

---

**Information Security Services Outsourcing on Security Culture Development  
Among Commercial State Corporations in Kenya**

---

**Article history:** Revised format: 20<sup>th</sup> March 2024, Available online: 20<sup>th</sup> May 2024

---

Joseph Karanja Wanjeri; Prof. John Ndikaru wa Teresia

**Abstract:**

**Purpose:** The primary objective of this study was to determine the effect of outsourcing information security services on the development of security culture among commercial state corporations in Kenya.

**Material/methods:** The study was anchored on the Protection Motivation Theory and employed a cross-sectional research design. The target population consisted of 108 heads of security, finance, procurement, and information and communication technology (ICT) departments from 27 commercial state corporations. A census technique was used, and data were collected through both open-ended and close-ended questionnaires. The dependability of the research tool was evaluated using the Cronbach alpha coefficient. Data analysis involved descriptive statistics (means and standard deviations) and inferential statistics, including Pearson correlation and multiple regression analysis.

**Findings:** The findings revealed that outsourcing information security services had a positive and significant effect on the development of a security culture among commercial state corporations in Kenya.

**Conclusion:** The study concluded that outsourcing information security services not only contributes to the development of a robust security culture but also addresses challenges related to accountability, risk assessment, and confidentiality. The use of access control models and the effective tools employed by security firms were found to effectively mitigate the risks associated with outsourcing.

**Value:** The study recommended that commercial state corporations in Kenya should continue to harness the benefits of outsourcing information security services while prioritizing provider selection and risk assessment. This approach ensures that they can maintain a strong security culture and effectively manage associated risks.

**Keywords:** Information Security Services Outsourcing, Security Culture Development, Commercial State Corporations

**Paper Type:** Research Article

**Recommended citation:** Wanjeri, J. K., & wa Teresia, J. N. (2024). Information security services outsourcing on security culture development among commercial state corporations in Kenya. *Journal of Economics, Management Sciences and Procurement*, I(I), 70-81.

## **1. Introduction**

Organizational security culture originates from the interactions of the employees with the organizational resources and procedures, this will shape employees' behaviors from values and attitudes (Information Security Forum, 2015). Security service delivery involves management of security solutions in form of in-house corporate security and technology solutions. Security program implementations entail steps taken to enact security culture, policies, procedures, standards, and guidelines while security policy can be defined as the documentation in an organization which outlines how it should protect itself from threats (Chia, *et al.*, 2012). The top priority of any government is to establish prevention of crime in order to ensure the safety of all people, both non-citizens and citizens within their jurisdiction. The increase of security threats has resulted to state corporations hiring private security for protecting of their assets and data. This demand is thought to result from a state's inability to give its citizens adequate security. (Wairagu *et al.*, 2014). State corporations and organizations globally have invested heavily in financially and time wise into technical and physical solutions for the protections of their assets and resources (Feenstra & Hanson, 2019). Security outsourcing can be defined as the act of contracting protection of data/information resources, buildings/physical infrastructure, individuals and organization against risk of crime or attacks (Tu & Yuan, 2014).

In reaction to government service restructuring as well as the dynamic development of wartime, many corporations, including governmental institutions, are gradually outsourcing security services from private security firms, services that were previously performed by their police and military forces. As mentioned by BLS (2019) some of the outsourced security services comprise of information security, cash protection, property guarding security as well as bodyguard security. In Australia for instance, it is a typical for private corporations to outsource security services. Australian enterprises outsource security services to cut down on costs, gain access to cutting-edge innovation and skills, and to obtain all-day support (Wood, 2015). Employing a security staff internally requires paying benefits and salaries, incurring other cost of operations and building offices. State enterprises that outsource security only make payments for the services. Additionally, while outsourcing security, a corporation employs a firm whose only activity is protecting other firms. This indicates that because managed security services are their primary source of income, they have the greatest software, hardware and experienced staff. Additionally, because security is a delicate topic, all managed security service providers give support 24/7 for the duration of the contract's validity (Hinde, 2018). In Sub-Saharan Africa, various organizations including state-owned corporations have also adopted security outsourcing. Multinational organizations such as Shell have also made it a standard policy to employ private security firms for their operations. Outsourcing security firms currently in the region operates as security development nexus. Outsourcing security firms are themselves global assemblages, as politicized and internationalized as their customers. It is estimated that 15% of outsourcing security firms have a background in Congo (Schouten, 2021).

Locally, in Kenya private security firms vary in size with majority of them being owner-managed and they are categorized as small and medium firms with fewer than 100 staff. The overwhelming majority of these businesses are active in major towns

and only few of them operate in rural areas, where they operate in one town or locality (Abrahamsen & Williams, 2015). According to Mbote and Akech (2011), the idea of "responsibility" refers to the technique of determining whether one person may be held responsible for any of the actions of another. Guracha and Kiruthu (2019) investigated how commercial state-owned firms in Nairobi County felt about outsourcing security services. The study relied on descriptive research design, where 29 commercial state-owned enterprises and the unit of analysis was 900 security staffs. Questionnaires utilized in gathering data.. The study came to the conclusion that the service delivery of commercial state-owned firms is considerably and causally impacted by security outsourcing (information security, guarding security, bodyguard security, and cash protection security services). The study suggests that commercial state-owned businesses should outsource highly qualified security services because doing so will improve property protection, cash protection, and security services.

The significance of fostering a robust security culture within organizations, particularly state-owned businesses, has been widely acknowledged in both academic literature and practical contexts. Studies by Von-Solms (2020) and Conolly (2020) underscore the pivotal role of organizational beliefs and strategies, such as security outsourcing, in shaping security culture and ensuring the integrity of assets and resources. However, in the Kenyan context, many state-owned enterprises face challenges in integrating security protocols and combating cybersecurity threats effectively. Kaaria (2023) highlights the pressing need for enhanced cybersecurity measures, with a substantial portion of businesses failing to prioritize employee training on emerging threats. Forecasts from G4S (2023) project a surge in security risks facing Kenyan corporations, including supply chain breaches and physical assaults, underscoring the urgency for proactive security measures. Despite the prevalence of security breaches, limited research exists on the impact of security outsourcing on organizational security culture, particularly in Kenya. This study aims to fill this gap by investigating the effects of security outsourcing on security culture development within Kenyan commercial state corporations, thereby contributing valuable insights to both academia and industry stakeholders. The main purpose of this study was to examine the effects of information security services outsourcing

## **2. Theoretical and Literature Review**

The study utilized Protection Motivation Theory (PMT) to investigate the influence of outsourcing property guarding security services and bodyguard services on security culture development among commercial state corporations in Kenya (Lee et al., 2018; Jiow et al., 2021). PMT, a well-established psychological framework, has been extensively employed in cybersecurity research to understand information protection behavior and security culture among various populations. Siponen et al. (2014) demonstrated the relevance of PMT in explaining employees' compliance with information security policies, emphasizing the motivational factors driving adherence to security protocols within organizations. Furthermore, PMT has been used in this study to understand many protections of security culture through outsourcing security services, such as security service delivery, security program implementations, and security policies (Sharma & Aparicio, 2022; Rogers, 1975). The theory is essentially grounded in the observation that people conduct threat assessments to evaluate current conditions in safety and health and participate in related mitigation techniques (Sharma & Aparicio, 2022). Their decision to take precautions is influenced by this assessment

process, which can result in either maladaptive or adaptive behavior. Adaptive behaviors are advised actions (security information outsourcing services) that are thought to be successful in defending the person against the threat (security culture).

### *2.1. Empirical Review*

An examination of the crucial success elements for efficient information security management was undertaken by Tu and Yuan (2014). The study used a technique called critical success factors. Findings showed that successful management of information security controls are effectively built by effective culture, awareness, IT skills, business alignment, and organizational support of security controls and hazards. Since a theoretical model was generated from a literature review but was not tested, the study left a methodological research gap.

Elvin and Johansson's (2017) comparative study between Sweden and Japan in 2017 studied how information security is impacted by organizational culture during the advancement and adoption of IT systems in the banking sector. Semi-structured interviews were employed in the study to gather data from the two nations. Additionally, it interviewed experts in the field of IT. According to the study's findings, banks in Sweden and Japan both treat information security seriously from both an organizational culture and a technical standpoint. The study further concluded that development of IT systems from an information security perspective was impacted by organizational culture aspects. The study created a methodological research gap since it failed to investigate whether the banking industry differs from other industries such as manufacturing in regards to how security cultural aspects affect information security when developing IT system.

Da-Veiga and Martins (2015) established information security culture among firms in south Africa and how it is affected by policies of information security. The research employed quantitative research design and it employed 3927 employees from various organizations in South Africa. In the context of information management and an information security system, the research emphasized the significance of policies pertaining to information security. These actions help to promote a helpful and advantageous security of information culture. The review left a conceptual research gap as it did not look into external factors like national policies with the possibility of impacting the information security culture.

In Ma's (2022) most recent study, it was investigated how to motivate information security (IS) experts to fortify against prospective hazards. The theoretical foundations of the theory of planned behavior (TPB), protection motivation theory (PMT), and essential organizational predecessors relevant to the workplace, such as commitment to the organization and job fulfillment, were utilized in this inquiry. Structural equation modeling (SEM) analysis was used to analyze a sizable sample size of 804 questionnaires, and the study found strong evidence for the interaction of different predictive factors. With clear implications for information security protective practices, the study found notable connections. First, it was determined that information security protective behaviors were significantly influenced by information security attitudes and subjective norms, which are essential elements of TPB. Threat evaluations—which consider threat vulnerability and threat seriousness—and coping evaluations—which

take into account self-confidence and response expenditure—have proven to be effective in forecasting preventative measures pertaining to information security. Organizational commitment is yet another key factor supporting security of information protective actions.

Steinbart and colleagues (2018) team started looking into the results of information security initiatives and the effects of strengthening the relationship between internal audit and information security departments in 2018. Utilizing a cutting-edge dataset, this study examined the nuanced dynamics of how the quality of interaction between internal audit and information security effects quantitative measures relevant to an organization's overall performance in information security. The study's findings revealed a number of convincing insights. The strength of this interfunction link, in particular, had a positive impact on a number of other variables, such as the total number of reported internal control vulnerabilities and instances of noncompliance. Additionally, even before the instigation, the strength of this association was evident in the quantity of security incidents that were both preventative and retrospectively discovered.

### **3. Material and methods**

A cross-sectional survey method was used to investigate the growth of security culture and how it is affected by security outsourcing on the. A cross-sectional survey design, according to Kothari and Gaurav (2014), is used to comprehend a phenomenon at a particular moment

#### ***Sampling***

The study focuses on a target population comprising 108 Heads of Departments (HODs) selected from 27 Commercial State Corporations in Kenya. These HODs represent various departments within the corporations, including Information and Communication Technology (ICT), security, finance, and procurement, ensuring a broad representation across organizational functions. Each department contributes 27 HODs to the total population, ensuring comprehensive coverage. The selection of HODs ensures the inclusion of individuals directly involved in managing security culture within their respective departments. The study employed the census technique, as recommended by Mugenda and Mugenda (2003) when the population is less than 100 respondents, resulting in a sample size of 108 respondents selected through the census sampling strategy.

#### ***Reliability and Validity of Measurement of Variables***

A self-administered open and close ended questionnaire was used to gather information from the respondents with a Likert scale style ranging from 1 to 5 were used to elicit structured responses. Construct validity was measured by exposing structured questions to specialists who asserted the tool validity. The KMO and Bartlett Test was used to establish content validity, where a value higher than 0.5 was accepted. The Cronbach Alpha was employed in establishing internal consistency, where an alpha higher than 0.7 was accepted for each component. all items were retained for further analysis and none was dropped since the Cronbach's alpha coefficients were all above considered and recommended threshold of 0.7 and above Cronbach's alpha (Rovai et

al, 2013; Sekeran and Bougie, 2010).

### ***Data Analysis and model specification***

The data analysis process incorporated descriptive statistics to transform raw data into interpretable formats, facilitating a comprehensive understanding of the responses. Utilizing SPSS software, frequencies, percentages, and means were computed, providing insights into the level of engagement and variations across the population. Additionally, inferential statistics, including correlation and regression analyses, explored the relationships among variables, enhancing the understanding of the study's dynamics. The adoption of a multiple regression model allowed for a deeper exploration of cause-and-effect relationships between security outsourcing services and the development of security culture, aligning with established methodologies in empirical research. The regression model looked like this:

$$Y = \beta_0 + \beta_1 X_1 + \varepsilon_i$$

Where: Y = Development of security culture,  $\beta_0$  = Constant,  $\beta_1$  = Coefficient of determination,  $X_1$  = Information Security Outsourcing

## **4. Findings and Discussion**

This section contains the analysis of the data and its interpretation. A total of 108 questionnaires were disseminated, 93 were fully filled and returned giving a response rate of 86.11%. Mugenda & Mugenda (2013) established that response rates above 50% are acceptable, while rates surpassing 60% are considered good, and those exceeding 70% are very good. Hence, this approach proved efficacious and provided substantial evidence for comprehensive examination across various dimensions of the researched subject matter.

### ***Sample Characteristics***

The findings from table 1 reveal that a significant portion of employees in commercial state corporations in Kenya have substantial job tenure, with 79.6% having been in their current positions for 11-15 years. This data underscores the importance of considering employee tenure in analyzing attitudes and experiences related to security outsourcing and security culture within these organizations. Moreover, the distribution of department sizes indicates that most departments have between 21-30 employees, suggesting a moderate workforce size across the sampled corporations. Understanding department sizes is crucial for assessing the potential impact of security outsourcing on security culture development within different organizational structures. Additionally, the varied operational durations of the participating firms, ranging from 6 to 24+ years, offer insights into the diverse organizational backgrounds represented in the study. This diversity enriches the analysis of security outsourcing effects, providing a comprehensive understanding of its implications for security culture cultivation across Commercial state corporations in Kenya.

**Table 1: Demographic Information**

		<b>Frequency</b>	<b>Percent</b>
Job tenure	Less than 5 years	9	9.7
	5 - 10 years	10	10.8
	11 -15 years	74	79.6
	<b>Total</b>	<b>93</b>	<b>100</b>
number of the employees in your department	1-10	9	9.7
	11-21	26	28
	21 - 30	30	32.3
	above 30	28	30.1
	<b>Total</b>	<b>93</b>	<b>100</b>
long has the firm been in operation	between 6 - 11 years	1	1.1
	between 12 - 17 years	27	29
	between 18-23 years	46	49.5
	above 24 years	19	20.4
	<b>Total</b>	<b>93</b>	<b>100</b>

### *Descriptive Statistics*

The findings from Table 2 reveal a general consensus among respondents regarding the importance of various aspects of outsourcing information security services among commercial state corporations in Kenya. Notably, participants overwhelmingly agreed on the significance of holding outsourced firms accountable for security breaches involving organizational data, highlighting the crucial role of accountability in outsourcing arrangements. However, the moderate level of dispersion in responses suggests some variability in opinions among participants, reflecting differing perspectives on accountability challenges. Additionally, respondents recognized the complexities associated with ensuring accountability in information security outsourcing, emphasizing the need for robust contractual agreements and governance mechanisms. Furthermore, the study highlighted respondents' concerns about the risk of losing confidentiality when outsourcing information security services, underscoring the importance of confidentiality in safeguarding organizational data. While participants generally agreed on the effectiveness of outsourcing arrangements in protecting against data theft, there was divergence in opinions regarding the specific aspects of evaluating potential exposure to data theft through outsourcing. This discrepancy underscores the need for further examination of outsourcing practices to address the evolving cybersecurity threats faced by commercial state corporations effectively. Overall, the findings emphasize the complexity of managing information security in outsourcing arrangements and underscore the importance of comprehensive strategies and governance mechanisms to mitigate security risks effectively.

**Table 2: Outsourcing Information Security**

	<b>Mean</b>	<b>Std. Dev</b>
The outsourced firm must be accountable to any security breaches of organizational data	3.97	0.70
The accountability required in information security has been one of the most troubling aspects of outsourcing of this service	2.42	0.74
The risk of losing confidentiality is taken into account when outsourcing information security	3.91	0.84
Confidentiality concerns are usually addressed when choosing outsource information security	3.99	0.81
Through outsourcing of information security commercial state corporations are protected from data theft	4.06	0.72
Commercial state corporations' potential exposure to data theft are measured through outsourcing of information security	2.02	0.75
<b>Outsourcing Information Security</b>	<b>3.70</b>	<b>0.61</b>

The results from Table 3 demonstrate the significant role that outsourcing security firms play in shaping the security service delivery culture within commercial state corporations, as indicated by a high mean score of 4.16 with a moderate standard deviation of 0.85. This suggests a consensus among respondents regarding the influence of external partners on security practices within these organizations. Additionally, respondents perceive security culture within commercial state corporations as encompassing patterns of behavior contributing to asset protection, highlighting its holistic nature and importance in safeguarding organizational resources. The proactive approach taken by these corporations in adapting security measures to align with evolving threats is evident, as reflected in the implementation of security programs through modifications to organizational culture, policies, procedures, standards, and guidelines, with a mean score of 4.11 and a standard deviation of 0.87. Moreover, the interaction of employees with organizational resources and procedures is seen to shape security culture, emphasizing the role of organizational dynamics in influencing employee behavior and attitudes towards security. Lastly, the documentation of security policies is deemed essential, underscoring the importance of formalizing security measures to ensure clarity and consistency in security practice.



**Table 3: Development Security Culture**

	<b>Mean</b>	<b>Std. Dev</b>
Outsourcing security firms plays a significant role in security service delivery culture of the commercial state corporations	4.16	0.85
Security service delivery involves management of security solutions inform of in-house organization security and technology solutions through outsourcing security firms	4.15	0.85
Commercial state corporations security culture as the totality of the patterns of the behaviors in the institution that contribute to the protection of assets and other resources	4.08	0.91
Security program implementations are taken by commercial state corporations through modification of culture, policies, procedures, standards, and guidelines.	4.11	0.87
Commercial state corporations security culture has been depicted from the interactions of the employees with the organizational resources and procedures, this will shape employees' behaviors from values and attitudes.	4.13	0.90
All the security has been documented through its security policies	4.10	0.86
<b>Development Security Culture</b>	<b>4.12</b>	<b>0.74</b>

### *Regression analysis*

The model summary of the regression model is presented in table 4 below. The study found that outsourcing information security, explained 63.5% of the variation in development of security culture among Commercial state corporations in Kenya. The model fit was good, according to the overall test of significance, which had an F value of 38.2 and a p-value of 0.000. This means that the model was able to adequately explain the variation in the data. The findings in table 4.11 revealed that outsourcing information security has a positive and significant effect on security culture development among Commercial state corporations in Kenya where,  $\beta_1 = 0.219$ , p-value = 0.006 implying that a unit increase in outsourcing information security would result in 0.219 unit increase in security culture development. Thus, we can conclude that outsourcing information security has a positive and significant effect on security culture development among Commercial state corporations in Kenya. This is supported by the research findings of Elvin and Johansson (2017), who assert that information security outsourcing can assist commercial state corporations in mitigating security risks and facilitate the exchange of business information in an open and transparent manner. Similarly, Tu and Yuan (2014) corroborated that the successful management of information security controls is effectively established through a combination of factors including a strong security culture, awareness, IT skills, alignment with business objectives, and organizational support for security controls and risk management. Furthermore, Da-Veiga (2015) emphasized the importance of information security policies as a crucial component of information regulation and the establishment of an information security system. This, in turn, cultivates a supportive culture for information security.

**Table 4: Regression analysis**

	Unstandardized Coefficients		Standardized Coefficients		
	B	Std. Error	Beta	t	Sig.
(Constant)	0.561	0.444		1.263	0.21
Outsourcing Information Security	0.264	0.094	0.219	2.814	0.006
Model Summary					
R	.766a				
R Square	0.587				
Adjusted R Square	0.586				
Mode fitness statistics					
ANOVA (F stat)	476.621				
ANOVA (F-prob)	.000				

a Dependent Variable: Development Security Culture

## 5. Conclusion and Recommendations

In conclusion, the study underscores the importance of outsourcing information security services for commercial state corporations in Kenya. It demonstrates that outsourcing not only contributes to the development of a robust security culture but also helps address accountability, risk assessment, and confidentiality challenges. By selecting reliable and trustworthy outsourcing providers, commercial state corporations can strengthen their security posture, mitigate risks, and protect their data from potential theft.

## 6. Further Research

The primary objective of the study was to examine the effects of security information outsourcing on security culture development among commercial state corporations in Kenya. Future scholars could conduct a comparative analysis of the effectiveness and impact of security outsourcing services across different industries in Kenya.

## References

- Chia, P., A. Maynard, S., B., and Ruighaver, A., B., (2012). Exploring Organisational Security Culture: Developing a comprehensive research model. *Research Gate*, 1, 1-14.
- Conolly, P. (2020). Security starts from within. *Information World*, 22 (28), 39-40.
- Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, 162-176.
- Feenstra, C., & Hanson, H. (2019). The impact of outsourcing and high technology capital on wages. *Quarterly Journal of Economics*, 4 (34), 451-467.

- Guracha, A., & Kiruthu, F. (2019). Attitudes towards Outsourcing Security Services on Service Delivery in Commercial State Owned Enterprises in Nairobi City County, Kenya. *International Journal of Current Aspects*, 3, 1-13.
- Hinde, S. (2018). Recent Security Surveys. *Computers and Security*, 17 (3), 207-210.
- Information Security Forum. (2015). *Information Security Culture - A preliminary investigation*. New York, USA: ISF.
- Jiow, H. J., Mwangwabi, F., & Low-Lim, A. (2021). Effectiveness of protection motivation theory based: Password hygiene training programme for youth media literacy education. *Journal of Media Literacy Education*, 13(1), 67-78.
- Johansson, E., & Elvin, G. (2017). The impact of organizational culture on information security during development and management of IT systems: A comparative study between Japanese and Swedish banking industry.
- 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.
- Lee, H. J., Kho, H. S., Roh, E. H., & Han, K. S. (2018). A Study on the Factors of Experience and Habit on Information Security Behavior of New Services-based on PMT and UTAUT2. *Journal of Digital Contents Society*, 19(1), 93-102.
- Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, 59(1), 102744.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change<sup>1</sup>. *The journal of psychology*, 91(1), 93-114.
- Schouten, P. (2021, Oct). Political topographies of private security in Sub-Saharan Africa. Danish Institute for International Studies, pp. 51-80. Retrieved from Danish Institute for International Studies.
- Sharma, S., & Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among IT employees. *Computers & Security*, 120.
- Siponen, M., Mahmood, M. A., & Pahnla, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, 51(2), 217-224.
- Smith, T. (2020). Managing the Outsourcing Process. In T. Smith, *Credit and Financial Management Review* (pp. 42-50). Estate Investors.
- Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, 71, 15-29.

- Tu, Z., & Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review.
- Von-Solms, B. (2020). Information Security - The Third Wave? *Computers and Security*, 19 (7), 615-20.
- Wood, S. (2015). Integrated Approach Includes Information Security. *Security*, 37 (2), 43-44.