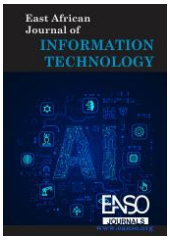
Article DOI: https://doi.org/10.37284/eajit.6.1.1612



East African Journal of Information Technology
eajit.eanso.org
Volume 6, Issue 1, 2023
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Human Resource Information Systems Information Security and Organizational Performance of Commercial State Corporations in Kenya

Dr. Ann Gaceri Kaaria, PhD[1*]

[1] Kiriri Women's University of Science and Technology, P. O. Box 49274 – 00100. Nairobi, Kenya.
* Correspondence email: ann.gaceri.k@gmail.com.

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

Date Published:

08 December 2023

Keywords:

Information Security, Organisational Performance, Commercial State Corporations

ABSTRACT

The purpose of this study was to establish the influence of HRIS information security on the organisational performance of commercial state corporations in Kenya. A Cross-sectional descriptive research design was used. The population was drawn from 55 Commercial State Corporations in Kenya. The units of observation were the managing directors or chief executive officers, directors of human resources, and deputy directors of human resources. The study used qualitative and quantitative methods to collect primary and secondary data. Data were collected from 110 respondents. Questionnaires and interviews were used to collect data for the study, supplemented by secondary sources. SPSS version 23.0 was used to analyse data using descriptive analysis, factor analysis, Pearson correlation, analysis of variance (ANOVA), and regression. The correlation and regression results revealed that HRIS Information Security had a positive and significant relationship with Kenya's Organizational Performance of Commercial State Corporations. The null hypothesis indicating no significant relationship between HRIS Information Security and Organisational performance of Commercial State Corporations in Kenya was rejected. From the study findings, it was recommended that organisations should keep a record of who is in charge of implementing the security agenda across the board and let all employees know about it. Information security policies, organisational internet usage policies, software management policies, and security expectations that align with the functions' tasks should all be explained to and covered in the training for employees.

APA CITATION

Kaaria, A. G. (2023). Human Resource Information Systems Information Security and Organizational Performance of Commercial State Corporations in Kenya. *East African Journal of Information Technology*, *6*(1), 256-278. https://doi.org/10.37284/eajit.6.1.1612

CHICAGO CITATION

Kaaria, Ann Gaceri. 2023. "Human Resource Information Systems Information Security and Organizational Performance of Commercial State Corporations in Kenya". *East African Journal of Information Technology* 6 (1), 256-278. https://doi.org/10.37284/eajit.6.1.1612.

HARVARD CITATION

Kaaria, A. G. (2023) "Human Resource Information Systems Information Security and Organizational Performance of Commercial State Corporations in Kenya", *East African Journal of Information Technology*, 6(1), pp. 256-278. doi: 10.37284/eajit.6.1.1612.

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

IEEE CITATION

A. G. Kaaria. "Human Resource Information Systems Information Security and Organizational Performance of Commercial State Corporations in Kenya", *EAJIT*, vol. 6, no. 1, pp. 256-278, Dec. 2023.

MLA CITATION

Kaaria, Ann Gaceri "Human Resource Information Systems Information Security and Organizational Performance of Commercial State Corporations in Kenya". *East African Journal of Education Studies*, Vol. 6, no. 1, Dec. 2023, pp. 256-278, doi:10.37284/eajit.6.1.1612.

INTRODUCTION

HRIS is described as a masterpiece of computer application, either self-contained or a group of programs, electronic structure information(database), information technology infrastructure (hardware and software) obligated to amass, preserve, manage, diffuse, purvey, and utilise data on Human Resource (Parry & Battista, 2019: Mauro & Borges-Andrade, 2020).Ahmer (2013) avers that the success of a firm is proportionate to a contemporary knowledge economy and the competency of the Human capital. Therefore, human capital management ought to be enhanced/boosted through creativity, innovations, and Information Technology. It is presumed that business establishments not only gain and sustain competitive advantages from the acceptance of information communication technology (ICT) but also utilize it to match other resources. Dery et al. (2009), further indicated that the most efficacious way of running global enterprises is through appropriate application of information technology (IT) in managing human resources. Dessler (2013) agrees that multinationals and global conglomerates are making rational advancements by expanding their company's human resource information systems (HRIS) to other subsidiaries and regional branches. A case in point where the management of Build net, Inc., in United States agreed to computerize and incorporate their discrete HRIS subsystems of applicant tracking, learning, and development as well as wage and salary administration, the company picked MyHRIS from NuView, Inc. which is an internet-based software package/ online solution to address its challenges. This web-based system encompasses employee salaries and other benefits administration, tracking interviewee applications, curriculum vitae scanning, administration of learning and development, career plans, talent management as well as succession planning.

MyHRIS had helped the managers in all of the firm's subsidiaries to evaluate and bring up-to-date more than 200 reports which are inbuilt and include summary terminations and unfilled positions in the organization. The company's management can also gain access to data and control worldwide human capital activities regularly. Parry and Tyson (2011) agreed that the overall outcome of e-HRM against the projected goals and objectives in UK-based firms established that even though the introduction of e-HRM led to increased efficiency, enhanced delivery of services, and normalization with roundabout transformational effects, there was a lack of evidence on increased employee participation in the decision-making processes within the organization. Similarly, a study by the Netherlands government prompted the approval and appreciation of the quality features of the content as the structure of electronic HRM applications had a meaningful and positive influence on strategic and technical HRM efficiency and effectiveness (Ruël, Bondarouk, & Van der Velde, 2007). This was later emphasized by Parry and Tyson (2011) in their investigation that established that e-HRM has culminated in more strategic decisions. It was not meant to necessarily lessen the process of HR headcount as HR practitioners could be redeployed from doing transactional to advanced strategic HR functions within their business establishments. Further than offering software solutions, business establishments need to invest in HRIS modules improves employee productivity by capturing their diverse capabilities, as well talents (talent mix). Richards-Carpenter (1989), as cited by Olughor (2016), quoted that forty percent of United States corporations had endorsed and invested in HRIS by the 1980s. Instantaneous

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

technological headway made in reference to globalization, volatility, uncertainty, complexity, and ambiguity in the business/work milieu has culminated into knowledge leaning units that call for newer and innovative technologies as well as enhanced knowledge management systems (Awad & Fairhurst, 2018).

Regional Perspective of Human Resource Information Systems

Many organizations still rely on sending parcels and other non-automated means of communication. As a consequence, the Human Asset Management function in many African enterprises in various countries has not been very proactive in the utilization of ICT through providing its assimilated services and conveying information effectively (Saaredra, 2010; Okeke-Uzodike & Chitakunye, 2014). Nonetheless, human resource planning has been one of the biggest challenges in the management of human assets for a long time. Reliable, well-timed, and information with minimal errors has over time been insubstantial and easily damaged, thus delaying decision-making meant to improve service delivery (Adeleye, 2011). Sungwa 2021 startlingly affirmed that numerous organizations in Africa are faced with numerous challenges (among them lack of top management support and financial/budgetary constraints) of substituting the traditional human resource management practices with electronic human resource management. A study done by Osei -Nyame and Boateng (2015) on the Adoption and Use of Human Resource Information System (HRIS) in Ghana also revealed that only 40% of Ghanaian firms have adopted HRIS meaning that much needs to been done to support and facilitate the adoption of the same. It was also apprehended a majority of the companies (that is about 95%) used the manual system in the management of their human resources. These firms included Small and Medium Enterprises as well as limited guarantee business establishment.

Many factions in various economies of Africa require up-to-date and accurate data on human resources to support the management of the same. Al Mamary, Shamsuddin & Aziati, (2014) affirm that operational and effective human resources information system (HRIS) help the organizational leadership in responding to crucial policy and management issues that affect the delivery of vital services in many business establishments. An effective, operational, and efficient information system makes sure that production, analysis, dissemination, and usage of dependable and well-timed information by organizational key individuals. This is made possible through an effective decision-making process at various levels of management which is coherent, articulate, and timely in all eventualities (Al Mamary et al., 2014).

Local Perspective of Human Resource Information Systems

In the global-based or centred economy, the socio-economic standards and productivity of businesses, organizations, and institutions of higher learning are highly influenced by the evolution of technology and digital services (Karua, 2017; Awad & Fairhurst, 2018).Cutting-edge technology allied to sentience, responsiveness, and readily available information aids in the establishment and increase in democracies invention, innovation, and production capacity which are significant to the economic growth of any country (Al Mamary, Shamsuddin & Aziati, 2014). The Kenyan government's strategic goal is to turn Kenya's economy into a principal place in place of business process outsourcing (BPO) and a worldwide ICT centre. This whole idea led to the creation of Kenya's ICT board in 2007 which is in line with Kenya's vision 2030 (Musimba, 2010).

Various actions and initiatives have been taken, to allow the populace to reach maximum technological levels. The government also recognizes IT as a chauffeur towards the empowerment of Kenyans socially and economically (GOK – Ministry of Information 2006). This demanded the formulation and implementation of a National ICT Policy resulting in the ratification and validation of National ICT policy, 2006. Consequently, Human resource

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

information systems have been adopted as the driving force behind the enhanced organizational performance. Muriithi et al., (2014) affirm that ICT acceptance and utilization in many enterprises have steered value addition in all businesses processes by stimulating the efficacy of transactional services and other administrative activities. Waters et al., (2013) posit that the health sector in Kenya continues to experience various challenges in the management of human resources for health (HRH) including an inadequate integer of competent employees and the distribution of employees in the health sector in various places. To antithesis these tendencies and enhance health service delivery, the Ministry of Medical Services (MOMS) and the Ministry of Public Health and Sanitation (MOPHS) have put in place the necessary strategies to mitigate the challenges faced in the development and management of human resources for health.

An all-inclusive human resources information system (HRIS) to support the function of human resources in the public health sector was implemented by the Ministry of Health. The HRIS, supported by the USAID-funded Capacity Kenya project, was amalgamated with present human resources (HR) and other health sector information systems. Currently, the HRIS is being instituted and inaugurated to cover all healthcare divisions in all counties in Kenya as a way of enhancing service delivery (Ministry of Health [MOH], 2015). Kenya's health professional regulatory agencies and ministry of health through the use of the following platforms, Integrated Personnel Payroll Database (IPPD), Kenya Health Workforce Information System (KHWIS), Regulatory Human Resources Information System (rHRIS), and Human Resource (HR) data systems, have been able to collect, store and retrieve health workforce data needed for proper regulation of the nursing workforce, deployment, payroll management, and other HR management data respectively. It, therefore, follows that in measuring the relationship between HRIS and organizational performance in commercial state corporations in Kenya, the researcher should be guided by amongst others; whether or not there is a need for enacting cost-cutting measures in the HR functional unit by ensuring that there is improved and correctness of HR stored data, service delivery, proper and regular training, and other organizational developmental initiatives (Waters et al., 2013).

Problem Statement

According to the 2013 Presidential Parastatal Reforms Report, there was a significant decline in the performance of commercial state corporations, as evidenced by their financial reports, which highlighted 21%, 23%, and 24% declines in performance in 2011/2012, 2010/2011, and 2008/2009 respectively. Studies by Mose (2017) and Murithi (2016) also affirmed that CSCs in Kenya have been performing abysmally due to ineffective leadership, governance, and management practices. Other signs of underperformance included dwindling levels of employee satisfaction, a performance management charter that was inappropriately linking individual performance to institutional performance as well as State Corporations' performance to national development goals, along with the institution's ability to recruit, invite, and retain skill sets necessary to drive performance (RPR, 2013; Kabiru et al., 2018). The upshot of this was an increase in stock debt – the total amount of debt a nation owes to all lenders – as well as a decline in shareholder confidence in CSC investments. Most empirical studies (e-HRM) have ignored the infrastructure and design aspects of HRIS and concentrated on the core functions of the human resource value chain (Ahmed, 2013; Bichanga & Aunga, 2015; Midiwo, 2015).

The impact of HRIS on the performance of public universities (Midiwo, 2015), the adoption of HRIS innovations in Pakistani organisations (Ahmer, 2013), and the impact of HRIS usage on employee performance (Yilmaz et al., 2016) are a few examples of empirical studies that have concentrated on direct relationships: however, the HRIS-organizational performance link can be influenced by other factors among them top management commitment with communication,

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

budgetary allocation, and policy development as well as execution (Mata et al, 2015; Bamel et.al., 2014; Kavanagh et al., 2012). In the Kenyan Context, a plethora of research surveys have been conducted on the organisational performance in Kenyan state corporations, such as Midiwo's (2015) study on the influence of human resource information systems on performance in Kenya public universities and Mukulu et al., (2015) study on the influence of management participation on the adoption of HRIS in Teachers Service Commission (TSC) operations in Kenya. This scenario prompted the researcher to evaluate the influence of HRIS information Security on organisational performance in Kenyan Commercial State Corporations.

Hypothesis

H_0: HRIS Information Security has no influence on the Organisational Performance of Commercial State Corporations in Kenya.

EMPIRICAL REVIEW

HRIS is described as a masterpiece of computer application, either self-contained or a group of programs, electronic structure information(database), information technology infrastructure (hardware and software) obligated to amass, preserve, manage, diffuse, purvey, and utilise data on Human Resource (Parry & Battista, 2019: Mauro & Borges-Andrade, 2020). It is also designated as Human Capital Management software (HCM) or Human Resource software. These configurations are miniature explicit presentations that incorporate distinctive management practices and procedures or a unified corporate management structural design that is executed on a huge scale (Mauro & Borges-Andrade, 2020). In addition, HRIS acceptance, utilisation, and usefulness can be expedited through key success elements, amongst them executive support and orientation for the acceptance of contemporary and innovative technologies, a well-fashioned business strategy for the execution of disruptive technologies besides the necessary ICT proficiency (Parry & Battista, 2019; Obeidat, 2018).

Al-Batashil and Dattana (2019) agree that the human resource information systems models that define its functionality include the HRIS Success Model, which brings together the systems quality, information quality, and easiness in use as well as its usefulness, the HRIS adoption model, which captures the human, technological, organisational, and environmental dimensions, in addition to the input-output model (Input subsystems, HRIS database, and the output subsystems). The human dimension outlines the innovativeness of the top management and employee IT capabilities, technological dimension details the IT infrastructure, compatibility, and intricacies of the system; the environmental dimension highlights competitive force, technology vendor support besides government regulations and support, and the organisational dimension which stipulates the relative advantage, top management support, perceived cost and ratification and validation of the said system (Liang et al., 2020; Kluemper et al., 2016).

Superior comprehensive data, managerial long-term plans, and strategic decision support systems can be made available through the strategic HRIS at the organisational level (Liang et al., 2020; Jani et al., 2021). Hasty globalism, consumerism, multiculturalism, hyper-competition, and unmatched technological advancement have contributed to extreme dynamism and complexity in the management of human capital (Parry & Battista, 2019). With these heightened challenges, companies must be innovative enough to respond to relentless business threats and pressures and lead-ins arising from the vivacious and competitive commercial sceneries globally (Ankrah & Sokro, 2016). The concept of managerial commitment and governance is gaining a novel dimension in the cybereconosphere of the fourth section of the digital insurgency age in which individuals began to understand the information time of life with attention drawn to e-government, e-commerce, Internet of Things (IoT), Cloud Computing as well as Big Data. A major realisation of digitally acknowledged standards for companies in their quest to arrive at and attain sustainable

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

competitive advantage is having a well-resourced and competent staff in the cyberspace and info stage, besides exhausting this key managerial resource successfully and proficiently (Noutsa et al., 2017). Firms need an efficacious Management Information System (MIS), which is acquiescent with all business procedures and developments and human resources, to be specific, for a speedy and opportune recital for the decision-making process, forecasting, modelling, and managerial processes. Management information system linked with human resources is described as the subsystem of Human Resources Information systems (Yilmaz et al., 2016).

Successful HRIS adoption and utilisation supported by the top management improves employee productivity at all echelons of management. The implementation phase takes into account the pursuit of a vendor process, planning and alignment endeavours headed by a navigation committee and senior employees from the human resource division, defining and designing, configuration and testing, training, and communication, as well as utilisation and sustainability which is primarily labelled as " going live".

State-owned enterprises, according to exist for a variety of purposes, including the following: first, to address market failures; second, to pursue social, economic, and political goals; third, to offer high-quality services for the public's health and education; and, fourth, to reallocate funds for the development of Kenya's rural areas. The number of Parastatals in Kenya was estimated by Getuno et al., (2015) to be 187, although the Report of the Presidential Taskforce on Parastatal Reforms of 2013 disputes this, citing a total of 262. A state corporation is defined as a body corporate established before or after the effective date of this Act by or under an Act, according to the State Corporations Act, Chapter 446 of the Kenyan Laws. It is also referred to as a company incorporated under the Companies Act of the Laws of Kenya that is not wholly owned or controlled by the Government or by a state corporation, a building society established in accordance with the Building Societies Act, and a cooperative society established under the Cooperative Societies Act.

According to the Guidelines on Terms and Conditions of Service for State Corporations (2017), public enterprises, regulatory organisations, executive agencies, public universities, tertiary education/training institutions, and research institutes are among the functional categories of state corporations. To carry out the objectives and initiatives set forth by the Kenyan Government for socio-economic development, State Corporations are established. Their founding ideologies include functional independence, manageability, an emphasis on outcomes, value for money, increased accountability, and openness in providing Kenyan citizens with services deemed difficult to obtain in the conventional government bureaucracy. The departments in these organisations are distinct from those in other government ministries. This falls under their conception, independence, orientation toward business and quasi-business, self-accounting philosophies, and accountability ("Report of the Presidential Taskforce on Parastatal Reforms", 2013).

What are the Components of Information Security and Cyber-Security?

The internet is the most often used resource for obtaining data and information in the twenty-first century. While 48% of people worldwide used the internet in 2017, the percentage of developed country residents who used it frequently climbed to 81%. The main purpose of the internet is to convey information from one node to another over the network. The development of mobile devices, networks, and computer systems has significantly expanded internet usage. The Internet is a global network comprising millions of unique computers, networks, and related devices that are connected for efficient data delivery. Information that is important and needs to be protected is contained in these data that were moved from one machine to another (Eze1, Ugwu & Ugwuanyi, 2023). Since information, in all of its forms, is an organization's most valuable asset, information

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

security flaws have the potential to endanger not just the integrity but also the very existence of organisations. Protecting the confidentiality, integrity, and availability of information is the main goal of information security (Chapple, Stewart & Gibson, 2018; Al-Matari, Helal, Mazen & Elhennawy, 2021). To achieve this, administration and governance are needed and data-driven performance measurement metrics must be used by organisations' IT governance, risk management, and compliance functions to make decisions (Vaibhav, 2022). The process of guarding against and controlling risks associated with the use, processing, storing, and transmission of data and information systems is known as information assurance, or IA. The safeguarding of user data's confidentiality, integrity, availability, authenticity, and non-repudiation is one of the Five Pillars of Information Assurance proposed by the U.S. Department of Defence (Infinit-O, 2018).

Although the phrases "Information security" and "Cybersecurity" are sometimes used synonymously, they differ slightly even if they have similar objectives. Both are essential parts of the overall security strategy of an organization. Cybersecurity is a broader term that encompasses the protection of systems, networks, and programs in the digital realm, including the internet. It involves safeguarding electronic data from theft, damage, or unauthorized access (Chapple, et.al., 2018). Cybersecurity is a multidisciplinary field that addresses a wide range of threats, from malicious hacking attempts to the protection of critical infrastructure. Information security, on the other hand, is a subset of Cybersecurity. It specifically focuses on the protection of information assets, regardless of the form they take (electronic, physical, or even human). Information security aims to ensure the confidentiality, integrity, and availability of data (Diamantopoulou, Tsohou, & Karyda, 2020).

Information infrastructure protection is aided by the interconnected concepts of cybercrime, cyber safety, network security, internet security, and information security. The safeguarding of information infrastructure depends upon these elements working together. Cybercrime is the term used to describe illegal activity conducted via networks, computers, and the internet. It includes many other types of illegal activity, such as ransom ware, phishing, hacking, and identity theft. Cybercriminals directly jeopardise information infrastructure because they exploit vulnerabilities in networks and systems to compromise data availability, confidentiality, and integrity. Cyber safety, on the other hand, refers to procedures and policies that guarantee the responsible and safe use of digital technology, including the internet. Its main goals are to raise awareness of online dangers and encourage responsible online behaviour among users, particularly young people and vulnerable populations. The defence of computer networks against intrusions, attacks, and disturbances is known as network security. To secure data in transit, it consists of steps like firewalls, intrusion detection/prevention systems, and encryption.

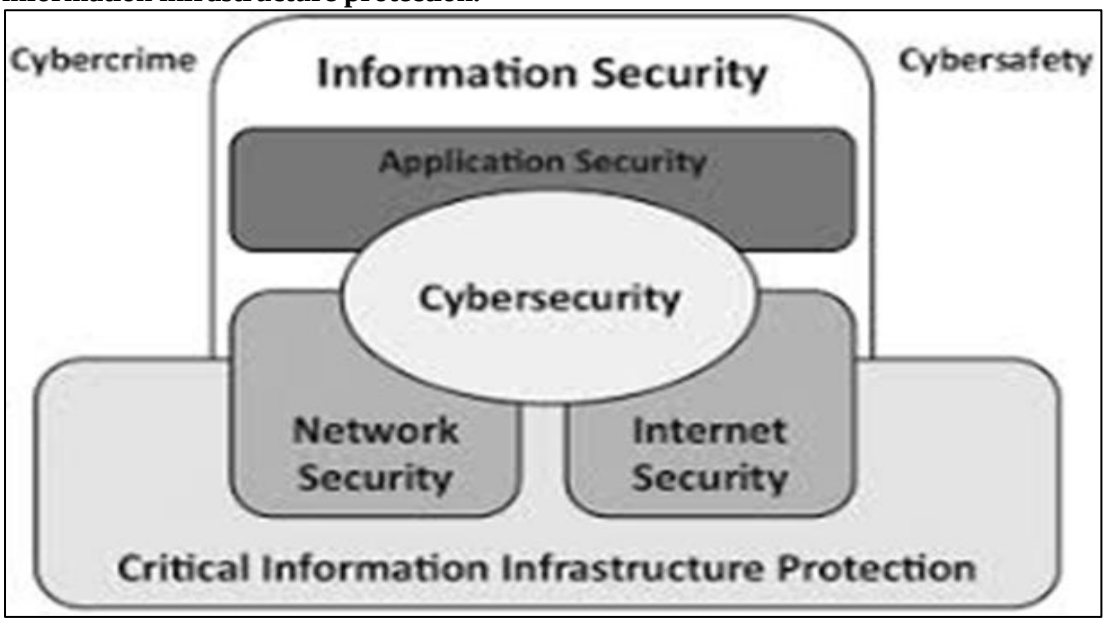
A fundamental component of information infrastructure protection is network security. Information may be transmitted and stored safely thanks to secure networks, which lower the possibility of unwanted access and data breaches. Internet security includes countermeasures against cyber-attacks for connected systems and data. Securing email accounts, web browsers, and online communication channels are all included in this. Network security and internet security are closely related; however internet security focuses on the online components of information infrastructure. It fixes flaws in internet-facing programmes and services (Dlamini, Eloff, & Eloff, 2009). Protecting information assets (data) against unauthorised access, disclosure, alteration, destruction, or disruption is known as information security. It includes methods, technology, and policies for data management and security. Network and internet security are included in the larger idea of information security. It covers the general safeguarding of data assets while they are in motion and at rest and incorporates safeguards including data backup, access limits, and encryption. Cyber safety

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

addresses the human dimension, which enhances other security components. Users that are informed and vigilant are less likely to become victims of cybercrimes and help create a safer online environment. Cybercrime draws attention to the risks, whereas cyber safety deals with user awareness. Information security guarantees the thorough safety of data throughout its lifecycle, while network and internet security offer technical means to safeguard the infrastructure. To effectively defend information infrastructure, a comprehensive strategy that incorporates these elements is essential (Von Solms and Von Solms, 2018). An organisation is engaging in cybersecurity if it deploys intrusion detection systems, firewalls, and encryption methods to safeguard its computer networks and systems against online threats such as malware and hacking attempts. Information security is practised by the same company if it uses encryption, access controls, and secure storage methods to safeguard private client data kept in databases (Awad & Fairhurst,2018). Cybersecurity includes safeguarding a company's website or network infrastructure from distributed denial of service (DDoS) attacks. This entails taking steps to guarantee the accessibility and appropriate operation of online services. Information security includes things like making sure that a customer's financial information is kept private and unaltered while doing online transactions. This entails safeguarding the confidentiality and integrity of certain data (Von Solms & Von Solms, 2018).

Dlamini, Eloff, & Eloff, (2009) argued Cybersecurity includes informing staff members about the risks associated with phishing scams and putting policies in place to stop illegal access through social engineering. Information security includes things like enforcing stringent access restrictions to prevent employees from accessing sensitive databases and making sure private information is handled properly. However, there is a lack of defined cybersecurity and Internet governance from organisational, national, and international/global levels with this push for ubiquitous Internet access and widespread usage of digital services (Diamantopoulou, Tsohou & Karyda, 2020). For instance, senior management at companies has not given cybersecurity a comprehensive consideration despite their growing awareness of cyber threats, security, and the significant risks to people and organisations. This is because they believe that cybersecurity is the exclusive domain of the information technology department and its employees (Nolan, Lawyer & Dobb, 2019; Vaibhav, 2022).

Figure 1: Links between network security, information security, cybercrime, cyber safety, and information infrastructure protection.



Source: Von Solms and Von Solms (2018)

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

Information security, industry, the Internet of Things (IoT), legal and regulatory developments, cyber security culture, and digitalization all interact in intricate ways that are vital to the changing face of technology-driven settings (Eze1, Ugwu & Ugwuanyi, 2023). Digitalization can be described as the process of incorporating digital technologies into different facets of society and business. By utilising technology like cloud computing, big data analytics, artificial intelligence (AI), and automation, digitalization brings about revolutionary changes in the industrial context. Digitalization is being adopted by industries more and more to improve productivity, creativity, and competitiveness (Quaosar & Rahman, 2021). When it comes to digital transformation, industries are leading the way. They use cutting edge technologies to improve decision-making, streamline operations, and develop cutting-edge goods and services. The Fourth Industrial Revolution, or Industry 4.0, refers to the continuous transformation of traditional manufacturing and industrial practises through the integration of digital technologies, advanced analytics, the Internet of Things (IoT), cloud computing, artificial intelligence (AI), and other emerging technologies. Industry 4.0 is popularly known as the integration of digital technologies in industry. Smart factories, predictive maintenance, and optimised supply chains are the results of this paradigm shift towards smart, linked systems that can function more effectively, react to changes, and create new opportunities for innovation (Vaibhav, 2022).

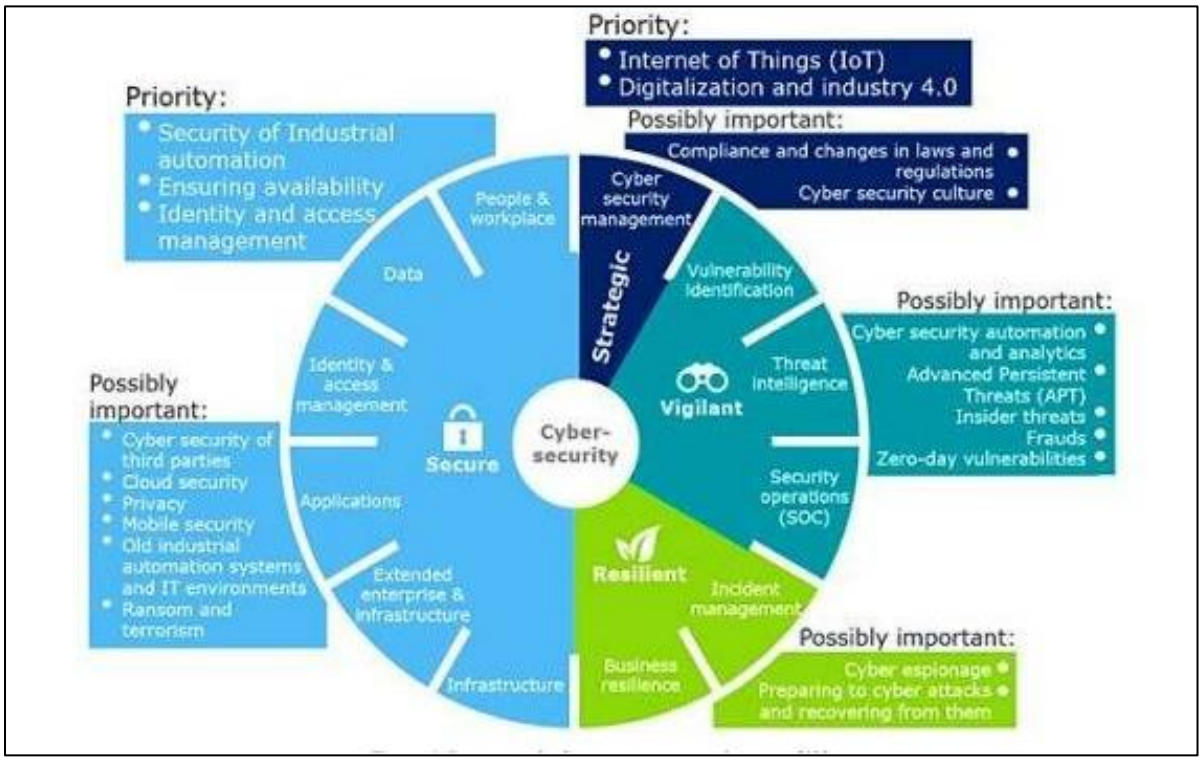
Nolan, Lawyer, & Dodd, (2019) affirm that an interconnected network of things and gadgets that exchange data and communicate with one another is referred to as the IoT. IoT is essential to the industrial sector because it makes real-time information sharing between machines, systems, and processes possible. In industrial contexts, this connectivity improves automation, efficiency, and data-driven decision-making. The quick speed at which technology is developing and digitising society calls for constant revisions to legal and regulatory frameworks. Laws are being modified by governments and international organisations to handle new issues pertaining to cyber security, data privacy, intellectual property, and ethical issues (Al-Matari, Helal, Mazen, & Elhennawy, 2021). In order to reduce legal risks and foster confidence, firms must adhere to these changing regulations. Organisations must have a robust cyber security culture in place to safeguard sensitive data and digital assets. It entails promoting knowledge, instruction, and a sense of shared accountability for cyber security procedures among staff members. Prevention of security breaches, efficient incident response, and adaptation to changing cyber threats are all made possible by a healthy cyber security culture. Information security includes methods and techniques to safeguard data's availability, confidentiality, and integrity. Data volume and relevance expand considerably with increasing usage of IoT and digitalization. Strong information security procedures are necessary to protect data from breaches, illegal access, and other online dangers (Eze1, Ugwu & Ugwuanyi, 2023).

These elements have interconnected ties with one another. Industry transformation is fueled by digitalization, which incorporates IoT technology to build environments that are data-rich and networked. The need for information security and a cyber-security culture to fend off emerging cyber threats is heightened by this greater connectedness (Anass, Assoul, Ouazzani & Roudies, 2020). Modifications to laws and regulations influence how businesses handle cyber security and information security by providing a framework for the ethical and lawful use of digital technologies. In addition to being required by law, adhering to these regulations helps to establish confidence among stakeholders and customers. The modern technological environment is based on the intersection of digitalization, industry, IoT, legal and regulatory developments, cyber security culture, and information security. Businesses that carefully traverse and include these components will be in a better position to prosper in the digital age, properly controlling risks and guaranteeing the

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

security of vital data (Awad & Fairhurst, 2018; Ankrah & Sokro, 2016).

Figure 2: Describes the intricate relationship or interplay between digitalization, industry, the Internet of Things (IoT), legislative changes, cyber security culture, and information security which is pivotal in shaping the dynamic landscape of technology-centers



Source: Eze1, Ugwu & Ugwuanyi (2023). Kiu Publication Extension

Human resource management (HRM) has seen a general shift in its role from traditional (also known as personnel management) to a strategic one, according to Quaosar & Rahman, 2021. HRIS describe the integration of IS and HRM. In contemporary organisations, one of the greatest neoteric HR tools is HRIS. It gained popularity at the start of the current century in wealthy nations. But since this decade, very few MNCs and business organisations in poor nations like Bangladesh have begun to adopt and use HRIS. However, only a small number of medium-sized to large-sized organisations have adopted and used it. The main goals of the study were to identify the uses of human resource information systems (HRIS) and the results that results from different types of enterprises. The important information regarding the main obstacles to HRIS adoption was taken as alternative goal line of this investigation. Lastly, it discusses how to acquire knowledge about HRIS and the extent to which it can be extended thus provided the basis for this study.

THEORETICAL REVIEW

Contingency Theory

The contingency theory, which holds that many organisations today are shaped by their work contexts, as supported by Cole and Kelly (2015). Every organisation is assumed to have a unique collection of internal and external limitations that impact it (Kavita, 2010). Fred Edward Fielder put forth this hypothesis in his seminal article titled "A Contingency Classical Model of Leadership Effectiveness", which was released in 1964. The essential idea in the contingency proposition is congruence or fit or a good fit, flanked by the internal structure of the company and its business environment. Since the middle of the 1960s, contingency theory has dominated the research on general enterprises' performance. According to

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

Browning et al. (2009), contingency theory is frequently characterised from the standpoint of open systems. The idea nevertheless emphasises the requirement for flexibility. According to Belcourt and McBey (2010), the contingency theory is based on the idea that no single method exists for managing businesses. The strategy contends that there are numerous strategies for delivering good leadership and management in businesses (Mullin, 2010). According to the structural contingency theory, there is no ideal strategy to harmonise, guide, and improve decision-making processes. Instead, the ideal itinerary depends on both internal and external organisational circumstances. Setting up a support structure in advance for use in an emergency is called contingency.

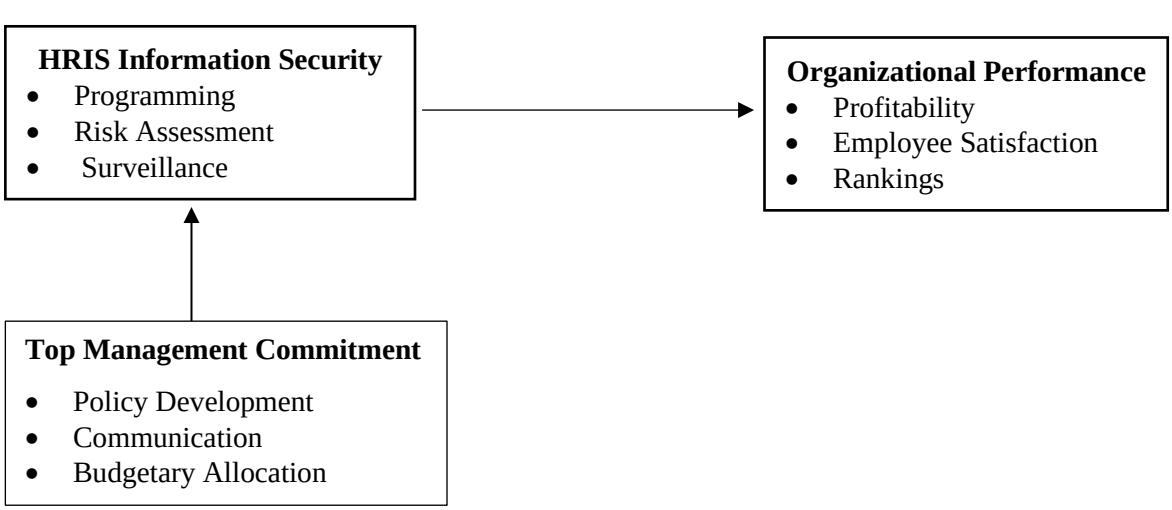
According to structural contingency theory, firms and commercial establishments should have a plan to promote change as necessary. It emphasises that each business establishment must make modifications to ensure that they are operating in well-organised structures for the sustainability of the business and that a firm's structure must be flexible for every business organisation (Shala et al., 2021; Reinking, 2012). When running any business enterprise, contingent frontrunners are nimble when choosing and adapting to laconic tactics that bring together changes in the state of affairs in a certain period. According to contingency philosophers, information security management is a component of contingency administration and control that aims to identify, prevent, and mitigate dangers, pressures, and susceptibilities, as well as shifts inside and outside of any commercial firm. In order to protect only their information communication technology (ICT) equipment, services, data, and information, enterprises should also focus on cybercrime upsurges and impulsive natural adversities. Businesses worldwide cannot predict when natural disasters or security breaches will occur, according to Reinking (2012). However, companies must develop a plan that monitors the frequency of security breaches in order to help lessen the effects. This posture might be thought of as a contingency plan for cyber security. A laid-out risk management document that provides strategies, recommendations, worries, and considerations of a business entity on how to recover its ICT information, services, and data in the event of a safety violation, adversity, or system distraction is known as a cyber-security contingency strategy. Its principal goal is safeguarding data, assets, and information following a security breach or catastrophic event. Similarly, it continues to support techniques that aid in gathering and preserving information and developing a root cause inspection or examination (Shala, Prebreza & Ramosaj, 2021).

Commercial State Corporations operate under open systems that strongly emphasise the connections between an organisation and the environment in which it operates to achieve the vital goals necessary for their continuing existence. These organisations are open systems that rely on outside knowledge and resources (including human and financial resources, among others) to flourish (Jaafreh, 2017). According to Mullin (2010), the effectiveness of this theory is attributable to the numerous research investigations that have established the validity of the various linkages between internal integration and unforeseen events (contingencies) in businesses today. The ability of state corporations in Kenya to use the available resources effectively while taking into account the contingencies in the environment they operate in, under top management commitment that recognises that not a single situation fits all, assists in improving their chances of survival and organisational performance. As a result, this study's conceptual framework is founded in part on the contingency theory and linkages between top management commitment, human resource information systems, and performance. In recognition of the fact that organisations are influenced by their environments, which include age, technology, size, and organisational culture, and do not operate in a vacuum, it continues to tie the variable of information security, a necessity in the acceptance and effective operationalisation of HRIS. As a collection of interconnected parts, with technology as one of them, many businesses

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

also adopt open systems (Shala et al., 2021). Information security is required where technology is present to protect sensitive and important organisational data from rivals and other interested parties.

Figure 3: Conceptual framework



On the Relationship to Programming, Risk Assessment, Surveillance, and HRIS information Security, the combined efficacy or effectiveness of risk assessment procedures, secure programming, surveillance, and HRIS security mechanisms affects an organization's overall performance. The dependability of HR operations is improved by a secure HRIS, which boosts overall organisational effectiveness. On the other hand, subpar risk management, insufficient monitoring, or HRIS security have a detrimental influence on performance of any given organization. There is a mutually contingent relationship between programming, risk assessment, surveillance, information security, and organisational effectiveness in human resources. Ensuring the confidentiality, integrity, and availability of HR information through a comprehensive approach that incorporates these factors eventually aids the organisation in accomplishing its objectives and upholding stakeholder confidence.

Top management's dedication guarantees that budgetary allocation, policy creation, and communication initiatives are coordinated. A thorough strategy incorporates these elements into an all-encompassing HRIS security plan. On Comprehensive Security Posture, policies are more than simply written documents when senior management is dedicated to HRIS information security. They are actively enforced, backed by sufficient resources, and successfully disseminated to all relevant parties. The relationship between HRIS information security and other elements including policy creation, financial allocation, and communication is largely dependent on the commitment of senior or top management. It ensures that security measures are not only established but also successfully carried out and maintained throughout time. It also sets the tone for an organisational culture that is security-conscious. This pledge is necessary to protect confidential HR information and uphold the HRIS's general integrity and reliability.

Conceptual Framework

Figure 3 shows the conceptual framework adopted in the study.

RESEARCH METHODOLOGY

Using a census method, the population was drawn from 55 Commercial State Corporations in Kenya. The units of observation were the managing directors or chief executive officers, directors of human resources, and deputy directors of human resources being the authorities

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

in HRM-related concerns. The study used both qualitative and quantitative methods to collect primary and secondary data. Data was collected from 147 respondents as the target population was equals to sample size. Questionnaires and interviews were used to collect data for the study, which was supplemented by secondary sources. SPSS version 23.0 was used to analyse data using descriptive analysis, factor analysis, Pearson correlation, analysis of variance (ANOVA), and regression.

FINDINGS AND DISCUSSION

Response Rate

The number of questionnaires that were administered to Pure Commercial State Corporation and Strategic Commercial State Corporation were 147. Response rate results were presented as shown in *Table 1*.

Table 1: Response rate

Questionnaires	Frequency	Percentage (%)
Responsive	110	74.83
Non-Responsive	37	25.17
Total	147	100

A total of 110 were properly filled and returned. This represented an overall successful response rate of 74.83 %, as shown in *Table 1*. This agrees with Babbie (2016), who affirmed that return rates of 50% are acceptable to analyse and publish, 60% is good, and 70% is very good. Based on this affirmation, a 74.83 % response rate was statistically acceptable.

Descriptive Results

The objective of the study was to establish the influence of HRIS Information Security on Organisational Performance in Commercial State Corporations in Kenya. A 5-point Likert scale with options of strongly disagree, disagree, neutral, agree, and strongly agree were presented for answering by respondents. The results were presented in the form of percentages, mean and standard deviations.

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

Table 2: Descriptive Results for HRIS information security

Statement	SD	D	N	A	SA	Mean	SD
The HRIS is well-designed, and employees are adequately trained to avoid security breaches due to human error	7.60	12.60	21.80	24.40	33.60	3.64	1.27
There are measures to protect HRIS from security problems as a result of damage by employees	7.60	10.10	22.70	29.40	30.30	3.65	1.23
There are safeguards for misuse of computer systems as a result of unauthorised access	7.60	2.50	30.30	30.30	29.40	3.71	1.14
There are measures to guard against information theft from HRIS	8.40	13.40	16.80	37.00	24.40	3.55	1.23
HRIS in this organisation has safeguards against computer-based fraud	11.80	11.80	18.50	24.40	33.60	3.56	1.37
Ways of dealing with security threats by viruses, worms and trojans are in place	10.10	10.10	10.10	21.80	47.90	3.87	1.38
There are security features to ward off hackers	10.10	24.40	8.40	19.30	37.80	3.50	1.45
There are safeguards against proofing and sniffing	10.10	10.10	21.80	14.30	43.70	3.71	1.38
Average						3.65	0.97

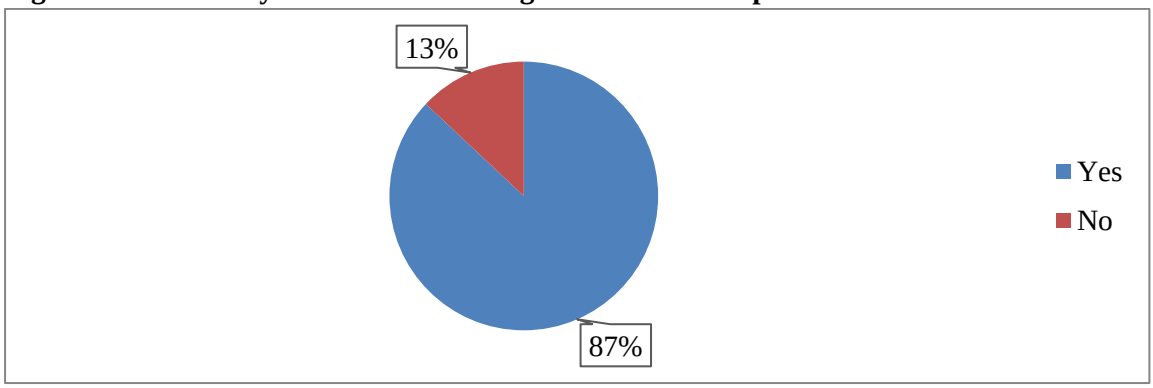
Article DOI: https://doi.org/10.37284/eajit.6.1.1612

The result revealed that most respondents agreed with the statement that the HRIS is well-designed and maintained, and employees are adequately trained to avoid security breaches due to human error (*M* = 3.64). The standard deviation was 1.27, implying that the answers were varied from the mean. The result revealed that most of them agreed with the statement that there are measures to protect HRIS from security problems due to damage by employees (*M* = 3.65). The standard deviation was 1.23, implying that the answers were varied from the mean. The result revealed that the majority of the respondents agreed with the statement that there are safeguards for computer system misuse due to unauthorised access to or use of information, particularly when it is confidential and sensitive (*M* = 3.71). The standard deviation was 1.14, suggesting that the answers varied from the mean. 120 The result revealed that most respondents agreed with the statement that there are measures to guard against information theft from HRIS (*M* = 3.55). The standard deviation was 1.23, deducing that the answers were varied from the mean.

These findings were consistent with that of Chen et al. (2011), who found out that protecting organisational information is an essential element of a company's security policy formulation and implementation, and in many countries, it is a legal requirement and part of corporate social responsibility. The result revealed that most respondents agreed with the statement that HRIS in this organisation has safeguards against computer-based fraud (*M* = 3.56). The standard deviation was 1.37, implying that the answers were varied from the mean. These findings agree with that of Kavanagh et al. (2012), who assert that when large amounts of data are stored in electronic form, they are vulnerable to many more kinds of threats than when they exist in manual form. The result revealed that most respondents agreed with the statement that ways of dealing with security threats by viruses, worms and Trojans are in place (*M* = 3.87). The standard deviation was 1.38, suggesting that the answers varied from the mean.

The result showed that most respondents agreed with the statement that there are security features to ward off hackers (*M* = 3.5). The standard deviation was 1.45, implying that the answers varied from the mean. Finally, the result revealed that the majority of the respondents agreed with the statement that there are safeguards against spoofing and sniffing (*M* = 3.71). The standard deviation was 1.38, implying that the answers varied from the mean. These results concur with those of Chen et al. (2011), who argue that protecting organisational information is an essential element of a company's security policy, and in many countries, it is also a legal requirement and part of corporate social responsibility. On a five-point scale, the average mean of the responses was 3.65, which means that most respondents indicated that they agreed with the statement; however, the answers were varied, as shown by a standard deviation of 1.31. In addition, the respondents were asked to indicate if measures were put in place to mitigate loss and disruption of information in the human resource information system in case of natural disasters. Results are presented in *Figure 2*.

Figure 4: Availability of measures to mitigate loss and disruption of information in the HRIS



Article DOI: https://doi.org/10.37284/eajit.6.1.1612

Figure 2 above revealed that the majority of the respondents (87%) indicated that there were measures put in place to mitigate loss and disruption of information in the human resource information system in case of natural disasters, while only (13%) of the respondents disagreed with the statement. These findings were consistent with that of Chen et al. (2011), who found that protecting organisational information is an essential element of a company's security policy, and in many countries, it is also a legal requirement and part of corporate social responsibility.

From the interviews, a content analysis was carried out on the questions from the interview guide that were based on the information security of the organisations. This sought to further assess the status of the phenomenon of information security of the firms based on qualitative information gathered from interviews. Content analysis was based on a thematic analysis approach where themes on Information Security were sought from the qualitative responses given by the interviewees, coded and the frequency of occurrence of the coded themes assessed and reported in frequency tables. *Table 3* summarises the coded themes resulting from content analysis of Information Security.

Table 3: Content analysis

Themes	Frequency	Percentage
Back up	78	71.4%
No Back Up	6	5.0%
Maintenance	26	23.6%
Total	110	100%

The majority of the respondents 95% (71.4% +23.6%) consented that there were measures to mitigate loss and disruption of information in the human resource information in case of natural disasters, while only 5% of the remainder indicated no measures to mitigate loss and disruption of information in the human resource information in case of natural disasters. This implies that the organisation is well equipped for eminent natural disasters, which is very vital for any organisation. The respondents were asked to indicate if there were any challenges in regard to job security. *Table 4* summarises the coded technology adoption themes resulting from content analysis of Information security.

Table 4: Challenges in regard to Job Security

Themes	Frequency	Percentage
Adopting technology will render employees jobless	70	63.9%
Initial stages challenges	30	26.9%
No challenges	10	9.2%
Total	110	100%

The majority of the respondents (63.9%) indicated that adopting technology is a challenge since it will render employees jobless. Another (26.9%) of the respondents indicated that there are challenges in the initial stages, while the remaining (9.2%) of the respondents indicated that there are no challenges faced. This implies that most employees of Commercial State Corporation face challenges in their work environment.

Correlation Analysis

The researcher performed a correlation analysis between HRIS Information Security Organisational Performance in Commercial State Corporations in Kenya. The results are displayed in *Table 5.*

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

Table 5: Correlation Analysis

		HRIS Info Security	Performance
HRIS Information Security	Pearson Correlation	1	
	Sig. (2-tailed)		
Organizational Performance	Pearson Correlation	.508**	1
	Sig. (2-tailed)	0.000	

The results show a positive and significant correlation between HRIS information security and organisational performance in Commercial State Corporations in Kenya (r=0.508, p=0.000). These findings were consistent with that of Chen & Hsiao (2012), who found out that organisational information protection is an essential element in the company's security policies. In most countries globally, it is a legal requirement and a constituent of corporate social responsibility.

Regression Analysis

Regression analysis was conducted to show the influence of HRIS information security on organisational performance in Commercial State Corporations in Kenya. The results are shown in *Table 6.*

Table 6: Model Summary

Variable	R	R Square	Adjusted R Square	Std. Error of the Estimate
Coefficient	.508[a]	.358	.251	.865

a. *Predictor: HRIS Information Security*

Information Security was found to be a satisfactory variable in explaining performance. This is supported by the coefficient of determination, also known as the R square, of 35.8%. This means that information security explains 35.8% of the variations in the dependent variable, which is organisational performance. This also implies that 64.2 % of the variation in the dependent variable is attributed to other variables not captured in the study. These findings agreed with that of Palmer et al. (2009), who found out that protecting organisational information is an essential element of a company's security policy, and in many countries, it is also a legal requirement (cyber-security laws) and part of corporate social responsibility.

Table 7: ANOVA

	Model	Sum of Squares	df	Mean Square	F	Sig.
1	Regression	30.413	1	30.413	40.626	.000[b]
	Residual	87.587	117	0.749		
	Total	118.000	118			

a. Dependent variable: Organizational Performance
b. Predictors: HRIS Information Security

Table 7 provides the results of the analysis of the variance (ANOVA). The results indicate that the model on the direct influence of information security on organisational performance was significant, as supported by a p-value of 0.000, which is less than the level of significance of 0.05. The direct bivariate influence of HRIS Information Security on organisational performance was thus found to be significant in this study; however, this agrees with the findings of Palmer et al. (2009), who found that protecting any firm's information an integral constituent of a company's security policy and in many countries, it is also a legal requirement and part of any given organisation's corporate social responsibility.

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

Table 8: Regression Coefficients

Variables	β	Std. Error	t	Sig.
(Constant)	-5.96E-007	0.079	0.000	0.001
HRIS Information Security	0.508	0.080	6.374	0.003
Dependent variable: Organizational Performance				

Regression coefficients showed that HRIS system quality has a positive, significant, and direct influence on organisational performance (β=0.508, t=6.374, p=0.000). These findings agreed with that of Palmer et al. (2009), who found out that protecting any firm's information is an integral constituent of a company's security policy, and in many countries, it is also a legal requirement and part of any given organisation's corporate social responsibility.

$Y = 0.508X + e$

Where X is HRIS information security while Y is organisational performance, these findings agreed with that of Beadles et al. (2015), who found that confidentiality of employees' data builds trust, confidence, and loyalty among the stakeholders (employer, employee, and business owners) which ultimately enhances employee productivity.

Hypothesis testing for HRIS Information Security and Organizational Performance

The hypothesis stated that HRIS information security does not significantly influence the organisational performance of Commercial state cooperation in Kenya. The results revealed that Fcal (40.626)> Fcritical (3.94), and thus, the null hypothesis was rejected. The results further indicated that the t cal (6.374) > t critical (1.96). Therefore, the study concluded that HRIS information security significantly influences the Organisational Performance of Commercial State Corporation in Kenya.

SUMMARY, CONCLUSIONS AND RECOMMENDATION

Summary of Findings

The descriptive analysis results showed agreement on the security and privacy of the organisational information as all the indicators had high scores above 3.0. The result revealed agreement by the respondents that HRIS is well designed and maintained and employees adequately trained to avoid security breaches due to human error. There was also agreement that the organisations have measures to protect HRIS from security problems as a result of damage by employees and have put in place safeguards for misuse of computer systems as a result of unauthorised access to or use of information, particularly when it is confidential and sensitive. The correlation results indicated that information security has a positive significant relationship with organisational performance. The regression results further revealed that information security significantly influences Organisational Performance in Commercial State Corporations in Kenya.

Conclusion

For successful and effective managerial decision-making, it is necessary to provide accurate, timely and relevant information to decision-makers who are also the policymakers. Moreover, management information system improves information quality and consequently improve efficacy in the managerial decision-making process. Protecting the firm's information is a vital element of the organisation's security policy, a legal requirement. From the study, it was concluded that the common security threats are human errors, where an HRIS is not well designed, developed and maintained. Where employees are also not adequately trained, there is a high potential threat of security breaches. In addition, the study concluded that HRIS information security has a significant influence on organisational performance in commercial state corporations in Kenya. The study regression analysis results were used to test the hypothesis that HRIS Information security has no significant

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

influence on the organisational performance of Commercial State Corporations in Kenya. The p-value of the coefficient estimate was found to be less than 0.05; thus, the null hypothesis was rejected, and a conclusion was drawn that HRIS information security has a significant influence on the organisational performance of Commercial State Corporations in Kenya. When private information about the workforce, business partners, or customers could fall into the hands of competitors, such a breach of security may lead to business losses, lawsuits, bankruptcy or winding up of the company.

Recommendation

Every firm needs an information security policy, which should not just be a blueprint capturing its motivation, goals, applicability, and relevance, among other things. Additionally, organisations should keep a record of who is in charge of implementing the security agenda across the board and let all employees know about it. Information security policies, organisational internet usage policies, software management policies, and security expectations that are in line with the tasks of the functions should all be explained to and covered in training for employees. Monitoring the adoption of policies and procedures through employee attestation is essential because it offers valuable feedback on the methods for enforcing and educating about the policy document. A specific role policy, such as one on enterprise software management, should be scoped and scanned, considering appurtenant personnel, including those from the IT Systems department, and being disseminated, reviewed, and acknowledged by all employees. The HRIS system should be regularly updated and upgraded to newer technology, according to management. They should also set up a committee to create and carry out policies for managing information security. Additionally, it should support and encourage organisational-level system surveillance and risk assessment measures. The Data Protection Acts of 2019 and the national cyber-security policy, which offer strategic interventions for tackling national cyber-security concerns and threats, should be enforced and strengthened by the Government. On the other hand, the Government should promote information security and hold ongoing efforts to raise awareness of its significance.

REFERENCES

Adeleye, I. (2011). Theorizing Human Resource Management in Africa: Beyond Cultural Relativism. *African Journal of Business Management*, 5 (6) 2028-2039.

Ahmer, Z. (2013). Adoption of Human Resource Information Systems Innovations in Pakistan Organizations. *Journal of Quality and Technology Management*, 9(2) 25-50.

Al-Batashil, F., & Dattana, V. (2019). Effectiveness and Implementation of HRIS: A Case Study of the AL Tameer Star Company (TS*). Journal of Engineering Science*, 10(12)

Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. *Information Security Journal: A Global Perspective*, 30(4), 189–204. https://doi.org/10.1080/19393555.2020.1834649

Al Mamary, Y. H., Shamsuddin, A., & Aziati, N. (2014). Factors Affecting Successful Adoption of Management Information Systems on Organizational Performance. *American Journal of Systems and Software*, *2*(5), 21-126

Ahmer, Z. (2013). Adoption of Human Resource Information Systems Innovations in Pakistan Organizations. *Journal of Quality and Technology Management, 9(2)* 25-50.

Anass, R., Assoul, S., Ouazzani, T. K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information and Computer Security*, 28(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Ankrah, E., & Sokro, E. (2016). Intention and usage of Human Resource Information

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

Systems among Ghanaian human resource managers. *International Journal for Business Management*, 11(1) 241–248

Awad, A.I. & Fairhurst, M (2018*). Information Security, Foundation, Technologies, and Applications.* London, United Kingdom: The Institute of Engineering and Technology.

Babbie, E. (2016). *The Practice of Social Research* (14th ed.). Belmont, California: Wadsworth Cengage.

Bamel, N., Bamel, K. U., Sahay, V., & Thite, M. (2014). Usage, Benefits, and Barriers of Human Resource Information Systems in Universities. *Journal of information and knowledge management systems,* 44(4).

Beadles, N. A., Lowery, C. M., & Johns, K. (2015). The Impact of Human Resource Information Systems: An Exploratory Study in the Public Sector. *Journal of Communications of the IIMA*, *5*(4), 56 – 147.

Belcourt, M., & McBey, K. (2010). *Strategic Human Resources Planning*, Boston, U.S.A: Cengage.

Bichanga, W.O., Aunga, C. N. (2015). The Influence of Human Resource Information Systems on Service Delivery in Kenya's Telecommunication Industry (A Case of Safaricom Kenya Ltd). *International Journal of Social Sciences and Information Technology*, 1(2).

Browning, V., Edgar, F., Gary, B., & Garret, T. (2009). Realising Competitive Advantage through Human Resource Management in New Zealand Service Industries. *The Service Industrial Journal,* 29(6), 741- 760

Chen, R. F., & Hsiao, J. L. (2012). The effects of Project Management Information Systems on decision making in Multi-Project Environment. *International Journal of Project Management,* 30(2), 162-175

Chen, S., Li, S., & Li, C. (2011). Recent related research in Technology Acceptance Model: A literature review. *Australian Journal of Business and Management Research,* 1(9), 124-127.

Cole, G.A., & Kelly, P. (2015). *Management theory and practice*. (8th ed.). Boston, U.S.A: Cengage.

Dery, K., Grant, D., & Wiblen, S. (2009). Human Resource Information Systems: replacing or enhancing HRM. *Proceedings of the 15th World Congress of the International Industrial Relations Association IIRA.* Sydney.

Dessler, G. (2013). *Human resource management* (13th ed.). New Jersey, U.S.A: Prentice hill.

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC27001: 2013 and ISO/IEC27002: 2013 to GDPR compliance controls. *Information and Computer Security*, 28(4), 645–662. https://doi.org/10.1108/ICS-01-2020-0004

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information Security: The moving target. *Computers & Security*, 28(3–4), 189–198. https://doi.org/10.1016/j.cose.2008.11.007

Eze1. V. H. U, Ugwu. C. N., & Ugwuanyi. I. C. (2023). *A Study of Cyber Security Threats, Challenges in Different Fields, and its Prospective Solutions: A Review*. INOSR Scientific Research 9(1):13-24. https://www.researchgate.net/figure/Priorities-of-cyber-security-in-manufacturing-15_fig1_367742804

Getuno, P.M., Awino, B. Z., Ngugi, P.K., & Mwaura, F.O. (2015). Public-private partnership regulations (2009) implementation and organisational performance of Kenyan state corporations. *International Journal of Information Research and Review*, 2(2), 433-440.

Infinit-O. (2018). The Five Pillars of Information Security and How to Manage Them. https://resourcecenter.infinit-o.com/blog/the-5-pillars-of-information-security-and-how-

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

to- managethem/#:~:text=The%20U.S.%20Department%20of%20Defense,non%2Drepudiation%20of%20user%20data.

Jani, A., Muduli, A., & Kishore, K. (2021). Human Resource Transformation in India: Examining the role digital human resource technology and human resource role. *International Journal of Organizational Analysis.* 1934-8835

Jaafreh, A. B. (2017). Evaluation Information Systems Success: Applied Delone and Mclean Information Systems in Context Banking System in KSA. *International Review of Management and Business Research, 6*(2).

Kabiru, F. C., Theuri, M. & Misiko, A. (2018). The influence of leading on the organizational performance of agricultural state-owned corporations in Kenya. *International Academic Journal of Innovation, Leadership and Entrepreneurship, 2*(2), 1-16

Kavanagh, M. J., Thite, M., & Johnson, R. D. (2012). *Human resource information systems: Basics, applications & directions.* Boston, U.S.A: Sage

Kavita, S. (2010). *An Analysis of the Relationship between the Learning Organization and Organization Culture, Human Resource Management, High Commitment Management, and Firm Performance*. Otago Graduate Review, 8, 57-68.

Kluemper, D.H., Mitra, A., & Wang, S. (2016). *Social Media Use in Human Resource Management: Research in Personnel and Human Resource Management*. Bingley, England: Emerald

Liang, X., Xiu, L., Fang, W., & Wu, S. (2020). How did a local guerrilla turn into a global gorilla? Learning how transformational change happened under dynamic capabilities from the rise of Huawei. *Journal of Organizational Change Management* 33(2), 401-414.

Mata, F. J., Fuerst, W. L., & Barney, J. B. (2015). Information Technology and Sustained Competitive Advantage: A Resource-Based Analysis. *MIS*, 12(23), 112 – 576.

Mauro, G.T., & Borges-Andrade, E.J. (2020). Human Resource System as innovation for organisations. *Innovation and Management Review* 17(2), 197- 214.

Midiwo, J. (2015). *Influence of Human Resource Information Systems on the Performance of In Kenyan Public Universities.* [Doctoral thesis, Human Resource Management, Jomo Kenyatta University of agriculture and technology, Nairobi, Kenya].

Ministry of Health (2015). *Devolved Human Resource Management Policy Guidelines on Human Resource for Health*. Nairobi, Kenya: Government Printer.

Mose, T. C. O. (2017). *Role of Corporate Culture on the Performance of Commercial State Corporations in Kenya.* [Doctoral Thesis, Human Resource Management, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya].

Mukulu, E., Karanja, K., & Warui, C. (2015). The Influence of Management Participation on Adoption of Human Resource Information Systems in Teacher's Service Commission (TSC) Operations in Kenya. *Journal of Academic Research in Business and Social Sciences*, 5(2) 46-60.

Mullin, L.J. (2010). *Management and Organizational Behaviour* (9th ed) London, England: Pearson.

Muriithi, G. J., Gachunga, H., & Mburugu, C. L. (2014). Effects of Human resource information systems on Human resource management practices and firm performance in listed commercial banks at Nairobi securities exchange. *European Journal of Business and Management*, *6*(29), 2014

Musimba, P.M. (2010). *Determinants of internationalization of information and*

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

communication technology in Small and Medium Enterprises in Kenya. [Doctoral thesis, Human Resource Management, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya].

Nolan, C., Lawyer, G., & Dodd, R. (2019). Cybersecurity: Today's most pressing governance issue. *Journal of Cyber Policy*, 4(3), 1–17. https://doi.org/10.1080/23738871.2019.1673458

Noutsa, F. A., Kamdjoung, J. R. K., & Wamba, S.F. (2017). *Acceptance and Use of Human Resource Information Systems and Influence on Organizational Performance of Small and Medium-Sized Enterprises in a Developing Economy: The Case of Cameroon*. Springer International Publishing, Advances in Intelligent Systems and Computing 569

Obeidat, B. Y. (2018). The relationship between human resource information system (HRIS) functions and human resource management (HRM) functionalities. *Journal of Management Research,* 4(4), 192-211

Okeke-Uzodike, O. E., & Chitakunye, P. (2014). Public Sector Performance Management in Africa, Policies, and Strategies. *Mediterranean Journal of Social Sciences*, *5*(26).

Olughor, R. J. (2016). The relationship between Human Resource Information System and Human Resource Management. *International Journal of economies, Commerce and Management. 4*(2).

Osei-Nyame, P., & Boateng, R. (2015). *The Adoption and Use of Human Resource Information System (HRIS) in Ghana.* [Proceedings of the 17th International Conference on Enterprise Information Systems]. DOI: 10.5220/0005458101300138

Palmer, I., Dunford, R., & Akin, G. (2009). *Managing Organisational Change*: Boston, U.S.A: McGraw Hill.

Parry, E., & Battista, V. (2019), "*The impact of emerging technologies on work: a review of the evidence and implications for the human resource function*", Emerald Open Research, 1(5).

Parry. E., & Tyson S. (2011). Desired goals and actual outcomes of e-HRM; Human *Resource Management Journal*, *21*(34), 335-354.

Quaosar, G. M. A. A., & Rahman, Md. S. (2021). Human Resource Information Systems (HRIS) of Developing Countries in 21st Century: Review and Prospects. *Journal of Human Resource and Sustainability Studies*, 9, 470-483. https://doi.org/10.4236/jhrss.2021.93030

Reinking, J. (2012). *Contingency Theory in Information Systems Research. In: Dwivedi, Y., Wade, M., Schneberger, S. (eds) Information Systems Theory. Integrated Series in Information Systems*. Springer, New York, NY.

Republic of Kenya (2013). *Report of the presidential task force on Parastatal reforms.* Nairobi, Kenya: Government Printer.

Ruël, H. J. M., Bondarouk, T. V., & Van der Velde, M. (2007). The contribution of E-HRM to HRM effectiveness: Results from a quantitative study in Dutch effectiveness. *Employee Relations*, *29*(6), 280-291.

Saaredra, P.A. (2010). *A Study of the Impact of Decentralization on Access to Service Delivery* [Doctorate Thesis, Georgia State University and Georgia Institute of Technology, Atlanta, United States of America].

Shala, B., Prebreza, A., & Ramosaj, B. (2021). The Contingency Theory of Management as a Factor of Acknowledging the Leaders-Managers of Our Time Study Case: The Practice of the Contingency Theory in the Company Avrios. *Open Access Library Journal*, 8, e7850.

Article DOI: https://doi.org/10.37284/eajit.6.1.1612

Sungwa, J. (2021) e-HRM within an African Context. *Open Access Library Journal*, *8*, 1-19.

Vaibhav, A. (2022). Information security governance metrics: A survey and taxonomy. *Information Security Journal: A Global Perspective*, 31(4), 466–478. https://doi.org/10.1080/19393555.2021.1922786

Von Solms, B. and Von Solms, R. (2018), "Cyber security and Information Security – what goes where?", *Information and Computer Security*, Vol. 26 No. 1, pp. 29. https://doi.org/10.1108/ICS-04-2017-0025

Waters, K. P., Zuber, A., Willy, R. M., Kiriinya, R. N., Waudo, A. N., Oluoch, T., Riley, P. L. (2013). Kenya's Health Workforce Information Systems: A Model of impact on Strategic Human Resource Policy, Planning, and Management. *International Journal of Media Informatics 82*(1) 895- 902

Yilmaz, A., Akgemci, T., & Kaygusuz, I. (2016). The impact of HRIS usage on organisational efficiency and employee performance research in industrial and banking sector in Ankara and Instabul Cities. *International Journal of Business and Management*, 4(4).

