoring employee online browsing behaviour is an area of improvement for private firms in Kenya. With a mean of 3.82, the findings indicate an above-average effort by private firms in Kenya to prevent security breaches by combining policy communication, training, monitoring, and disciplinary actions. This holistic approach to deterrence is critical for ensuring a safe environment.

4.4.3 Descriptive Analysis of Detection

The study also sought to understand the effect of detection mechanisms on competitive advantage in private firms in Kenya. The analysis highlights a robust focus on early identification and response to security incidents in private firms in Kenya. The overall mean of 3.85 suggests an above-average commitment to detection practices among the surveyed firms. The highest-rated statement, with a mean of 4.05, demonstrates that private firms prioritize early detection to reduce possible damage and losses. The usage of advanced monitoring tools and technologies such as intrusion detection systems and security information and event management solutions, received an average rating of 3.76. This suggests an above-average priority for early detection of suspicious activities.

Table 4. 9 Private firm's detection mechanisms descriptive results

Statements	**Mean**	**Std. Dev**
Our organisation places a strong emphasis on early detection of security incidents to minimize potential damage and losses.	4.05	1.033
We employ advanced monitoring tools and technologies, such as intrusion detection systems and security information and event	3.76	1.195

management (SIEM) solutions, to detect suspicious activities on our network.		
Our security operations centre (SOC) continuously monitors audit trails and log files for signs of unauthorized access or malicious behaviour.	3.73	1.197
We regularly conduct security audits and vulnerability scans to proactively identify potential threats and vulnerabilities.	3.80	1.226
We have established clear processes and procedures for investigating and responding to security alerts and incidents promptly.	3.89	1.139
Overall Mean	**3.8470**	**1.03848**

(Survey data, 2024).

The continuous monitoring of audit trails and log files by SOCs received an average rating of 3.73 (SD = 1.197). This variability suggests differences in the resources and capabilities of SOCs among private firms. Firms conducting regular security audits and vulnerability scans had a mean of 3.80 (SD = 1.226). These results highlight proactive efforts by private firms to detect vulnerabilities. However, the results indicate there is room for improvement in standardising these practices. Further, clear processes and procedures for responding to security incidents and alerts averaged 3.89. This reflects an above-average structured approach to incident management in private firms in Kenya. The standard deviation of 1.139 suggests that, while private firms have established procedures, their effectiveness may vary. Essentially, the results indicate an above-average commitment to detection mechanisms across private firms in Kenya**.**

4.4.3 Descriptive Analysis of Competitive Advantage

The descriptive statistics for competitive advantage reveal an above-average (mean = 3.77, SD = 0.71) perception of competitive advantage among private firms in Kenya. The findings indicate that private firms perceived themselves as outperforming their competitors across several aspects of competitive advantage, albeit with some variation in specific areas. The mean of 3.98 suggests firms perceive their products' quality as superior to competitors. The 0.93 standard deviation suggests consistency of firms' confidence in product and service quality. Further, an above average of 3.94 (SD = 086) suggests the perception of corporate image is above average.

Table 4. 10 Private firms' competitive advantage descriptive results

Statements	Mean	Std. Dev
The quality of the products or services that our company offers is better than that of competitors' products or services	3.98	.932
Our company is more capable of R&D and innovation than the competitors	3.76	.936
Our company has better managerial capability than the competitors	3.80	.922
Our company's profitability is better than that of the competitors	3.43	.985
Our corporate image is better than that of your competitors	3.94	.856
Our company is much more flexible (regarding risks and challenges) than the competitors	3.78	.867
Overall, our company's growth is better than that of the competitors	3.70	.931
Overall Mean	**3.7698**	**.71153**

(Survey data, 2024).

Private firms' ability to be flexible in response to risks and challenges had an average of 3.78 (SD = 0.867). This suggests a widespread trust in slightly above-average adaptability compared to competitors. Similarly, managerial capability (mean = 3.80, SD = 0.922) suggests that private firms believe their management teams have an above-average capability to competitors. R&D and innovation capabilities (mean = 3.76, SD = 0.936) indicate an above-average confidence in innovative abilities. The firms' perceived growth (mean = 3.70, SD = 0.931) points to an above-average outlook on long-term performance relative to rivals.

Profitability (mean = 3.43, SD = 0.99) highlights private firms are less confident about their competitive position arising from profits. This suggests variability in profitability perceptions. It potentially indicates that financial performance is a more challenging area for these firms. Altogether, results suggest that while private firms in Kenya perceive themselves as having a competitive advantage, the confidence varies across different dimensions. Quality, corporate image, managerial capability, and flexibility are viewed more positively. Conversely, profitability is seen as less of a strength.

4.5 Inferential Analysis

Inferential analysis, comprising both correlation and regression analysis, was conducted. The results are presented in this subsection. Before performing the analysis, the researcher needed

to determine which regression model to employ between ordinal regression and linear regression. A normality test was performed and the results are presented in table 4.11. The results indicate that all the study variables are not normally distributed. This is because the Kolmogorov-Smirnov test and the Shapiro-Wilk tests have significant results at $P < 0.001$. To this end, the study selected the non-parametric method to conduct the inferential analysis. In other words, the Spearman Rank correlation and the Ordinal regression analysis were used for this study. Ordinal regression is used when the dependent variable is ordinal and not normally distributed.

Table 4. 11 Normality test

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	**df**	**Sig.**	**Statistic**	**df**	**Sig.**
Defence	.179	247	<.001	.850	247	<.001
Deterrence	.131	247	<.001	.935	247	<.001
Detection	.182	247	<.001	.882	247	<.001
Competitive advantage	.092	247	<.001	.973	247	<.001

a. Lilliefors Significance Correction

(Survey data, 2024).

4.5.1 Correlation Analysis Results

The correlation matrix reveals significant relationships between the dimensions of information security systems and competitive advantage. There is a positive correlation between defence and deterrence mechanisms ($r = 0.686$, $p < 0.001$). This indicates that firms with robust defence strategies tend to also have effective deterrent measures. The correlation between defence and detection is positive ($r = 0.743$, $p < 0.001$), reflecting that firms with strong defence mechanisms are likely to implement advanced detection systems. Similarly, deterrence and detection are highly correlated ($r = 0.772$, $p < 0.001$). This implies that private firms investing in deterrent strategies also tend to excel in detection capabilities.

Table 4. 12 Correlations matrix

		Defence	Deterrence	Detection	Competitive advantage
Defence	Corr Coefficient	1.000			
Deterrence	Corr Coefficient	.686**	1.000		
Detection	Corr Coefficient	.743**	.772**	1.000	
Competitive advantage	Corr Coefficient	.299**	.356**	.336**	1.000

****. Correlation is significant at the 0.01 level (2-tailed).**

(Survey data, 2024).

Regarding competitive advantage, defence mechanisms show a weak positive correlation ($r = 0.299$, $p < 0.001$). As the importance of defence mechanisms in private firms increases, so does competitive advantage, though at a weaker level. Deterrence and competitive advantage are also moderately correlated ($r = 0.356$, $p < 0.001$). The coefficient infers that as the importance of deterrent measures in private firms in Kenya increases, so does competitive advantage. However, this correlation is weak. In addition, detection mechanisms have a weak positive correlation with competitive advantage ($r = 0.336$, $p < 0.001$). As detection in private firms in Kenya increases, so does competitiveness, though this movement towards the same direction is weak.

The significant correlations between defence and detection and deterrence and detection suggest that these variables (as predictors) may not be independent of each other. This preliminary analysis points out to the potential issue of multicollinearity. This could potentially inflate the estimated coefficients' variance in the regression analysis. The issue of multicollinearity is addressed in the following subsection.

4.5.2 Addressing Multicollinearity

The first step in determining the existence of multicollinearity was to check the Variance Inflation Factor (VIF). According to Kim (2019), multicollinearity is present within a dataset when the VIF is above 5. The VIF was calculated for each predictor variable and results are presented in Table 4.13. the results suggest that the variable with the highest VIF was deterrence (VIF 3.75), followed by detection (VIF = 2.98), and defence (VIF = 2.96). Further, a low tolerance value (lower than 0.1 to 0.2) is considered by Kim (2019) as problematic since

it implies multicollinearity. In this study's case, the tolerance for all variables was above 0.2 with deterrence as the lowest at 0.267.

Table 4. 13 Variance Inflation Factor results

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	2.615	.243		10.768	<.001		
	DF	.100	.084	.122	1.190	.235	.338	2.960
	DT	.211	.088	.245	2.396	.017	.336	2.980
	DTC	.033	.079	.049	.425	.671	.267	3.745
	FS	.005	.034	.011	.152	.879	.724	1.380
	FA	-.088	.060	-.098	-1.460	.146	.775	1.290

a. Dependent Variable: CA

(Survey data, 2024).

However, to ensure that the moderate collinearity was not problematic, the researcher standardised the predictors to address the multicollinearity observed in the predictors. This was achieved by saving the z-scores of each variable for analysis. The predictors were scaled, helping stabilise the variance of each coefficient estimate. Further, an ordinal regression analysis was carried out using these standardised predictors. The results are presented in the next section.

4.6 Regression Analysis Results

4.6.1 To Assess the Influence of Information Security Systems on Competitive Advantage in Private Firms in Kenya

Before conducting the multiple regression analysis to address objective 1, several diagnostic tests were performed. The first test was the model fitting information presented in Table 4.14. The model fitting information shows that the -2 Log Likelihood for the final model is 1343.83. This is significantly lower than the intercept-only model (1380.535). The Chi-Square value of 36.708 with 5 degrees of freedom and a $P < 0.001$ indicates that the final model fits the data significantly better than the intercept-only model. This suggests that the inclusion of the independent and control variables (defence, deterrence, detection, firm size, and firm age) improves the model.

Table 4. 14 Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	1380.535			
Final	1343.827	36.708	5	<.001

(Survey data, 2024).

The second test conducted was the goodness of fit test. This is presented in Table 4.15. The goodness-of-fit statistics include Pearson Chi-Square (4625.42) and Deviance (1326.16) with respective significance levels of 0.948 and 1.00. These results imply that the model fits the observed data well. The high p-values (0.948 and 1.00) for both tests suggest no significant difference between observed and expected frequencies. These results support the multiple regression model's adequacy.

Table 4. 15 Goodness-of-Fit

	Chi-Square	df	Sig.
Pearson	4625.423	4783	.948
Deviance	1326.158	4783	1.000

(Survey data, 2024).

This study has evaluated the influence of information security systems on competitive advantage in private firms in Kenya. The aim is addressed by the pseudo-R-square results in Table 4.16. The pseudo-R-square values provide insight into the regression model's ($CA = \beta_0 + \beta_1 DF + \beta_2 DT + \beta_3 DTCT + \beta_4 FS + \beta_5 FA + \varepsilon$) Explanatory power. The Nagelkerke pseudo-R-square value is 0.139. This value suggests that the interaction between the independent variables (defence, detection, and deterrence) and the control variables (firm size and firm age) explain 13.9% of the variance in competitive advantage in private firms in Kenya. While the value is low, it implies that information security systems do have some influence on competitive advantage in private firms in Kenya.

Table 4. 16 Pseudo R-Square

Cox and Snell	.138
Nagelkerke	.139

(Survey data, 2024).

The results of the multiple regression assessing the effects of each independent variable on competitive advantage are presented in Table 4.17. The coefficient of defence is 0.091 with a

P-value of 0.632. While the result is positive, it is non-significant. These results imply that defence does not have a significant effect on the competitive advantage of private firms in Kenya. Other aspects other than defence explain the competitive advantage of private firms in Kenya.

Further, the coefficient of deterrence is 0.508 with a P-value of 0.009. A unit increase in the deterrence mechanism leads to a predicted increase in the competitive advantage of 0.508, which is statistically significant at a P-value of 0.009. These results imply that deterrence mechanisms have a significant effect on the competitive advantage of private firms in Kenya.

Results in Table 4.17 indicate that the coefficient of detection is 0.139 with a P-value of 0.518. This result is non-significant. These results imply that detection does not have a significant effect on the competitive advantage of private firms in Kenya. Other aspects other than detection explain the competitive advantage of private firms in Kenya.

Firm size ($\beta = 0.059$, $P = 0.653$) and firm age ($\beta = -0.165$, $P = 0.191$) have statistically non-significant coefficients. This implies that they do not have a significant controlling effect on the association between defence, deterrence, and detection on the competitive advantage of private firms in Kenya. Other dimensions control the relationship between information security systems and competitive advantage.

Table 4. 17 Parameter estimates results for multiple regression.

	Estimate	Std. Error	Sig.
Intercept	-5.770	0.985	<0.001
Defence	0.091	0.191	0.632
Deterrence	0.508	0.194	0.009
Detection	0.139	0.215	0.518
Firm size	0.059	0.030	0.653
Firm age	-0.165	0.126	0.191

(Survey data, 2024).

4.7 Chapter Summary

The multiple regression analysis for assessing the effects of information security systems on competitive advantage in private firms in Kenya revealed several key findings. Results indicate that only deterrence mechanisms had a significant positive effect on the competitive advantage of private firms in Kenya ($\beta = 0.508$, $p = 0.009$). Conclusions cannot be drawn from the

coefficients of defence and detections considering their nonsignificant P-values. The inclusion of firm size and firm age as control variables has no significant effect on the interaction between information security systems and competitive advantage in private firms in Kenya. These findings are expounded further in the discussion section in the next chapter.

CHAPTER FIVE
DISCUSSION OF FINDINGS, CONCLUSION, AND RECOMMENDATIONS

5.1 Introduction

Chapter five wraps up the research on the influence of information security systems on competitive advantage in private firms in Kenya. It commences with a discussion of the study findings. This discussion is guided by each research objective. The discussion synthesises this study's findings with those of earlier studies included in the literature review. The study has revealed contrasting relationships between various dimensions of ISS - including defence, deterrence, and detection mechanisms and the competitive advantage of private firms in Kenya. The analysis has also highlighted the limited control effect of firm size and firm age on the relationship between ISS and the competitive advantage of private firms. More significantly, the study draws conclusions from the deduction of the findings of this investigation. This chapter further advances recommendations for the management of private firms in Kenya and policy. The chapter concludes with a discussion of the study's limitations and recommendations for further research focused on addressing these research limitations. The following discussion critically examines the results in the context of each objective.

5.2 Discussion of Findings

5.2.1 Effect of Information Security Systems on Competitive Advantage of Private Firms in Kenya

This investigation's primary objective was to assess the association between information security systems and the competitive advantage of private firms in Kenya. The study operationalised information security systems using three dimensions: defence, deterrence, and detection. Notably, findings have shown that only deterrence mechanisms had a significant positive effect on the competitive advantage of private firms in Kenya ($\beta = 0.508$, $p = 0.009$). These findings imply that increased deterrence significantly improves the competitive advantage of private firms in Kenya. Essentially, private firms investing in robust deterrence strategies are better positioned competitively. These results align closely with Dynamic Capability Theory. According to DCT, a firm's ability to adapt and effectively leverage existing resources in an ever-changing operating environment maintains a competitive advantage (Nayal et al., 2022). The positive association between deterrence mechanisms and competitive advantage implies that private firms actively managing deterrence strategies, such

as stringent security policies and robust incident responses, have adaptive capabilities they use to mitigate security threats (Kosutic, 2021). These findings are supported by empirical literature reviewed in this study, which highlights that a well-developed ISS framework enables firms to secure sensitive data, sustain operational integrity, reduce security-related disruptions, minimise resource drain, and build client trust (Šikman et al., 2019; Alanezi & Brooks, 2014). This strategic deterrence enhances operational resilience. They allow firms to respond proactively to security threats. This is a capability that competitors might struggle to replicate due to resource constraints. Hence, they contribute to a sustainable competitive advantage.

The disincentives of private firms' ISS in Kenya, such as penalties for non-compliance with security protocols, and formal policies establish a firm stance against security breaches. These strategies deter malicious ISS actions while developing a reputation of control and vigilance. These aspects are attractive to stakeholders such as customers, investors, and partners. Private firms that successfully implement robust deterrence policies have enhanced stakeholder trust and confidence. In line with DTC, this strengthens competitive advantage through proactive and adaptive security management that aligns with prevailing business needs (Nayal et al., 2022).

Further, deterrence measures in Kenyan private firms that focus on security awareness and regular training encourage a culture of vigilance among staff. This makes the internal stakeholder an active participant in the firms' ISS framework. Private firms that invest in internal awareness build an adaptive culture proactive to potential threats. In line with Gundu and Modiba (2020), awareness and training initiatives enhance operational resilience. This is through a reduction of human error, which is a significant contributor to ISS incidents. Ultimately, training and awareness support private organisations' competitive positioning.

This study has also established that deterrence through physical security measures, such as access control and surveillance, protects private firms' critical assets and information. This differentiates firms that invest in physical security measures from those that overlook them. From the stakeholder's eye - particularly customers and strategic partners, the visibility of physical security creates a perception of private firms' commitment to safeguarding assets. This aligns with the Information Security Policy Framework's assertion that visible, well-designed deterrent measures positively influence stakeholder perceptions (Rostami et al., 2020). This reinforces the competitive standing of such firms. Altogether, the disincentives of ISS, their deterrence policies, awareness, training, and physical security contribute to a

proactive and robust security stance that directly contributes to the competitive advantage of private organisations in Kenya. This study established that reducing breach likelihoods and enhancing stakeholder trust leads to a competitive edge beyond security risk mitigation.

Conversely, the study has established that defence and detection have no significant effect on competitive advantage; hence, no conclusion has been drawn. The non-significant effects of defence ($\beta = 0.091$, $p = 0.632$) and detection ($\beta = 0.139$, $p = 0.518$) suggest that these mechanisms alone may not directly contribute to a Kenyan private firm's competitive advantage. This could result from the essential yet non-differentiating nature of defence and detection measures. The argument is that, while these measures are critical to operational security, they fail to directly drive competitive advantage in the same way deterrence does. The commodity nature of defence and detection mechanisms means that they are often standardised in firms.

The Information Security Policy Framework argues that a security policy framework aims to create a holistic defence structure (Rostami et al., 2020). This study includes components that both prevent and deter threats. However, as this study has established, implementing defence and detection mechanisms may fail as sufficient factors of ISS that drive competitive advantage. This argument is supported by Gundu and Modiba (2020) who find that ISS that focuses on detection or defence may overlook broader strategic and adaptive capabilities that are required to enhance competitive advantage. While defence and detection are critical mechanisms for baseline-level security in private firms in Kenya, deterrence mechanisms are more aligned with strategic deterrence and competitiveness. This is because they align with the DCT's tenets of adapting practices to evolving threats.

Private firms' ISS defence, as exercised through the deployment of firewalls, authentication devices, and physical obstacles serve as procedural and technical security measures to unauthorised access in private organisations in Kenya. The finding suggests that the firewalls, authentication devices, and physical obstacles may be standardised across private firms in Kenya, failing to confer a unique edge to organisations that implement them.

Further, defence procedures could be compliance-driven. This means that they may be a requirement for operational continuity. While they meet regulatory standards, they may fail to enhance a private firm's market position or reputation. Concurring with Kosutic (2021), this study argues that the uniformity in defence mechanisms diminishes any potential differentiators as they fulfil minimum security expectations without creating a competitive edge.

On the other hand, security breach detection and internal control systems are primarily mechanisms for identifying issues as they arise. This makes them potentially reactive. While literature suggests that security breach detection and internal control systems are indispensable for managing security incidents in firms (Cohen et al., 2017; Kakucha & Buya, 2018), this study has found that they fail to enhance the reputation of private firms in Kenya. Similarly, audit trails serve a compliance role in ISS. This is by maintaining records of system activities and access. While audit trails ensure accountability in the event of a security breach, they remain a back-end process that fails to create more economic value compared to competitors, fails to provide above-average exploitation of existing opportunities while neutralising competitive threats, or protect what is wanted, scarce, and valued by the market (Serrado et al., 2020). This means that they fail to visibly impact the competitive advantage of private firms in Kenya.

This study's results align with Šikman et al.'s (2019) suggestion that, while defence and detection are key to securing operational integrity, they may not directly contribute to competitive advantage. According to DTC, competitive advantage arises from capabilities that allow firms to anticipate and adapt to changes in the operating environment. However, defence and detection are largely static in private firms in Kenya. As regulatory or policy-driven practices, they may fail to support the adaptive and proactive stance necessary for obtaining and sustaining competitive advantage.

5.2.2 Controlling Effect of Firm Size and Firm Age on the Influence of Information Security Systems on Competitive Advantage in Private Firms in Kenya

The findings have established that firm size and firm age do not significantly control the relationship between ISS and competitive advantage. The results indicated no significant controlling effects for either firm size ($\beta = 0.059$, $p = 0.653$) or firm age ($\beta = -0.165$, $p = 0.191$). These findings suggest that the strategic benefits of ISS are not confident to established or large private firms in Kenya. As Tran et al. (2019) argue, in line with the DCT, firms can enhance capabilities through ISS and foster responsiveness and agility irrespective of structural constraints. Further, Cohen et al. (2017) postulate that deterrence and defence ISS dimensions can adapt to fit firms of any age or size. Small or startup firms are vulnerable to information security threats, as is the case with large and established firms. This suggests that small firms can benefit from deterrent measures, securing operations while enhancing resilience.

These findings challenge the assumption that older or larger firms potentially leverage ISS differently to their advantage possibly because of their established market positions or greater resources. The findings signify that, concurring with Information Security Policy Framework (Whitman & Mattord, 2021), ISS practices are becoming standardised across firms of different sizes and ages. This means that ISS strategies could be universally accessible. Similarly, Saeidi et al. (2019) supports this assertion by indicating that firms of varying sizes benefit equally from well-developed and implemented ISS.

The failure of firm size and age to moderate ISS's effects on competitive advantage implies there is a shift towards more standardised ISS practices in Kenya. This could be driven by technological advancements, regulatory requirements, or the need to align with best practices in the industry. These findings point out that Kenya private firms' competitive advantages through ISS are more closely related to the strategic integration of deterrence, as opposed to the characteristics of the organisations.

5.3 Conclusions

This study has evaluated the influence of information security systems on competitive advantage in private firms in Kenya. The study concludes that the deterrence mechanism positively and significantly predicts competitive advantage. This is by building a security-conscious culture and operational resilience in private organisations in Kenya, increasing stakeholder confidence in the process. Visible disincentives, proactive policies, and continuous training directly support the Dynamic Capability Theory's emphasis on adaptability. Similarly, the findings support the Information Security Policy Framework's focus on integrated and structured policies. Conversely, this study has concluded that defence and detection measures, while essential for baseline security and fulfilling basic security requirements, fail to offer any unique value proposition or differentiation. The study highlights that Kenyan private firms seeking to leverage ISS for competitive advantage should enhance their deterrence mechanisms.

Private organisations in Kenya need to protect their information systems through defect detection, and deterrence of any unauthorised access to information or its modification. This is whether it is in information processing, storage, or transit. Practically, private firms in Kenya can gain from prioritising deterrence strategies. These strategies should align with regulatory standards and firm-level policies to strike a balance between foundational defence and strategic deterrence. Considering the limited variance explained by ISS, private firms in Kenya should

recognise that ISS forms just one component of a broader competitive strategy. As such, its value lies in effective integration with other strategic initiatives.

5.4 Recommendations

5.4.1 Policy Recommendation

This study recommends that private firms and other ICT stakeholders in Kenya should enhance regulatory standards for deterrence-oriented ISS. Considering the significant positive effect of deterrence mechanisms on competitive advantage, policymakers should develop and support regulatory frameworks that encourage Kenyan private firms to invest and adopt deterrence-focused ISS. These policies could range from incentives for private firms to implement rigorous deterrence strategies such as awareness programs, formal security policies, and physical security standards, to mandatory compliance requirements that reinforce adopting these policies.

5.4.2 Managerial Recommendation

For managers of private firms in Kenya, this study recommends that they embed security awareness in organisational culture. For instance, private firms' managers should make security awareness a component of the organisational culture. This is by encouraging employees to adopt a proactive stance on security. Besides, regular training, security workshops, and awareness campaigns will help employees internalise ISS practices. This will reduce vulnerabilities from human error while enhancing the overall security framework.

Second, the management of private firms in Kenya should balance ISS components while emphasising strategic deterrence. Defence (firewalls and authentication) and detection (audit trail and internal control) should be in place such that the private firms meet policy requirements. However, these firms should prioritise deterrence mechanisms in their strategy for a more holistic and strategic security framework that will contribute to the competitive advantage.

5.5 Theoretical Contribution

Theoretically, this study supports both Dynamic Capability Theory and Information Security Policy Framework. This is by highlighting ISS's role as both a structured policy framework and a strategic asset to firms. The study highlights deterrence mechanisms - such as security policies, awareness programs, and training - as adaptive capabilities. These adaptive

capabilities allow private firms to proactively respond to evolving threats in their operational environments. The study extends DTC by positioning ISS as a resource for both security protection and market competitiveness. Moreover, it supports Information Security Policy Framework's assertion that proactive deterrence policies, when designed strategically, are crucial to the strengthening of the competitive advantage of private firms. Finally, a focus on Kenya's private sector offers a contextual insight into developing markets. As such, deterrence, as a dimension of ISS, appears critical in contributing to the competitiveness of private firms in developing economies. The findings underline the relevance of private firms in developing markets to tailor their ISS strategies.

5.6 Study Limitations and Suggestions for Further Research

This study has two primary limitations that stem from its cross-sectional design and the exclusive adoption of quantitative methods. Considering that the cross-sectional design has captured the data on ISS and the competitive advantage of private firms in Kenya at one point in time, this limits the observation of changes to the relationships over time. This means that the concluded study may fail to account for potential temporal variations in the association between the dimensions of ISS and competitive advantage. Further, the use of quantitative methods in data collection, analysis, and presentation means there is a possibility that important subjective insights that could explain the direction of associations between the study variables have been excluded.

Future studies can address these limitations by, first, adopting a longitudinal design to track changes over time and, second, by incorporating qualitative methods. This is in the form of a mixed-method study that could incorporate key informant interviews or case studies. The mixed-method research will aid in gathering richer data that has both objective and subjective insights. Besides, future research could deepen the understanding of the association between ISS and competitive advantage by expanding the empirical context to other regions or comparing the association between industries.

.

.

REFERENCES

Abbasi Kamardi, A., Amoozad Mahdiraji, H., Masoumi, S., & Jafari-Sadeghi, V. (2022). Developing sustainable competitive advantages from the lens of resource-based view: evidence from IT sector of an emerging economy. *Journal of Strategic Marketing*, 1-23.

Accerboni, F., & Sartor, M. (2019). ISO/IEC 27001. In *Quality Management: Tools, Methods, and Standards* (pp. 245-264). Emerald Publishing Limited.

Adamik, A. and Nowicki, M. (2020). Barriers of creating competitive advantage in the age of industry 4.0: conclusions from international experience. In *Contemporary Challenges in Cooperation and Coopetition in the Age of Industry 4.0* (pp. 3-42). Springer, Cham.

Aidara, S., Mamun, A. A., Nasir, N. A. M., Mohiuddin, M., Nawi, N. C., & Zainol, N. R. (2021). Competitive advantages of the relationship between entrepreneurial competencies and economic sustainability performance. *Sustainability, 13*(2), 864.

Archibald, M. M., Ambagtsheer, R. C., Casey, M. G., & Lawless, M. (2019). Using zoom videoconferencing for qualitative data collection: perceptions and experiences of researchers and participants. *International Journal of Qualitative Methods, 18*, 1–8.

Arranz, N., Arroyabe, M., Li, J., & Fernandez de Arroyabe, J. C. (2020). Innovation as a driver of eco-innovation in the firm: An approach from the dynamic capability's theory. *Business Strategy and the Environment, 29*(3), 1494-1503.

Bal, H. Ç., & Erkan, Ç. (2019). Industry 4.0 and competitiveness. *Procedia computer science, 158*, 625-631.

Bandari, V. (2023). Enterprise data security measures: A comparative review of effectiveness and risks across different industries and organisation types. *International Journal of Business Intelligence and Big Data Analytics, 6*(1), 1-11.

Barafort, B., Mesquida, A. L., & Mas, A. (2019). ISO 31000-based integrated risk management process assessment model for IT organisations. *Journal of Software: Evolution and Process, 31*(1), 1-15.

Breda, G., & Kiss, M. (2020). Overview of information security standards in the field of special protected industry 4.0 areas & industrial security. *Procedia Manufacturing, 46*, 580-590.

Burt, A. (2019). Cybersecurity is putting customer trust at the centre of the competition. *Harvard Business Review*.

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., ... & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing, 25*(8), 652-661.

Chai, H. H., Gao, S. S., Chen, K. J., Duangthip, D., Lo, E. C. M., & Chu, C. H. (2021). A concise review on qualitative research in dentistry. *International Journal of Environmental Research and Public Health, 18*(3), 1-13.

Cheah, J., Leong, S. Y., & Fernando, Y. (2023). Innovation strategies and organisational performance: the moderating role of company size among small-and medium-sized companies. *Benchmarking: An International Journal, 30*(9), 2854-2868.

Chowdhury, M. M. H., & Quaddus, M. (2017). Supply chain resilience: Conceptualization and scale development using dynamic capability theory. *International Journal of Production Economics, 188*, 185-204.

Communication Authority of Kenya. (2023). *Cybersecurity report.* The National KE-CIRT/CC.

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76-105.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*, 101713.

De Arroyabe, I. F., Arranz, C. F., Arroyabe, M. F., & de Arroyabe, J. C. F. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security, 124*, 102954.

Deane, J. K., Goldberg, D. M., Rakes, T. R., & Rees, L. P. (2019). The effect of information security certification announcements on the market value of the firm. *Information Technology and Management, 20,* 107-121.

Deszczyński, B., & Deszczyński, B. (2021). *Firm competitive advantage through relationship management: A theory for successful sustainable growth*. Palgrave Macmillan

Edwards, D. J. (2024). Security Policies and Procedures. In *Mastering Cybersecurity: Strategies, Technologies, and Best Practices* (pp. 413-434). Berkeley, CA: Apress.

Farida, I., & Setiawan, D. (2022). Business strategies and competitive advantage: The role of performance and innovation. Journal of Open Innovation: Technology, Market, and Complexity, 8(3), 1-16.

Fast, V., Schnurr, D., & Wohlfarth, M. (2023). Regulation of data-driven market power in the digital economy: Business value creation and competitive advantages from big data. *Journal of Information Technology, 38*(2), 202-229.

Fincham, J. E. (2008). Response rates and responsiveness for surveys, standards, and the Journal. *American journal of pharmaceutical education, 72*(2). Retrieved October 12, 2024, from https://www.ajpe.org/article/S0002-9459(23)04200-6/pdf.

Gani, A., Imtiaz, N., Rathakrishnan, M., & Krishnasamy, H. N. (2020). A pilot test for establishing validity and reliability of qualitative interview in the blended learning English proficiency course. *Journal of Critical Reviews, 7*(05), 140-143.

Ghosh, S., Hughes, M., Hodgkinson, I., & Hughes, P. (2022). Digital transformation of industrial businesses: A dynamic capability approach. *Technovation, 113,* 1-18.

Goel, L., Russell, D., Williamson, S., & Zhang, J. Z. (2023). Information systems security resilience as a dynamic capability. *Journal of Enterprise Information Management, 36*(4), 906-924.

Gundu, T., & Modiba, N. (2020). Building competitive advantage from Ubuntu: An African information security awareness model. *In ICISSP* (pp. 569-576).

Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. B., Amjad, M. F., Malik, J., ... & Khan, A. W. (2021). Cybersecurity standards in the context of operating system: practical aspects, analysis, and comparisons. *ACM Computing Surveys (CSUR), 54*(3), 1-36.

Hamdi, Z., Norman, A. A., Molok, N. N. A., & Hassandoust, F. (2019). A comparative review of ISMS implementation based on ISO 27000 series in organisations of different business sectors. *Journal of Physics: Conference Series (Vol. 1339*(1), 1-8.

Haqqi, T. (2023). 14 Most Technologically Advanced Countries in Africa. Yahoo Finance. https://finance.yahoo.com/news/15-most-technologically-advanced-countries-

180436967.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALWtcbuHKNOKtgluypfMNtbJ5_DNNP_TvwKu0tv1JXNqEB3BYD_-EZE5SEoDUkslTwaX9sx8oXE4AdvX3ppmnLig15yD_XVBlZh1Ho50IzRzrrI3OTmUR-ZSnj4zi4fgaBOa6ANOi9mhmtQsH9QxZSFndDKc4ZtZPWfWVrcwjKeF.

Heeks, R., & Ospina, A. V. (2019). Conceptualising the link between information systems and resilience: A developing country field study. *Information Systems Journal, 29*(1), 70-96.

HR, G., & Aithal, P. S. (2022). Why is it Called a Doctor of Philosophy and Why Choosing Appropriate Research Philosophical Paradigm is Indispensable During Ph. D. Program in India? *International Journal of Philosophy and Languages (IJPL), 1*(1), 42-58.

International Organisation for Standardization. (2018). *Information technology - Security techniques - information security management systems: Overview and vocabulary* (5th ed. 2018-02). Geneva, Switzerland: International Organisation for Standardization.

Jann, W., & Wegrich, K. (2017). Theories of the policy cycle. In *Handbook of public policy analysis* (pp. 69-88). Routledge.

Kakucha, W., & Buya, I. (2018). Information system security mechanisms in financial management. *Journal of Information and Technology, 2*(1), 1-16.

Kamaziwe, D. W. (2023). *Information security governance shortfalls in non-IT organizations: A generic qualitative inquiry* (Doctoral dissertation, Capella University).

Kenya Bankers Association (2021). *Micro, Small & Medium Enterprises (MSMEs): Survey Report- 2021*. Kenya Bankers Association. Retrieved October 12, 2024, from https://www.kba.co.ke/wp-content/uploads/2022/05/MSMEs-Survey-Report.pdf.

Kenya Institute for Public Policy Research and Analysis. (2020). *Kenya economic report 2020: Creating an enabling environment for inclusive growth in Kenya.* Kenya Institute for Public Policy Research and Analysis.

Kenya Private Sector Alliance. (2022). *Annual report*. Kenya Private Sector Alliance

Kim, J. H. (2019). Multicollinearity and misleading statistical results. *Korean Journal of Anesthesiology, 72*(6), 558-569. https://doi.org/10.4097/kja.19087

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77-81.

Kosutic, D. (2021). The impact of cybersecurity on competitive advantage (Doctoral dissertation, Grenoble Ecole De Management).

Kosutic, D., & Pigni, F. (2022). Cybersecurity: Investing for competitive outcomes. *Journal of Business Strategy, 43*(1), 28-36.

Leavy, P. (2022). *Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches*. Guilford Publications.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons, 64*(5), 659-671.

Lee, K., & Yoo, J. (2019). How does open innovation lead competitive advantage? A dynamic capability view perspective. *Plos One, 14*(11), 1-18.

Lochmiller, C. R. (2021). Conducting thematic analysis with qualitative data. *The Qualitative Report, 26*(6), 2029-2044.

Lorenzo, J. R. F., Rubio, M. T. M., & Garcés, S. A. (2018). The competitive advantage in business, capabilities and strategy. What general performance factors are found in the Spanish wine industry? *Wine Economics and Policy, 7*(2), 94-108.

Makhija, A. K. (2021). Information Security Management Systems- Evolving landscape & ISO 27001: An empirical study. *Journal of Accounting, Finance, Economics and Social Sciences, 6*(1), 19-27.

Makupi, D. (2021). *An ISO 27001 based model to determine university information security maturity under uncertainty* (Doctoral Dissertation, Kabarak University).

Meriah, I., & Rabai, L. B. A. (2019). Comparative study of ontologies based iso 27000 series security standards. *Procedia Computer Science, 160*, 85-92.

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & Security, 109*, 1-23.

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis. *IEEE Transactions on Engineering Management, 68*(1), 87-100.

Mirtsch, M., Pohlisch, J., & Blind, K. (2020). International diffusion of the information security management system standard ISO/IEC 27001: Exploring the role of culture. *European Conference on Information Systems,* 1-18.

Murphy, G. (2022). The journey to ISO 27001 certification. *Strategic Finance, 104*(1), 62-63.

Mwaura, J. (2024). Silicon Savannah or digitising marginalisation? A reflection of Kenya's government digitisation policies, strategies, and projects. *In Communication Rights in Africa* (pp. 38-54). Routledge.

Naanani, A. (2021). Security in Industry 4.0: Cyber-attacks and countermeasures. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12*(10), 6504-6512.

Naveh, E., & Marcus, A. (2005). Achieving competitive advantage through implementing a replicable management standard: Installing and using ISO 9000. *Journal of Operations Management, 24*(1), 1-26.

Nayal, P., Pandey, N., & Paul, J. (2022). Covid-19 pandemic and consumer-employee-organisation wellbeing: A dynamic capability theory approach. *Journal of Consumer Affairs, 56*(1), 359-390.

Nickels, W., McHugh, J., & McHugh, S. (2024). *Understanding Business*. McGraw Hill.

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European journal of information systems, 26*(1), 1-20.

Njenga, K., Garg, L., Bhardwaj, A. K., Prakash, V., & Bawa, S. (2019). The cloud computing adoption in higher learning institutions in Kenya: Hindering factors and recommendations for the way forward. *Telematics and Informatics, 38*, 225-246.

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry, 142*, 1-10.

Omoyiola, B. O. (2020). The evolution of information security measurement and testing. *IOSR Journal of Computer Engineering, 22*(3), 50-54.

Paiola, M., & Gebauer, H. (2020). Internet of things technologies, digital servitisation and business model innovation in B-B manufacturing firms. *Industrial Marketing Management, 89,* 245–264.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC press.

Saeidi, P., Saeidi, S. P., Sofian, S., Saeidi, S. P., Nilashi, M., & Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of information technology. *Computer Standards & Interfaces, 63*, 67-82.

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. Future Generation Computer Systems, 97, 587-597.

Sainsbury, D. (2020). Toward a dynamic capability theory of economic growth. *Industrial and Corporate Change, 29*(4), 1047-1065.

Sanchez, J. I., Bonache, J., Paz-Aparicio, C., & Oberty, C. Z. (2023). Combining interpretivism and positivism in international business research: The example of the expatriate role. *Journal of World Business, 58*(2), 1-13.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students*. Harlow, UK: Pearson Education Limited.

Serrado, J., Pereira, R. F., Mira da Silva, M., & Scalabrin Bianchi, I. (2020). Information security frameworks for assisting GDPR compliance in banking industry. *Digital Policy, Regulation and Governance, 22*(3), 227-244.

Sewpersadh, N. S. (2023). Disruptive business value models in the digital era. *Journal of Innovation and Entrepreneurship, 12*(1), 1-27.

Shrotryia, V. K., & Dhanda, U. (2019). Content validity of assessment instrument for employee engagement. *Sage Open, 9*(1), 1-7.

Šikman, L., Latinović, T., & Paspalj, D. (2019). ISO 27001-Information Systems Security, development, trends, technical and economic challenges. *Annals of the Faculty of Engineering Hunedoara*, *17*(4), 45-48.

Spector, P. E. (2019). Do not cross me: Optimizing the use of cross-sectional designs. *Journal of Business and Psychology*, *34*(2), 125-137.Seebeck, L. (2020). Digital technology, cyber security, and the public service challenge in Australia. *The Palgrave Handbook of the Public Servant*, 1-16.

Szymańska, K. (2020). Organisational culture in the industry 4.0 era: Introduction to research. In *Contemporary Challenges in Cooperation and Coopetition in the Age of Industry 4.0* (pp. 123-136). Springer, Cham.

Talafidaryani, M. (2021). A text mining-based review of the literature on dynamic capabilities perspective in information systems research. *Management Research Review*, *44*(2), 236-267.

Tatiara, R., Fajar, A. N., Siregar, B., & Gunawan, W. (2018). Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001. *Journal of Physics: Conference Series*, *978*(1), 1-7.

Teece, D. J. (2020). Hand in glove: Open innovation and the dynamic capabilities framework. *Strategic Management Review*, *1*(2), 233-253.

Thomas, O. O., & Lawal, O. R. (2020). Exploratory research design in management sciences: An X-Ray of literature. *Annals of the University Dunarea de Jos of Galati: Fascicle: I, Economics & Applied Informatics*, *26*(2), 79-84.

Tran, Y., Zahra, S., & Hughes, M. (2019). A process model of the maturation of a new dynamic capability. *Industrial Marketing Management, 83*, 115-127.

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in the aviation industry: A review of current and future trends. *Information, 13*(3), 1-22.

Unigwe, M. (2022). The Views of information security professionals toward information security objectives: Confidentiality, integrity, and availability Triad (Doctoral dissertation, Trident University International).

Wanyonyi, V. (2020). *Information security Management toolkit for ISO/IEC 27001 standard, case of small-to-medium sized enterprises (SMEs)* (Doctoral dissertation, University of Nairobi).

Winarno, H., Yasin, F., Prasetyo, M. A., Rohman, F., Shihab, M. R., & Ranti, B. (2020, September). IT infrastructure security risk assessment using the Center for Internet Security Critical Security Control framework: a case study at insurance company. In *2020 3rd International Conference on Computer and Informatics Engineering* (IC2IE) (pp. 404-409). IEEE.

Wu, M. J., Zhao, K., & Fils-Aime, F. (2022). Response rates of online surveys in published research: A meta-analysis. *Computers in Human Behavior Reports, 7*, 1-11. https://doi.org/10.1016/j.chbr.2022.100206

Wu, W., Shi, K., Wu, C. H., & Liu, J. (2021). Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance. J*ournal of Global Information Management (JGIM), 30*(3), 1-16.

Xu, S. (2019). Cybersecurity dynamics: A foundation for the science of cybersecurity. *Proactive and Dynamic Network Defense*, 1-31.

Xu, W., & Zammit, K. (2020). Applying thematic analysis to education: A hybrid approach to interpreting data in practitioner research. *International Journal of Qualitative Methods, 19*, 1-9.

Yoshikuni, A. C., Dwivedi, R., Favaretto, J. E. R., & Zhou, D. (2024). How enterprise information systems strategies-enabled strategy-making influences organizational agility: mediated role of IT-enabled dynamic capabilities in two BRICS countries study. *Journal of Enterprise Information Management, 37*(1), 230-258.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behaviour: A comparative study. *Journal of Computer Information Systems, 62*(1), 82-97.

APPENDICES

Appendix A: Introduction Letter

My name is Mike Kamau. I am an MBA student in the School of Management and Administration at Strathmore University. I kindly invite you to take part in this study towards the completion of my thesis on *Influence if Information Security Systems on Competitive Advantage in Private Firms in Kenya.* The survey will take about 5 minutes or less. You are one of a few persons I have chosen for this study who have extensive understanding of the topic being studied. Your participation in this study is entirely voluntary. You have the ability to withdraw from the study at any moment, without explanation or penalty.

I have taken steps to guarantee that there are no hazards associated with participating in the study. If something goes wrong, I will accept complete responsibility. I have compiled a list of questions to ask you concerning information security systems and competitive advantage in Kenya's private enterprises. I will not collect any personal information. All information will be kept confidential and private. Please read the instructions carefully and submit honest responses.

Your information will be utilised in the thesis for my degree program. The information will be given in an anonymous fashion and will not be saved in a database that others can access. Following Strathmore University's Privacy Policy, I will keep your information confidential, and only my supervisor and I will have access to it. Your information will be stored completely anonymously in a password-protected folder that only I will have access to. I will destroy the data once my dissertation has been graded.

If you have any questions concerning the research, please contact me using the email address shown in the contact section below. Thank you for your precious time and cooperation.

Researcher Contact Details:

Mike Kamau

Email Address: …….....

Appendix B: Questionnaire

Section A- Demographics

1. **Education Level**
    - High school
    - Diploma
    - University Degree
    - Master's Degree
    - Doctoral Degree
2. **Age**
    - 18-29
    - 30-39
    - 40-49
    - 50-59
    - Over 60
3. **Gender**
    - Female
    - Male
    - Prefer not to say
4. **How many employees does your organisation currently have?**
    - Less than 50
    - 50-100
    - 101-500
    - 501-1000
    - More than 1000
5. **How long has your organisation existed?**
    - 1-5 years
    - 6-10 years
    - Above 10 years

Section B: Defence, Deterrence, Detection, Competitive Advantage.

To what extent do you agree or disagree with the following statements? Please appropriately tick the box with your level of agreement:

N	Item	Strongly-Disagree (1)	Disagree (2)	Undecided (3)	Agree (4)	Strongly-Agree (5)
	Part A: Defence					
1	Our organisation prioritizes implementing robust defence mechanisms to protect valuable information assets.					
2	We invest in state-of-the-art security technologies, such as firewalls and access control systems, to safeguard our network infrastructure.					
3	Our organisation regularly updates and patches software to address vulnerabilities and enhance our defensive capabilities.					
4	We have established clear procedures and protocols for handling security incidents to minimize the impact of potential breaches.					
5	Our defensive controls are designed to mitigate various threats, including software vulnerabilities, bugs, and accidental data damage.					
	Part B: Deterrence					
1	Our organisation implements effective deterrent measures to discourage employees from engaging in unauthorized activities.					
2	We communicate clear security policies and consequences for policy violations to all employees to promote compliance and deter potential threats.					
3	Our organisation provides regular security training and awareness programs to educate employees on the importance of cybersecurity and their role in maintaining a secure environment.					
4	We actively monitor employee web browsing behaviour to identify and address any security policy violations.					
5	Our organisation utilises disciplinary actions, such as warnings and termination, to enforce security policies and deter employees from engaging in risky behaviour.					
	Section C: Detection					
1	Our organisation places a strong emphasis on early detection of					

	security incidents to minimize potential damage and losses.					
2	We employ advanced monitoring tools and technologies, such as intrusion detection systems and security information and event management (SIEM) solutions, to detect suspicious activities on our network.					
3	Our security operations centre (SOC) continuously monitors audit trails and log files for signs of unauthorized access or malicious behaviour.					
4	We regularly conduct security audits and vulnerability scans to proactively identify potential threats and vulnerabilities.					
5	We have established clear processes and procedures for investigating and responding to security alerts and incidents in a timely manner.					
	Section D: Competitive Advantage					
1	The quality of the products or services that our company offers is better than that of the competitor's products or services					
2	Our company is more capable of R&D and innovation than the competitors					
3	Our company has better managerial capability than the competitors					
4	Our company's profitability is better than the competitors					
5	Our corporate image is better than your competitors					
6	Our company is much more flexible (regarding the risks and challenges) than the competitors					
7	Overall, our company's growth is better than the competitors					

Questions adapted from Alanezi and Brooks (2014); Cheah, Leong, & Fernando (2023), Cohen et al. (2017), Gundu and Modiba (2020), Kakucha and Buya (2018), Saeidi et al. (2019), and Safa et al. (2019).

Appendix C: NACOSTI Research Permit

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: 270315

Date of Issue: 04/July/2024

RESEARCH LICENSE

This is to Certify that Mr.. Mike Kamau of Strathmore University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Baringo, Bomet, Bungoma, Busia, Elgeyo-Marakwet, Embu, Garissa, Homabay, Isiolo, Kajiado, Kakamega, Kericho, Kiambu, Kilifi, Kirinyaga, Kisii, Kisumu, Kitui, Kwale, Laikipia, Lamu, Machakos, Makueni, Mandera, Marsabit, Meru, Migori, Mombasa, Muranga, Nairobi, Nakuru, Nandi, Narok, Nyamira, Nyandarua, Nyeri, Samburu, Siaya, Taita-Taveta, Tanariver, Tharaka-Nithi, Trans Nzoia, Turkana, Uasin-Gishu, Vihiga, Wajir, Westpokot on the topic: Influence Of Information Security Systems On Competitive Advantage In Private Firms In Kenya for the period ending : 04/July/2025.

License No: NACOSTI/P/24/37125

270315

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions

Appendix D: Institutional Ethics Permit

Strathmore UNIVERSITY

10th June 2024

Mr Kamau Mike,
mike.kamau@strathmore.edu

Dear Mr Kamau,

RE: Influence Of Information Security Systems on Competitive Advantage in Private Firms in Kenya

This is to inform you that SU-ISERC has reviewed and **approved** your above SU-masters proposal. Your application reference number is **SU-ISERC2283/24**. The approval period is from **10th June 2024 to 9th June 2025**.

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used.
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-ISERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-ISERC within 72 hours of notification.
iv. Any changes anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-ISERC within 72 hours.
v. Clearance for the export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to the expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days of completion of the study to SU-ISERC.

Before commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research-portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,

Mr Ambrose Rachier,
Chairperson; SU-ISERC

Ole Sangale Rd, Madaraka Estate, PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034000
Email admissions@strathmore.edu www.strathmore.edu