www.idosr.org Quimette
©IDOSR PUBLICATIONS
International Digital Organization for Scientific Research ISSN: 2579-0773
IDOSR JOURNAL OF ARTS AND HUMANITIES 7(1): 1-17, 2022.

A Design Model for Improving Information Security Adoption for SMEs in Uganda

Sheila Mutesi Ouimette

School of Computing and Information Technology, Nexus International University Uganda.

ABSTRACT

Although information systems security is a popular research field in these times, SMEs in developing countries are still finding it difficult to adopt the practice and this is said to be brought about by several facilitating factors relating to technology, governance in these countries, level of education and expertise. However, this study has identified some bottlenecks and proposed a model derived from existing models of technology adoption as an approach to improve the adoption of information security by small and medium enterprises, using the SMEs in the Greater Kampala region. The study began with a detailed and informative background description of the research topic, where the current state of information security adoption was analyzed and presented to support the problem by justifying the gap and informing the desired situation which is to improve the adoption rate for information security by SMEs. Also, existing literature has been reviewed which has predominantly focused on identifying the inputs to support the development of the model. The study argues that to implement the model, understanding the current models and approaches should be greatly considered. To uncover specific actions that constitute logical steps within every dimension of the information security adoption process, the study follows a Design science research method to construct constituting parts of the model and that had been used by several researchers in information science. The study designed a conceptual model consisting of steps and actions, technological, organizational, and environmental factors assessments covering the whole enterprise. Other logical models inform of activity diagrams, sequence diagrams, and dataflow diagrams have been constructed and evaluated by experts on the subject matter who were purposely sampled. The results have been analyzed and the proposed model has been recommended to serve as a starting point for future research in the adoption of information security, which should focus on a detailed quantitative investigation of the cause-effect relationships and the contingency factors to validate all the propositions.

Keywords: Information systems, SMEs and Model Designs

INTRODUCTION

There is no universally accepted definition for Small and Medium Scale Enterprises (SMEs) in Africa [1]. A recent study by [2] alludes that the government of Uganda classifies SMEs as business firms employing 5-50 people as small scale and 51-500 people as medium scale. It is estimated that SMEs in Uganda constitute 90 percent of the private sector and are directly linked to over 80 percent of manufactured output, with many of them being in urban areas and are largely involved in trade, agro-processing, and small manufacturing [3]. SMEs contribute approximately 75 percent of the gross domestic product (GDP) and employ approximately 2.5 million people, signifying their importance in the economic development of Uganda [4]. Ultimately there are a lot of business documents being generated by SMEs today than ever before. Uganda's Small and Medium Enterprise sector is credited with contributing 20% to the country's Gross Domestic Product (GDP) in 2019 [5]. While the level of adoption of technology as a key component of operations within the sector remains unclear, its effective

utilization requires entities to also embrace safety and security measures as a priority identifying security controls to defend against cyber threats and data protection thus formed the basis of discussions at a cyber-standard training workshop for SMEs in Uganda.

According to [5], a report based on a global survey of cyber security managers and practitioners, cyber security and information security is considered a technical issue rather than a business imperative. Another study by [6] also echoed sentiments held by civil society organizations that face similar digital security threats including increasingly sophisticated threats and rate of incidents and revealed that various computer service operations were concerned about or had been victims of hacking attempts on their email accounts and internal networks, that they had been targeted by phishing emails, and that they feared their activities were being surveilled by authorities. To be better positioned to address cyber threats, civil society and SMEs need to be equipped with skills encompassing both online and offline responses. These include know-how on policy and compliance, physical environmental protection, risk assessment, access controls, incident management, monitoring, backup, malware identification, and technical intrusions. Through a cyber-essentials course and practical exercises, participants at the Annual SME Re-Tooling Workshop (2018) were equipped with basic skills for enabling non-technical users to establish five information security controls including malware protection, access control, patch management, secure configuration, boundary firewalls, and internet gateways.

It should be noted that SMEs, in virtually all developing countries, play a key role in national economic development strategies by facilitating the flows of information, capital, ideas, people, and products. The contributions of SMEs to employment and the countries' gross domestic product (GDP) are by no means trivial [6]. Equally, the potential benefits of Information and Communication Technologies (ICTs) to Small- and Medium-Sized Enterprises (SMEs) are well known. ICTs enhance SME efficiency, reduce costs, and broaden market reach, both locally and globally. Since the SME plays a major role in national economies, these benefits to individual SMEs collectively translate into positive results in the form of job creation, revenue generation, and overall country competitiveness [7]. The application of these ICTs in information management as well is pertinent in the efficient functioning of SMEs. Governments, therefore, should have an interest in the promotion of access to, and use of ICTs by SMEs especially in the management of records and information. Unfortunately, several factors hinder or discourage SMEs from fully realizing the benefits of ICTs, including, among others, a lack of knowledge, resources, and trust. Governments, using public policy as a tool, can play a critical role in addressing these concerns. Lack of ICT skills and business skills are widespread impediments to effective uptake once adoption decisions are made. There should be policy considerations that focus on issues related to a healthy business environment, network infrastructure and broadband deployment, human capital and skills development among SMEs, access to information, good e-governance, and public-private-civil society partnerships [8]. Generally, the ability of ICTs to rapidly respond to litigation and investigation about the firm cannot be doubted anymore. SMEs need to comprehensively adopt ICTs applications in business transactions, records, and information management for efficient operations. In the adoption of ICTs, business enterprises should ensure that there are ICTs or e-records policies in place. In support of the policies, Duan [9] observed that information management in ICT systems must be governed by the same organizational policies and accountabilities as records management in all other forms, including paper filing systems and records created and held by office systems (email, correspondence,

memoranda, reports, and spreadsheets)". Good policies or policy statements can be used for an enterprise assessment of the legal, policy, and accountability framework that supports all forms of records management and business operations. As [10] noted that the adoption of ICTs in whatever form or category should consider what the system must do to support the creation, organization, use, retention, and final disposition of records. The sub-categories that are important when adopting ICTs to support records and information management include: creating and capturing records; managing and maintaining records; managing hybrid records; searching, accessing, and retrieving records, and retaining and disposing of records [11]. Moreover, the ICTs adoption by SMEs in records and information management creates a better and efficient means of operation not only in faster decision making but the customers' satisfaction.

It is generally believed that information technology enables a firm to access information needed to make decisions, to make efficient use of resources by reducing labor and manufacturing costs, to seize opportunities in its markets, and to position itself effectively with its contenders [12]. Unfortunately, it is the same environment where both big and SMEs operate and there is a need for the small enterprises to survive in this environment. We live in a very competitive world with the competition becoming fiercer. It has become so volatile that it takes more than success to stay alive. The threat posed to SMEs by the big enterprises is such that they can be swallowed at any time. One of the ways by which SMEs can achieve a competitive advantage in the era of globalization is through the implementation of technology advancement through Information Systems (IS) in their organizations.

According to [13], implementation and practice of Information systems come at a cost and its increasingly high cost is a concern to management, especially in the SMEs sector. With a lack of sufficient funds to acquire such skills smaller organizations often implement Information Systems (IS) in a less than optimal way, thereby attaining fewer benefits than larger organizations. The decision to invest the few available funds in information technology needs to be worth it as SMEs do not have the luxury of funds big enterprises have.

Traditionally, the success of Information Systems (IS) has been studied in the context of large organizations. Most businesses, however, are small and medium enterprises (SMEs) and they have increasingly adopted packaged application software to meet their information processing requirements. Small and medium-sized enterprises exert a strong influence on the economies of all countries, particularly in the fast-changing and increasingly competitive global market [14]. They have been a major engine of economic growth and technological progress [15]. [16] said that SMEs are often more fertile than larger firms in terms of innovation. Most Information Systems (IS) research focuses on large firms, yet most of the firms in most developing economies are SMEs. It is amazing how SMEs form the bedrock of every country's economy, yet they always find it hard to survive not to talk of competing in an environment where the big enterprises have an enormous edge. Though these SMEs cannot match the financial investment of the big enterprises, they need to find a way of balancing their investment to keep abreast of what is happening in their environment.

Statement of the Problem

Currently, the formulation of information security management practices largely excludes SMEs, which practices are primarily being developed mainly for larger enterprises and have traditionally left the SMEs out of the loop. SMEs in developing nations cannot take on the general information security adoption approach but rather require a more customized alternative, their businesses are always vulnerable to information theft and other information security issues. This leaves them exposed to business information compromise and

sophisticated ransomware attacks, not excluding the device administration shortcomings and lack of dedicated information security resources. Records and information management are not being given the attention it requires in the transition to the electronic environment among many enterprises. "In too many cases, ICT systems are introduced without the essential processes and controls for the capture, long-term safeguarding and accessibility of electronic records" [17]. Organizations or enterprises need to act to ensure that ICT systems provide trusted information that is reliable, complete, unaltered, and useable. However, with the new internet paradigms and the ever-changing technologies, it is deemed necessary to increase attention towards the adoption and implementation of information security which has become very vital and a must-have by SMEs, so that all business stakeholders take the appropriate proactive information security measures to secure the most valuable assets for the business survival and growth. Since information today is a valuable resource, without a proper adoption model for SMEs, means that their existence is also threatened in this world of intense competition [18].

Aim of the study

This study aims at designing a model for improving information security adoption for SMEs in Uganda.

METHODOLOGY

The Design Science Research Method

The study employed the design science research method as recommended by [19]. This research method consists of a semantic pursuit of knowledge that combines the identification of a specific problem, collection, and analyzing the data by utilizing scientific reasoning approach to achieve the required results. Based on the objective of the research, adopted for this study. Among the methods that were identified as appropriate are case study [20], and the design science research methods as proposed and applied by several studies [21]. Based on the objective of this research, which is a design of a model for improving the adoption of information security by SMEs in Uganda, the design science research method was identified as

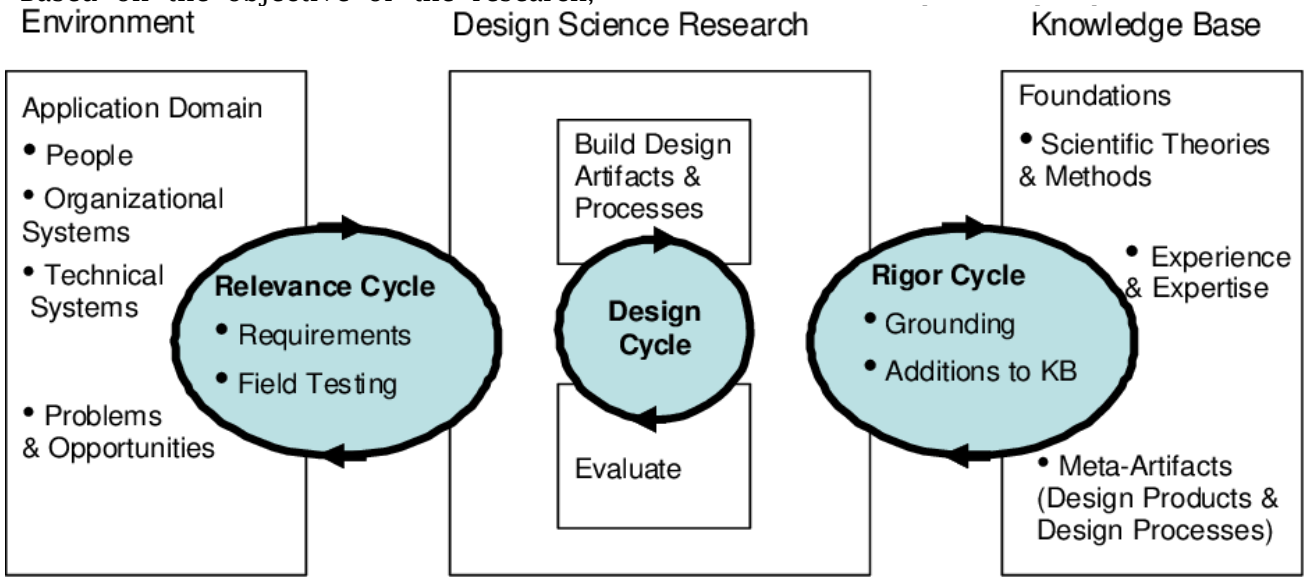


Figure 1: Data science research method visualization [21]

Research design

The study adopted an exploratory study design aimed at comprehending the adoption of information systems security by SMEs in Uganda. According to [22], this design captures data at a specific point in time, contains multiple variables at the time of the data snapshot, and study findings and outcomes can be analyzed to create new theories/studies or in-depth research. By utilizing a mixed approach, which combines qualitative and quantitative research, allowing breadth and depth understanding plus offsetting the weaknesses that are inherent if each approach is separately used. This allowed benefiting from triangulation possibility that comes such an approach is used, this prompted the study to identify aspects of a phenomenon more accurately by approaching it from different vintages by using different approaches and research techniques.

Study population

Population refers to the entire group of people, events, or things of interest that the researcher wants to study [23]. The study considered respondents located in Kampala Metropolitan districts in the central region of Uganda and during data collection, respondents were selected from different categories including SME managers registered with Uganda Investment Authority. These were selected because they are actively involved in the implementation of the day-to-day operations in these departments and are potential people who reliably informed the study on information systems security adoption in the region and reviewing the proposed model by this study.

The sample size and sampling technique

The sample size consisted of 130 respondents from the study area, and these were selected as follows: 40 SMEs managers. This selection of sample size will help the researcher to minimize resources such as time and money plus to other resources.

Table 1: Showing The Uganda Investment Authority database (2019)

Category of respondents	Study Population	Sample size	Sampling technique
SME managers	120	40	Purposive sampling
Total	**120**	**40**	

Sampling Techniques and Procedure

According to [24] sampling is the process of choosing the research units of the target population, which are to be included in the study. A probability sampling method is applied on grounds that elements have an equal chance of being selected [25]. This entails purposive sampling and simple random sampling.

Purposive sampling

In this study, purposive sampling technique under non-probability sampling was used to select Staff at middle, senior management, and heads of department. The technique was chosen because the focus of the study was to get in-depth information and not simply generalizing. Those selected were provided the required information in-depth trough model walk throughs, since their selection was based on their appropriateness to give the required information.

Data collection

During the study, data about the information systems security adoption in developing countries was mined to get a clear understanding of the problem of low information security adoption rates amongst SMEs in Uganda and how to use different technology adoption models and frameworks to derive a more efficient logical model that could be proposed to SMEs in Uganda. Since descriptive analytics are normally driven by static data derived from several sources, like information security adoption evaluations, User perceptions and behaviors, organizational environments, and other contributing factors, understanding the inputs to be used in developing the model

was the major target. Therefore, subsequent reporting included both quantitative and qualitative data, putting into account that this kind of data is post hoc and often summative data. The data that came from documents available online, simulations designed to capture the IS security adoption process by SMEs, and/or direct observation formed ground to elicit the model components. Since Measuring the adoption of technology is a difficult task, the study continued to refine data and methods to achieve insights into the adoption process. The data collected was mainly from two sources that are: primary data source in form of surveys data and interviews which supported the model evaluation, as well as a secondary data source from documents reviews that formed a basis to capture the inputs for the model. Primary data is very paramount because it gives the research real facts about the study thus a good bias for study recommendations [26]. Primary data was collected from respondents with the use of research tools like an Interview guide and a questionnaire tool which were answered by the study respondents (the experts selected).

Questionnaire Survey method.

A questionnaire survey is a research method that consists of a series of questions and other prompts to gather information from respondents [27]. This will be used to collect primary data from the SME Managers in the Kampala district.

Interview method

Interview refers to a method of collecting data by asking people questions and following up or probing and prompting their answers [28]. This method was used to collect primary data from key informants which were the SME managers. The interviews were appropriate because the staff has vital information yet no time to fill the questionnaires [29], this method also enabled the study to get in-depth information from the experts where 6 respondents were interviewed in this study.

Table 2: Interview Respondents Details [29]

Respondent Names	Experience in IT & Services industry	Respondent Current Designation	SME Size
A	9+ Years	CEO, Founder of Organisation A	15+ employees
B	7+ Years	Managing Director	20+ employees
C	10+ Years	CTO	25+ employees
D	15+ Years	Managing director	15+ employees
E	19+ years	Technical Security Lead (Testing Services)	10+ employees
F	15+ years	Research Lab and Security Services Manager	20+ Employees

Documentary Review

According to [30], Documentary review refers to the critical review of materials to get information that supplements gathered information by use of other data collection methods. This method was used to collect secondary data and was guided by a documentary review checklist.

Data collection Instruments

Self-administered questionnaire tool

The questionnaire tool was used after having been formulated based on the

study objectives and this was closed. A questionnaire is a pre-formulated written set of questions to which respondents record their answer usually within closed defined alternatives as reported by [3]. It was self-administered where the respondent would be allowed to fill the questionnaire from an online link. The tool was used to collect information from respondents in the category of employees. The questionnaire method of data collection is to be used because of being cheap and that the method collects responses with minimum errors and a high level of confidentiality.

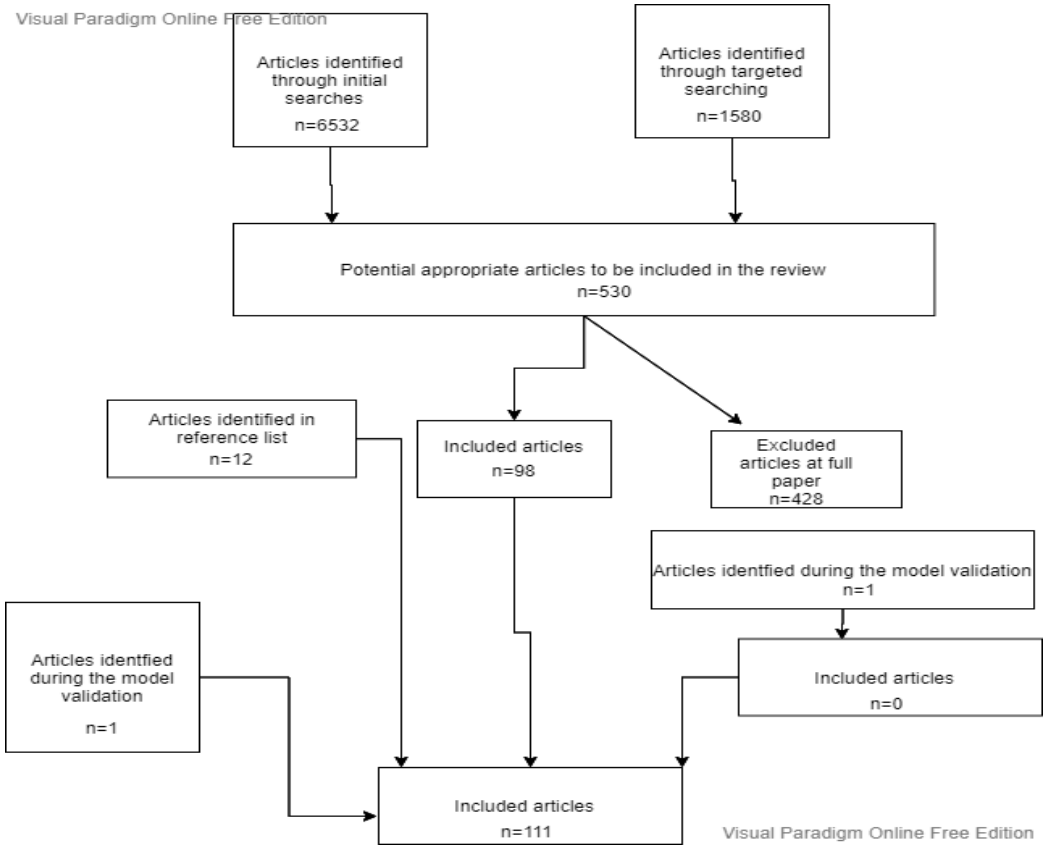
Interview Guide

An interview guide was drafted with a set of questions based on the study objectives and the researcher was able to ask the respondents during an interview and this was also closed. The researcher personally recorded the provided responses as per the study respondents during the process of carrying out an interview. The tool was administered to SME managers to collect information from respondents from the study area.

Document Review Checklist

To review a variety of existing sources like documents, reports, data files, and other written artifacts) to collect independently verifiable data and information. The researcher put much emphasis on brand awareness, brand association, brand loyalty, market share, customer acquisition, sales volume during the document review.

The checklist included the document that has a cover page with the title (name, document type), date, version number, status (craft ready for review, approved)? Had the document been subjected to an internal and external review? Was the relationship to prerequisite documents explicitly stated? Was the content consistent with other documents? Was the terminology used consistently, both within a document and across documents? Was duplication of information avoided? (Cross-referenced rather than copy)? The above process was to ensure that the documents and literature to review conform with the study variables.



VALIDITY AND RELIABILITY OF RESEARCH INSTRUMENTS

Validity

Validity is the extent to which differences found with a measuring instrument reflect true differences among those being tested [12]. After constructing the questionnaire, the researcher contacted three research experts to understand whether her questionnaire will be valid in a way of collecting information that will be used to understand the research problem. Hence the researcher constructed the validity of the instruments by using the expert judgment method as suggested by [9]. The instrument will be refined based on experts' advice. The following formula was used to test the validity index.

CVI =

$$\frac{\text{No. of items regarded relevant by judges}}{\text{Total No. of items}}$$

The questionnaire was considered valid, if the generated coefficient was 50% and above as recommended and when the score was below a recheck of the questionnaire attributes was done on grounds it would be valid and suggested by [11].

Reliability

Reliability of an instrument is the ability of the instrument to collect the same data consistently under similar conditions [16]. According to [7], a reliable data collection instrument must have the ability to consistently yield the same results when repeated measurements are taken of the same individuals under the same conditions. The researcher determined the reliability of the questionnaire by carrying out a Pilot study test in the study area before the time of the study. A pilot study was carried out to know whether the data instruments would be able to establish the required data and it only covered five (5) selected from the study, who were required to provide their views regarding the study variables after which the researcher was able to confirm that formulated data instruments were reliable for data collection if in any case, it was e not reliable the questionnaire content would have been rechecked and redone to fit the study purpose. Noting that reliability measures the consistency of the instrument in measuring what it is supposed to measure.

Data Analysis

This study applied a systematic documentation analysis and review to identify from the literature the relevant content and frameworks that were then employed to frame the components used to assess the adoption process of information systems security amongst SMEs in Uganda. A logical model was designed and proposed, through bilateral structured walkthroughs with experts in the SMEs operating in Uganda who were purposively sampled, the model was evaluated, and the results were reported to inform the effectiveness of the model. Data collected from the questionnaires and interview guides from the field surveys was edited and checked for consistency, totality, and accuracy of responses was then be coded and organized for empirical study analysis. However, qualitative approaches of data analysis were also used as the study was trying to justify the significance of the findings through exploration. Qualitative data consisted of text and information gathered from available different sources and the observations, semantic analysis, and text analysis were applied to typically aggregate the categories of the information and presenting the diversity of ideas gathered during data collection and further be used as a building block for the logical model design. After the model walkthrough with the experts, interviews are conducted as part of the evaluation process which also yielded more qualitative data that supported the evaluation of the model performance.

Model Design and Evaluation

The study acquired knowledge that led to the designing of a logical model for the adoption of information security in SMEs. These are logical steps to guide anyone on the implementation/adoption of information security in SMEs. The

proposed model was then evaluated to ensure that it is the right model for implementation. Maximum consultations with experts will be done to improve the validity and quality of the model, after it has been developed, the model has undergone vigorous validations by external experts as emphasized and effective dissemination of outcomes to interested parties.

Ethical Considerations

Ethics is a systematic approach of understanding, analyzing, and distinguishing matters of right and wrong, good, and bad, admirable, and deployable as they relate to the wellbeing of and the relationships among sentient beings [10]. The study took into consideration, various ethical issues as follows: A letter of introduction was acquired from the University to conduct the study. This was also presented to the SME authorities where the study was conducted for permission to conduct the study research. When was permission granted, the distribution of questionnaires to the respondents and interacting with them using an interview guide then commenced? The completed questionnaires with data from the interview that was conducted were then edited and the next stage was to conduct data analysis. During the study, informed consent was sought from each participant to participate in the study and at each stage, explanations to the respondents about the purpose of the study were thoroughly communicated. On the other hand, anonymity was guaranteed in this study by ensuring that the participants were protected to any extent that even other readers or researchers cannot equally equate what was being reported to what will be provided. This is because this is a very sensitive study that may affect the respondents' jobs as argued by [1]. The study also ensured confidentiality and privacy, this was assured as the researcher informed the respondents that the study was meant strictly for academic purposes and therefore, they should not fear giving information [19]. The study also assured respondents that all information shared was to remain confidential. Further on privacy, respondents were informed prior that their names are not required, and they will not be put under pressure on what they should or not say as suggested by [23]. Additionally, the study carried no bias during data collection and ensured timeliness and completeness of data while avoiding the bias of any kind. Precisely, plagiarism and fraud were avoided, and the study acknowledged each person's work that was used in the study. Consequently, the work was subjected to an anti-plagiarism test to ensure that cited work is duly acknowledged.

RESULTS

Model Design and Evaluation

The Conceptual Model

To further understand the inputs for the information security adoption model, a conceptual model was first designed, to identify the different components and inputs.

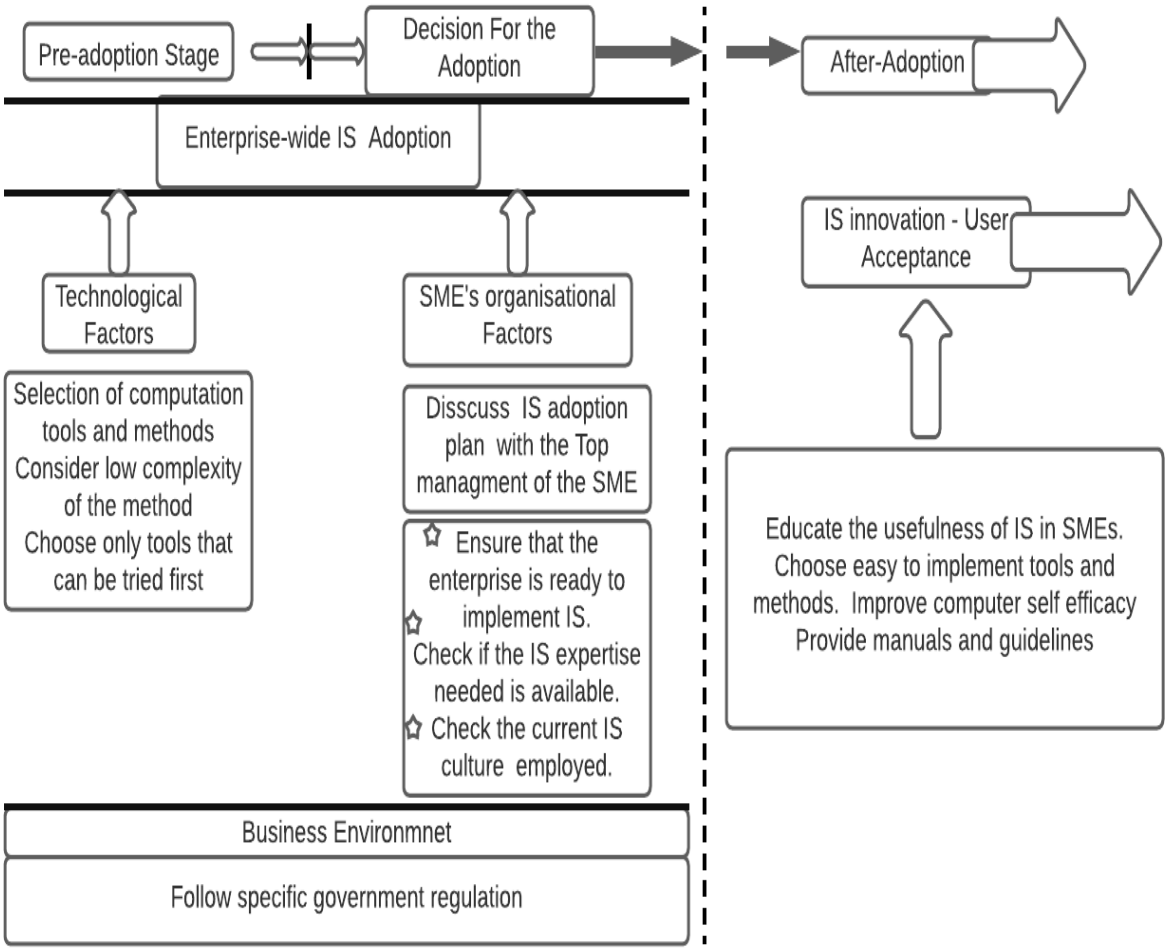


Figure 3: Conceptual Model for IS adoption [21]

With factors focusing predominantly on the information security (IS) adoption starting from the pre-adoption phase to after when the information security has been adopted by the SMEs. Describing all the factors that need to be considered which were identified during documentation review, which is also the attributes related to IS security and its adoption, the study only considered the factors that proved a significant relationship with IS security adoption. Hence, coming up with the following user acceptance and TOE factors. Compatibility of the IS innovation, a distinct Relative advantage, the complexity, and visibility as well as the trialability of the tools and methods as part of the technical factors. From the organizational perspective, the model proposed executive or top management support, size of the organization, awareness of information security, experience of the organization concerning information security, organizational policy, computational capacity, Information Systems security culture, and organizational training and learning culture.

Table 1: Showing definitions for IS adoption factors

Name	Description
	Technological factors
Complexity	How difficult the innovation is to understand and/or use
Visibility	As put forward by Lee and Kozar (2005), it the degree to which an individual observes others' adoption of the innovation
Compatibility	How consistent the innovation is with the values, experiences, and needs of the potential adopters
Relative Advantage	As defined in the diffusion of innovation theory developed by E.M. Rogers in 1962, is the degree to which an innovation is perceived as better than the idea, program, or product it replaces (Hameed *et al.*, 2012a)
Trialability	The extent to which the innovation can be tested or experimented with before a commitment to adopt is made.
	Organizational Factors
Top management support	The extent to which the top management of SMEs commit to providing resources and full support to the implementation and adoption of information security (Hameed *et al.*, 2012b)
Organizational Size	Number of employees the SME has or total sales revenue for the SME (Hameed *et al.*, 2012b)
Information Security Readiness	The degree to which information security innovation can fit or be utilized on an enterprise computer and networks (Lee and Kozar, 2005)
Information security culture	Prior experience of IS innovation in terms of knowledge of individuals and within the whole enterprise (Hameed *et al.*, 2012b)
Information security expertise	The behavior in the enterprise that contributes to the protection of Data and information of all kinds (Salleh *et al.*, 2015)
	Environment Factors
Government Regulation	Refer to government policies to promote Information systems security adoption and enterprise-wide concerns in ensuring compliance to security and data privacy regulations (Salleh *et al.*, 2015)
Risks of Outsourcing	Refer to the associated risks in security and privacy that may result from an organization-wide decision to outsource their innovation adoption initiative (Salleh *et al.*, 2015)
	User Acceptance Factors
User Attitude	The degree to which an individual has a favorable or an unfavorable feeling about a behavior (Lee and Kozar, 2008).
Computer Self-efficacy	The judgment of an individual's ability to use a computer and facilitating conditions (Hameed *et al.,* 2012b)
Perceived Ease of Use	The degree an individual believes innovation is free of effort, he or she would be more likely to use and accept it (Jones *et al.,* 2010)
Perceived Behavioural Control	This is the perceived ease or difficulty of performing the behavior, in this case, enforcing information security or adopting it (Lee and Kozar, 2008)
Subjective Norms	The degree to which an individual perceives social pressure to adopt or not to adopt innovation (Lee and Kozar, 2005)
Image	The degree to which the adoption of innovation enhances one's image as a technical and moral leader among his/her referents (Lee and Kozar, 2005)
Perceived Usefulness	Refers to the tendency to use or not to use innovation to the extent it is believed that it will help or enhance an individual's ability to perform his or her job better (Jones *et al.*, 2010)

The logical model (Sequence Diagram)

This component of the model logically shows the was messages that could be passed on between the key actors during the adoption process to ensure a more coordinated approach while coming up with the strategies and during the planning of a new information security adoption program by the SMEs in developing world. When a new plan is created it's stored in a system's database via a web server and whenever the IT manager what to add and information on the plan before its submission to the top management, there is a possibility to call up the plan and edit. The edits will be updated and when the plan is satisfactory, the IT manager submits the plan for review and the executives will receive an alert that there has been a new development that needs attention in the system. After a successful review, a notification will be sent to the IT manager and all the employees, informing

them that there has been a new security plan that has been approved for implementation. The employees will receive the plan and since the required training and supporting materials would have been stipulated in the plan, the employees will have access to the training guidelines to bootstrap the learning curve especially if it's an innovation or technology.

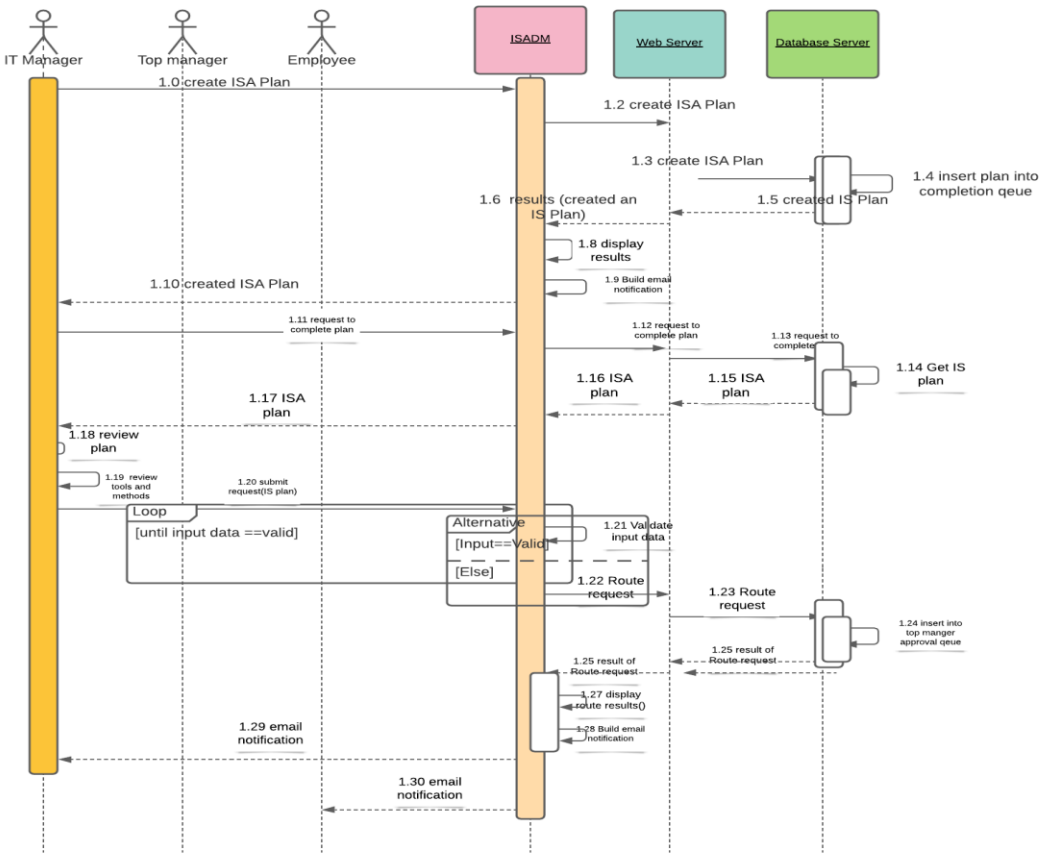


Figure 4: Logical Model (Data Flow diagram)

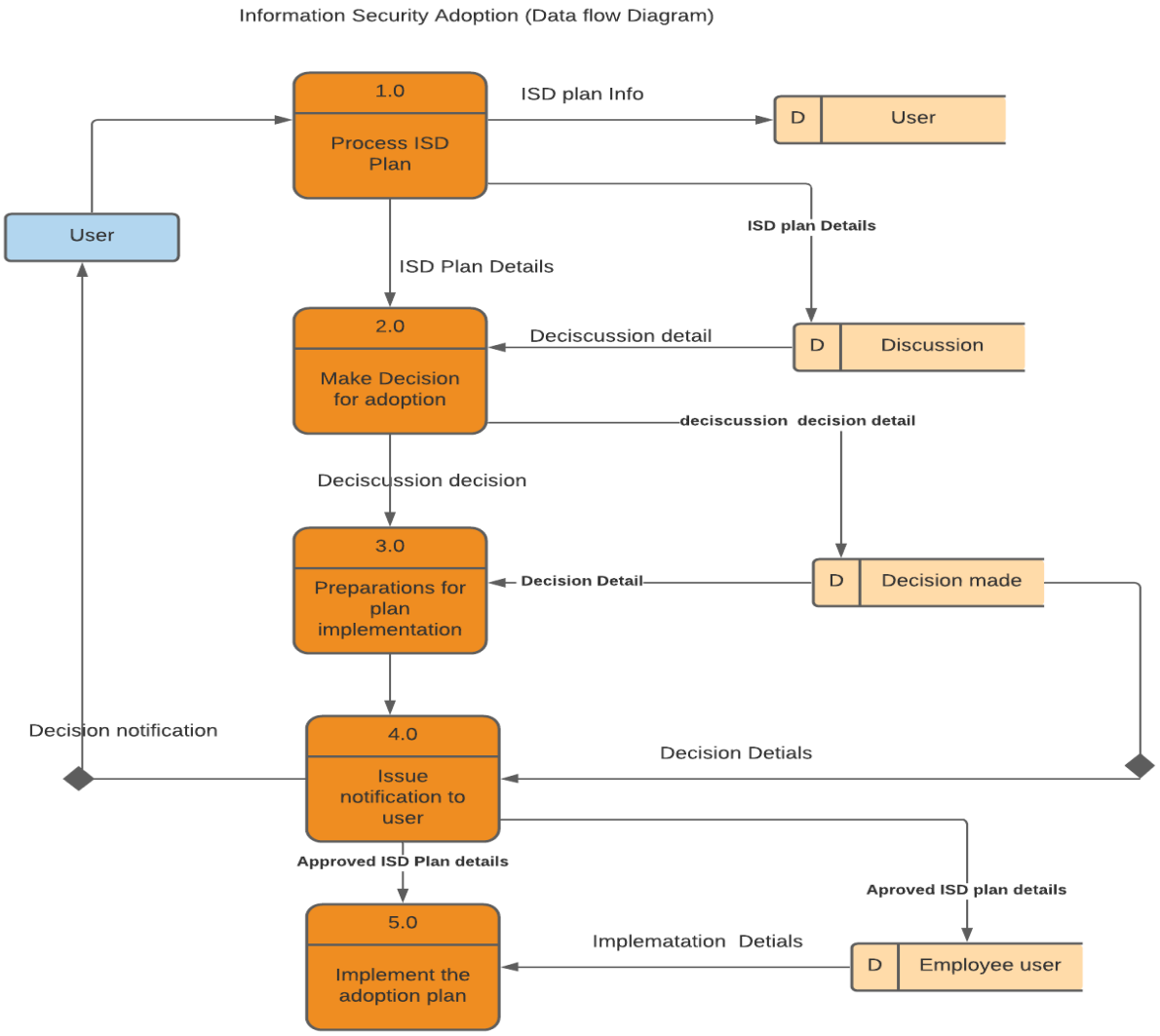


Figure 5: Showing Data flow in the IS adoption system process (Researcher's findings, 2021)

EVALUATION PROCESS OF THE PROPOSED MODEL

Exploratory Study

This section presents the results of the data that was collected and the analysis from the exploratory study interviews. It also highlights the process that was followed while conducting the exploratory study interviews, from the selection of the participants to the analysis of the interview responses and results presented. Based on the analysis, the propositions for model performance likelihoods were derived. And to arrive at this set of propositions, an appropriate process comprising of simple steps was followed. Initially, the interview responses were carefully transcribed. Thereafter, relevant arguments were extracted, gathered, and stored. Thirdly, all points that proved similarity based on respondents' views, notions, and experiences were categorized and where necessary rephrased. And then, all statements with any form of

redundancy had to be eliminated before the interview outcomes were analyzed. In the end, a set of propositions were finally derived from the analysis.

DISCUSSION

Base on the learning and review of the literature to generate new understanding and the analysis of the outcomes of the exploratory and evaluation interviews one can understand that the information security adoption process for SMEs in developing regions, needs a model that can accommodate the uniqueness of such businesses. Since there has been limited previous work that focuses on SMEs' information security adoption models especially that covering the low-resourced setting, the study has learned that a need for more awareness of the issues related to information insecurity is called for in countries located in such areas with limited resources. And that since we are in an era of big data and cloud computing a model to support information security is highly relevant for implementation.

The study has also identified that it's more of an issue related to information security adoption decision-making process and the wider curve for learning new technologies that have limited the adoption of information security by the SMEs and therefore, connecting these aspects in a more coordinated way would aid the adoption process and help in the implementation of new security innovations.

The study has also learned that it's easy for people to understand models connecting applications or models implemented in form of an app as reported by the experts during the interviews and justified by the approximately 87% acceptance rate as per responses from the empirical survey conducted. This makes it an opportunity for a system targeting SMEs to be deployed as a platform as a service app to further aid these businesses while tracking the adoption process as suggested by the experts who reported at a rate of 81% to be very satisfied with the model components involving the automation of the adoption process.

The study has established that a model could improve the time spent by SMEs planning for adoption and increasing the efficiency of the program through simulation of various information security aspects. The experts say that this makes it even less costly for SMEs with an abundance of help materials for supporting employee learning.

A similar conclusion was reached by [26], that for SMEs to compete with larger enterprises or even to succeed in this era of big data, information system within a company will no longer be an option, and study's results were also broadly in line with this argument. Because of the lack of sufficient time to conduct the study, we decided to not investigate the current state of technology diffusion in low resource setting to a broader extent but instead concentrated on information security innovations issues, the reason being that such issues also play a significant role in new technology adoptions such as e-business which has seen a light throughout the covid19 pandemic that saw all businesses migrating to online selling and buying of goods and services and left not the small business behind too. Therefore, the included factors in the model were primarily done to extend the proposed information security adoption model applicability to the SMEs and to prepare them for the dark times that are anticipated as many businesses move their workplaces to the cloud.

It is important to highlight the fact that Effective adoption of IS security innovation is critical in protecting an organization's information systems assets from intended potential malicious attacks and It is interesting to note that the adoption approach suggested by the proposed model, can only be considered successful only if it adds value to the businesses, however its also unclear whether this is suitable for SMEs built on grounds where technological infrastructure still lacks. In addition, several questions remain unanswered as to whether such businesses are ready to use a cloud-based solution putting into consideration that cloud security is far

more complex and requires vast investment and resources during the initial stages.

CONCLUSION

The study has developed and proposed a model for the process of IS security innovation adoption in SMEs. The study explored the theoretical background of IT adoption and user acceptance models and popular frameworks to build the integrative structure. The model was assessed to inform the IS security adoption process in SMEs, navigating from the initial adoption stage right through making enterprise-wise decisions and then post-adoption stages.

The model described levels of analysis, from initiating the adoption up until when innovation comes to acquisition which was assessed as Enterprise wise process which includes the analysis or technological factors, organizational factors and considering the environmental factors, and the second level as a process of user acceptance of the information security innovation which involves analysis in terms of the behaviors of the individuals within the organization. This structure combines frameworks such as TAM, TPB, TOE, and the DOI. The study considers a successful adoption of the IS security innovation as one that is accepted by the users and integrated into the SMEs businesses management structures allowing individual users a continuous usage of the innovation. By exploiting the DOI and TOE frameworks the enterprise adoption process was characterized until when innovation is accepted and integrated. The TAM and TPB frameworks were also used to construct the user acceptance of the information systems security innovations since the study focused on the adoption of IS security in SMEs.

The study, therefore, contributes through an enhancement of the understanding that IS security innovations can be adopted by the SMEs and clear improvement to the implementation process. By blending and drawing upon the rich literature in technology and innovation adoption theories, and applying it in the context of IS security, this field has rarely been empirically investigated. Nevertheless, the shortcoming of individual IS innovation adoption models like the DOI, and TAM were surmounted by the proposed model by combining different innovation adoptions models. This kind of merging allows the individual models to complement each other, hence, making the structure of the proposed model more robust and appropriate for SMEs of any size.

REFERENCES

1. Abramovici M, C. C. (2014). *"E-engineering services for small and medium-sized enterprises" Proceedings of the TMCE.* Lausanne, Switzerland.
2. AJ, J. (2011). *"Innovation in Australian small and medium sized enterprises (SMEs)" 2nd Arab Form on Small and Medium Industries".* Kuwait City, Kuwait.
3. Ang, J. and Koh, S. (2017). ''Exploring the relationships between user information satisfaction'', *International Journal of Information Management,* Vol. 17 No. 3, pp. 169-77.
4. Bart, I. Y., Shankar, V., Sultan, F. and Urban, G. L. (2015). "Are the drivers and role of online trust the same for all web sites and consumers? A large scale exploratory empirical study", *Journal of Marketing, Vol. 69, October,* pp. 133-52.
5. Beyene, A. (2012). Enhancing the competitiveness and productivity of small and medium scale enterprises (SMEs) in Africa: *An analysis of different roles of national governments through improved services. Africa Development xxvii (3):* 130-156.
6. Blili, S. and Raymonds, L. (2017). Adopting EDI in a network

enterprise: the case of subcontracting SMEs. *European Journal of Purchasing & Supply Management,* Vol. 3 No. 3, pp. 165-75.
7. Boyd, C. and Jacob, K. (2007). *Mobile Financial Services for the Underbanked: Opportunities for M-banking and M-payments. Chicago: Centre for Financial Services Innovation.*
8. Chou, D. and Chou, A.Y. (2010). "A guide to the Internet revolution in banking", *Information Systems Management,* 17(2), 51-7.
9. Claessens, S, Glaessner, T. and Klingebiel, D. (2010). E-Finance in Emerging Markets: *Is Leapfrogging Possible?" World Bank*.
10. Conklin, W. A. (2017). Barriers to Adoption of e-Government. *Proceedings of the 40th Hawaii International Conference on System Sciences*, pp. 1–8.
11. Corbitt, B. J. (2010). Developing intra-organizational electronic commerce strategy: an ethnographic study. *Journal of Information Technology,* 15:119-130.
12. Cragg, P. B. and King, M. (2013). Small-firm computing: motivators and inhibitors. *MIS,* Quarterly 17(2):47-59.
13. Delone, W. (2018). *'Determinants of success for computer usage in small business'', MIS Quarterly,*
14. Dirks, P. (2014). MIS investments for operations management: relevant costs and revenues'', *International Journal of Production Economics,* Vol. 35, pp. 137-48.
15. Duan, Y., Mullins, R., Hamblin, D., Stanek, S., Sroka, H., Machado, V. and Araujo, J. (2012). Addressing ICTs skill challenges in SMEs: Insights from three country investigations. . *Journal of European Industrial Training 26(9):430-441.*
16. Feeny, D. F. and Willcocks, L. P. (2018). 'Core IS capabilities for exploiting information technology'', *Sloan Management Review,* Vol. 39 No. 3, pp. 9-22.
17. Gregory, K. (2015). Implementing an electronic records management system: *Public sector case study, Records Management Journal,* 15(2): 80-85.
18. Hvolby, H., Jaques, H. F. and Allan, S. C. (2014). *Supply chain planning in Small and Medium Sized Enterprises. Manufacturing Information Systems,*
19. Kasekende, L. and Opondo, H. (2013). Financing small and medium-scale enterprises (SMEs): *Uganda's experience. BOU working paper.*
20. Khazanchi, D. (2015). Information Technology (IT) Appopriateness: The contingency theory "FIT" AND IT implementation in small and medium enterprises, *The Journal of Computer Information Systems*.
21. Lockett, A. and Littler, D. (2017). The adoption of direct banking services", *Journal of Marketing Management,* 13(8), 791-811.
22. Luarn, P. and Lin, H. H. (2015). Toward an understanding of the behavioral intention to use mobile banking". *Computer in Human Behaviour,* 21(6), 873-91.
23. Mayer, R. C., Davis, H. C. and Schoorman, F. D. (2005). An integrative model of organizational trust", *Academy of Management Review,* 20,709-34.
24. McKnight, D. H. and Chervany, N. L. (2012). What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology", *International Journal of Electronic Commerce,* 6 (2), 35-59.
25. MOFPA, Uganda. (2019). *Bridging Cyber Security Gaps: SMEs Trained in Uganda.* Kampala: Ministry of Finance.
26. Mugenda, M. (1999). *Research Methods Quantitative & Qualitative Approaches.* Nairobi: Nairobi Printing Press.
27. Mutula, S. M. and Van Brakel, P. (2016). E-readiness of SMEs in the

ICT sector in Botswana with respect to information access. *The Electronic Library,* 24(3):402-417.

28. Okello-Obura, C., Minishi-Majanja, M. K., Cloete, L. M. and Ikoja-Odongo, J. R. (2017). Assessment of business information access problems in Uganda. Partnership: *Journal of Library and Information Practice and Research 2(2).*
29. Palvia, P. and Palvia, S. (2009). An examination of the IT satisfaction of small users. *Information & Management,* Vol. 35, pp. 127-37.
30. R, P. (2014). *Delivering the business value of automating business processes to small and medium enterprises, White paper, IDC.*