Educational Data Processing Centers; Determinants of Security Innovations at Higher Education Institutions

Henry Techie-Menson [1]* Daniel Danso Essel[1] Delali Kwasi Dake[1] Alexander Asante [2]
Stephen Opoku Oppong [3]
1. ICT Education Department, University of Education, Winneba, Ghana
2. Head of MIS Section, University of Cape Coast, Ghana
3. ICT Education Department, University of Education Winneba, Ghana
* E-mail of the corresponding author: htechie_menson@uew.edu.gh

Abstract
Higher education institutions are facing unprecedented security challenges due to the increasing recognition of the importance of integrating technology into the core business of teaching and learning. This study sought to investigate the determinants of security innovation for data processing centers of higher educational institutions. Studies related to security innovation of higher educational institutions are limited considering the vast amount of data processing centers deployed for academic operations. In all, 300 respondents were selected from higher education institutions to participate in a survey to test the proposed model by using multinomial logistic regression. The study found out that four predictor variables; relative advantage, complexity, board approval, and IT competencies were significant and hence the model was suitable for studying security innovation at the organizational level.

Keywords: Security Innovation, Educational Data Processing Center, Information Security
DOI: 10.7176/JEP/14-7-02
Publication date: March 31st 2023

1. Introduction

The discovery and advent of the internet, software and hardware have compelled academic institutions to focus on acquiring computer network infrastructure in order to achieve their educational technology objectives. Many academic institutions, particularly universities are increasingly depending on Information Technology (IT), which is considered a key catalyst for changing any service industry of which education is not an exception (Alexei & Alexei, 2021; Ashrafi et al., 2020). Data Processing Centers (DPC) in Higher Education Institutions (HEI) has become a chosen paradigm to store large quantities of personal and educational information on students, instructors, and course records that function constantly, to obtain data from a large number of users (David & Anbuselvi, 2015). A data processing center defines everything ,virtual or physical, which assists institutions with underlying functions to process, serve, and store data that is essential for the survival of that company by providing information and networking required (Miah, Miah & Shen, 2020).

Educational data processing center focuses on the control of the operational IT processes and encompasses all activities which are necessary to maximize the utility of the provided IT services. Educational data processing center operations offer computerization to improve learning environments; provide a telecommunication networks to communicate with external informational spaces as well as the connection between structural departments; enhance related administrative services and improve staff teamwork (Binyamin, Rutter & Smith, 2017; Hansen et al., 2020).

Innovative technologies have rapidly changed the service sector, as well as the existing seller–buyer relationship (Jeon et al. 2020). Expansion, adoption, and appliance of technological innovations can lead to better productivity, increased employment rates, and reduced environmental pollution, but it can also lead to changes in the behavior of the existing societies and reduce social disparities among people (Kusuma et al., 2020).

The continuous development and use of data processing center technology in HEIs has resulted in security problems, particularly those who seek to benefit competitively via innovation. A secure educational data processing center denotes adhering to regulations that permit the protection of private information while collaborating and partnering with other organizations to achieve shared objectives. Educational data processing centers serve a large amount of critical and sensitive data flow where any loss of corporate data as a result of breaches will have a significant negative impact.

1.2 Motivation

A secure data processing center for educational institutions enables its users to concentrate on their primary tasks of conducting research, imparting knowledge, and facilitating learning rather than the hassles and anxiety associated with losing important and private data. However, educational data processing centers emerge as intriguing targets where hackers can profit both personally and financially. The rate of criminal attacks and intrusions into computers and data processing centers in HEI is spreading swiftly, without regard to location (Alexei & Alexei, 2021). Organizational awareness and development of adequate control mechanisms against current security risks are lacking because there is inadequate research that focuses on information security innovation related to the data processing centers of HEI (Ulven & Wangen, 2021; Singar & Akhilesh, 2020). Most importantly, HEI's are unaware of the elements encouraging or impeding the implementation of such innovative information security controls that can protect their assets.

1.3 Research Objective

Predict and explain the factors affecting the acceptance of security innovations at higher education institutions for their data processing centers

1.4 Research Question

What are the determinants of security innovations at higher education institution's data processing centers; and how are they determined?

1.5 Scope of Research

This paper aspires to study the determinants of security innovation in higher education. Security is a very broad concept comprising diverse themes of which this study may not be able to cover. This study will focus on themes such as governance, privacy, identity, access, physical, and personal security associated with educational data processing center.

Furthermore, the study will focus on security innovation at the macro or organizational level. It intends to understand how and why innovative security practices are accepted or denied/rejected at the organizational (macro-level)

1.6 Significance of the study

Academics and others interested in exploring additional data processing center security themes, educational technology, and innovation adoption may find the study's findings and outcomes helpful. This should inspire the creation of fresh concepts for a deeper comprehension of the elements that either encourage or restrict security innovations in educational organizational contexts.

2. Literature Review

2.1 Data Processing Centers in HEI

Information Technology is now regarded as an integral and central part of HEI and not a separate entity due to its vast utilization (Pegu, 2014). Complex IT infrastructure is the backbone of educational research and services which in the long run determines the institution's performance. HEIs boast of an increase in enrolment and reduction in expenditures due to a potent IT infrastructure which leads to enhanced decision making, competitive advantage, and faster reaction to the latest innovation adoption (Pinho, Franco & Mendes, 2018). Data processing centers offer judicious use of scarce resources to provide timely deliverables and guarantee persistent communication among units and departments with the aim of transforming educational service delivery (Pinto et al., 2012).

2.2 Educational processes and DPC alignment

Educational processes and DPC alignment concern how the strategies, goals, and aspirations of educational services are in harmony with IT services. The greater the use of IT in HEI, the higher the rate of performance improvement (Sakala & Chigona, 2020). IT empowers educational institutions by ensuring that specifications in terms of processes are met and hence the shaping of educational and business strategies (Utomo, Bon & Hendayun, 2017).

2.3 Improving Educational Processes

IT is more beneficial when it delivers collective services as opposed to standalone or single components technologically. This allows IT to assume the position of a service provider with both user and technical perspectives in a rapidly changing environment (Raja & Nagasubramani, 2018; Sakala & Chigona, 2020). IT has the tendency to provide customer and service-oriented management that corresponds to educational strategies (Tatili et al., 2016). IT offers a clear distinction between services that are deemed vital to the educational process and those that are not, as well as how those services can be designed and implemented to fit business needs. IT can be seen as addressing complex educational structures that thwart the development of Integrated IT standards (Ghavifekr & Rosdy, 2015)

2.4 Innovation

The construct of innovation is deemed a complex one that has motivated studies from diverse schools of thought in multiple contexts and measured with varying analysis levels. Innovation is considered generating and using new behavior or ideas (Hisrich et al. 2017). Others see the concept of innovation as the practice an organization uses for the first time irrespective of whether different organizations have utilized that technology or practiced it before. Innovation is regarded as a specified tool for entrepreneurs, and the avenues through which changes are exploited as the basis for opportunities and services that are diverse (Viswanathan & Sreekumar, 2019).

Similarly, Porters (1990) contend that competitive advantage can be achieved through acts of innovation by an approach in its widest sense, using technological advances and creative ways of accomplishing tasks. Moreover, innovation is perceived as the vital systematic processes of incorporating problem solving notions that are new to be used.

2.5 Innovation Adoption

An innovation, more specifically in security by an organization such as HEIs is an ongoing phase-based procedure that unfurls over time (Nam et al., 2019). From the view of technological diffusion, adoption describes the organizational campaign to spread IT innovation across its departments (Puklavec et al., 2018). According to Rogers (1995), the innovation adoption begins with a first cognition, consciousness, and assessment of innovation by a firm. The preliminary levels or initial phases include identifying the needs or problems and determining potential innovations to help address that problem (Rogers, 1995). The initiation phase involves design and schedule leading to a decision of adoption. The final stage is implementation, which in the views of Rogers (1983) is the vent decisions, actions involved in implementing innovation.

2.6 Research Model

The TOE framework underpins this study (Tornatzky & Fleischer, 1990) as it depicted in Figure 1 where three contexts; technological, organizational, and environmental factors have an organizational impact on technological innovation. The technological relevance in this context refers to both internal and external technological developments within an organization. The organizational context illustrates how corporate characteristics affect whether an innovation is adopted or not. The external environment is the platform on which a firm runs its operations. (Tornatzky & Fleischer, 1990).

2.6.1 Technological Context

Tornatzky and Klein (1982) reported on ten variables that adoption studies most often address, which include complexity, cost, compatibility, relative benefits, communicability, divisibility, profitability, observerability, social approval and trialability. Just three of the total characteristics of innovation were, however, consistently and significantly correlated with innovation adoption, according to a meta-analysis of 75 innovation research. They include complexity, compatibility, and relative advantages. As a result, our study will now concentrate solely on the three constructs under the technological context.

Relative advantage is the degree to which an innovation is preferred to the concept it replaces (Rogers, 1995; Panchal and Krishnamoorthy, 2019). In this research, relative advantages rest in asset management to determine whether innovative security solutions are more appropriate in HEIs than the outdated technology they intend to replace (Gangwar 2018; Narwane et al., 2019; Pan & Pan, 2019). It looks at the benefits of new technology in HEIs compared to security technologies already in use. I, hypothesize that;

H_1– High levels of perceived relative advantage positively affects DPC security innovation

Compatibility will focus on how the new security innovations should adhere to current processes and procedures at HEIs. It needs to be consistent and logical with adopting organizations ' ethics and technological requirements (Verma & Bhattacharyya, 2017; Ahmad & Siraj, 2018). There is a likelihood of a positive impact if the new technology is considered being highly compatible with the technologies already utilized at HEIs (Tornatzky and Fleischer, 1990; Dubey et al., 2016). We hypothesize that;

H_2–Compatibility of current technologies with what is required positively affects DPC security innovation.

Complexity relates to how difficult users perceive to understand and use an invention (Rogers, 2003). Adoption of an innovation will be less likely if it is perceived as more challenging to utilize. Emerging innovations need to be user-friendly and simple to use in order to enhance adoption rates at HEIs (Verma & Bhattacharyya, 2017; Ramanathan et al. 2017; Ahmad & Siraj, 2018). We hypothesize that;

H_3–Complexity in using technologies negatively affects DPC security innovations

2.6.2 Organizational Context

The organizational context studies the mechanisms and structure of an organization, which either restricts or enables innovative adoption and implementation (Lai et al. 2018). The approval from board members at HEIs is essential as they provide the resources necessary for innovation to happen (Lautenbach et al., 2017; Raguseo, 2018; Khan et al., 2020; Najib & Fahma, 2020). The willingness to invest in security in terms of training, logistics, and regulations will show a strong level of support from the HEI board. We hypothesize that;

H_4–Board approval for improved security positively affects DPC security innovations

IT competency deals with the capabilities of the infrastructure already in place and the knowledge of how to use new technologies (Ghasemaghaei et al., 2018; Braganza et al. 2017; Kim & Eunil, 2020). IT competencies is an important factor in the successful adoption of innovation by HEIs as the availability of financial, technological, and human resources influences whether they plan to acquire new technology. We hypothesize that;

H_5–Competencies in IT positively affects DPC security innovations

2.6.3 Environmental Context

The Environmental contexts are the domains where the firm is in charge of running its business (Tornatzky & Fleischer, 1990). Organizations can develop and offer new products in response to competition (Gangwar, 2018; Chen et al., 2015; Igwe et al., 2020). HEIs will innovate due to the pressing necessity to outperform rivals in the market. We hypothesize that;

H_6–Pressure from rivals positively affects DPC security innovations

Again, regulatory compliance can influence competitive pressures for organizations either unfavorably or positively. The availability of different information security rules and regulations frequently forces businesses to act and invent in order to maintain credibility and conformity with governmental agencies or departments (Dutta & Bose, 2015; Igwe et al., 2020). We hypothesize that;

H_7–Regulatory Compliance positively affects DPC security innovations.

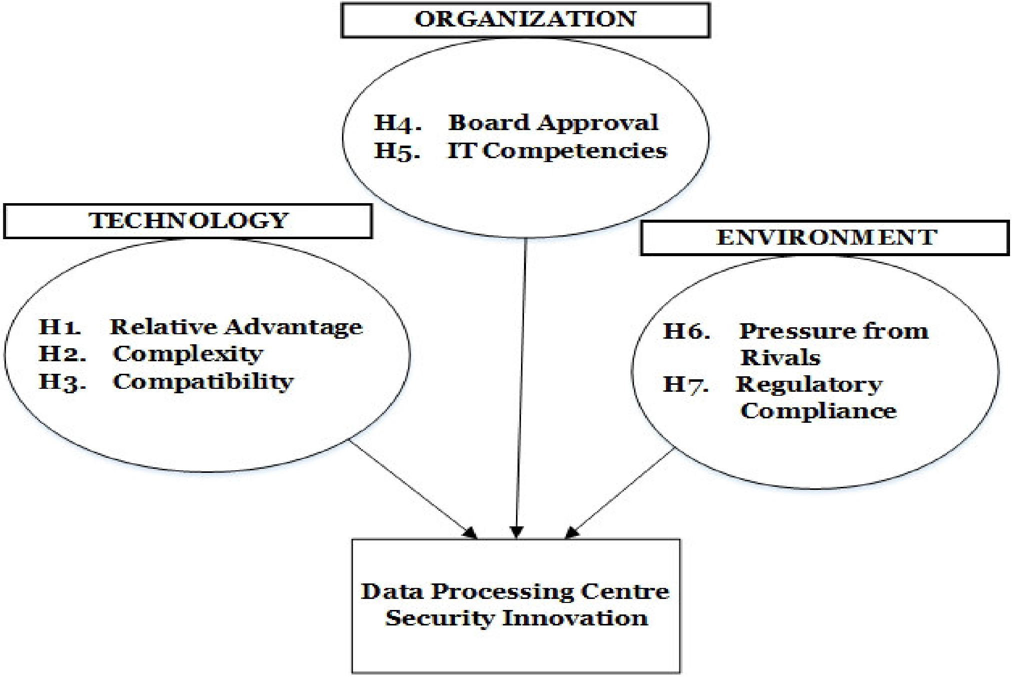


Figure 1. The research model

3. Methodology

The two major approaches for conducting research are inductive and deductive approaches. Using the inductive approach, one or more results based on a particular observation should be generalized. Conclusions drawn from induction should be followed by testing through experiment and deduction. An inductive approach enables more versatility in the design of research as well as to explore the topics and entries emerging from the data. Because of the less organized nature of the research design, the above approach can lead to criticism, which can necessitate a degree of uncertainty (Saunders et al., 2009). In this study, a deductive approach will be used. The use of a deductive approach improves research generalization and the use of tailored quantitative questions will also enhance the reliability and validity of the data.

3.1 Research Design

The research will be designed in a descriptive way with data collection used to answer questions regarding the present state of the subject under study. There are two categories; qualitative and quantitative for the research methods. Quantitative is frequently used to synonymize any data gathering method such as from a questionnaire or a process of statistical analysis like charts or statistical analysis that generates or uses numerical data (Saunders et al., 2009). Qualitative, on the other hand, is commonly used for the synonym of all methods of data recollection, along with interviews or data analysis, such as the categorization of non-numerical data produced or used. (Saunders et al., 2009).

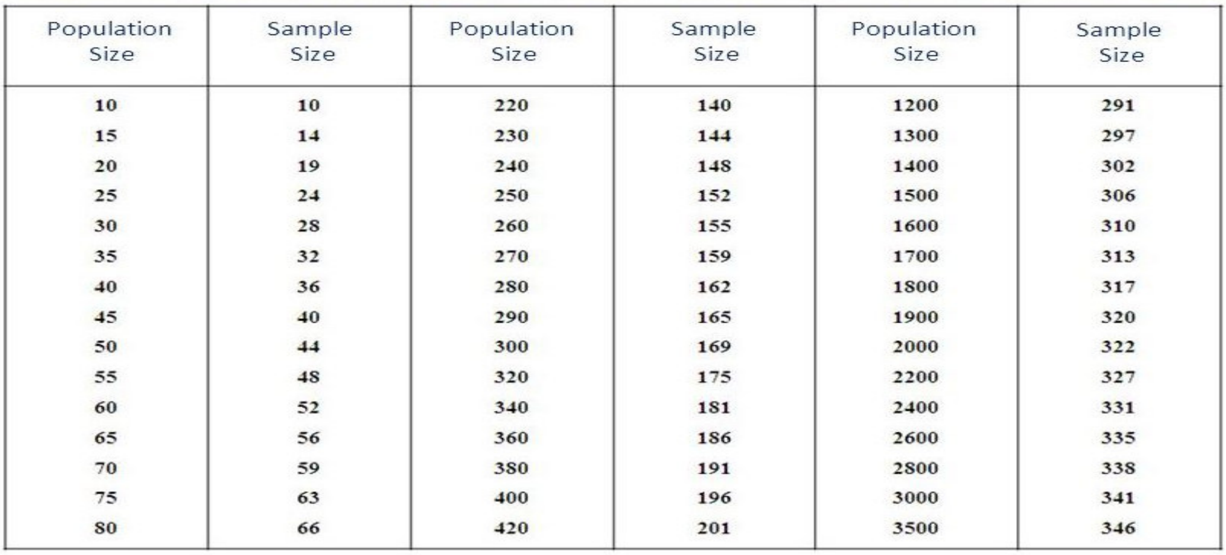
3.2 Population

The accessible population for the study consists of management staff and IT support staff at three HEIs in Ghana, namely, the University of Education, Winneba (UEW), Kwame Nkrumah University of Science and Technology (KNUST) and the University of Cape Coast (UCC). Due to their continuous engagement with IT-related equipment and services where security is crucial, IT support staff were included. Management staff are taken into account since they affect the adoption of IT and security innovations at their respective HEIs and are seen as policy implementers.

3.3 The Sample and Sampling Procedure

The selection of sample sizes was based on the recommendation of Krejcie & Morgan(1970) on determining the sample size of a given population.

Table 1. The determination of the population's sample size



Population Size	Sample Size	Population Size	Sample Size	Population Size	Sample Size
10	10	220	140	1200	291
15	14	230	144	1300	297
20	19	240	148	1400	302
25	24	250	152	1500	306
30	28	260	155	1600	310
35	32	270	159	1700	313
40	36	280	162	1800	317
45	40	290	165	1900	320
50	44	300	169	2000	322
55	48	320	175	2200	327
60	52	340	181	2400	331
65	56	360	186	2600	335
70	59	380	191	2800	338
75	63	400	196	3000	341
80	66	420	201	3500	346

Source: (Krejcie & Morgan, 1970)

The sample size of the target population of 1,400 was 300, based on Krejcie and Morgan's (1970) claim as depicted in Table 1. Probability sampling was used because it offers equivalent opportunities of selection for each group in the population as well as improving generalization from data collected from a population. The bigger the size, the smaller the probability of error for the public generalization (Saunders et. al, 2009).

3.4 Data Analysis

The Statistical Package for the Social Sciences (S.P.S.S) software version 23 was used to analyze the data. The majority of the variables in this study comprised of items of the type Likert, and therefore, the coefficient alpha of Cronbach was used to assess the consistency of the items. Multinomial Logistic Regression (MLR), which is a multivariate analysis technique, was utilized to test the predicted model. The use or relevance of multinomial logistic regression is that it takes into account two or more dependent classification outcomes due to its extension of binary logistic regression. Due to its failure to adhere strictly to normality, homoscedasticity, and linearity, multinomial logistic regression most often is a preferred tool to be used in data analysis.

4. Results

The study sought to investigate the determinants of security innovations of DPC in HEIs. For the goal of gathering data, a series of questionnaires were given to 159 IT Support workers and 141 management staff of the chosen institutions. The question guiding the study was; what are the determinants of security innovations at higher education institutions; and how are they determined.

In order to ascertain the importance of the model predictors, the results of the likelihood ratio tests in Table 2 can be used (Field, 2009). Complexity, Board approval, IT competencies and relative advantage were the four predictor variables significant at ($p< 0.05$.). The test of likelihood ratio is a general statistic that shows which determinants predicted the results significantly, but does not tell the particular results specifically (Tabachnick & Fidell, 2011).

Table 2. Likelihood ratio test

	Model Fitting Criteria	Likelihood Ratio Tests		
Effect	-2 Log Likelihood of Reduced. Model.	Chi-Square.	Df.	Sig.
Intercept.	610.560	4.332	2	.115
Relative Advantage	614.119	7.891	2	.019
Complexity	611.552	5.324	2	.040
Board Approval	614.096	7.869	2	.020
Pressure from Rivals	609.472	3.244	2	.198
Compatibility	610.308	4.080	2	.130
IT Competencies	620.353	14.125	2	.001
Regulatory Compliance	608.029	1.801	2	.406

Regarding the assumptions presented here, it is apparent that the HEIs ' decisions on security innovation for DPC are influenced by relative advantage, board approval, complexity, and IT competencies. Table 3 offers a summary of the accepted and rejected hypotheses.

Table 3. The summary of hypotheses

Technological	Accepted
H1:Relative Advantage	
H2:Compatibility	Rejected
H3:Complexity	Accepted
Organizational	
H4: Board Approval	Accepted
H5: IT Competencies	Accepted
Environmental	
H6: Pressure from Rivals	Rejected
H7: Regulatory Compliance	Rejected

Two major MLR applications exist. First, to anticipate group membership by calculating the chances that an organization will be in one of the phases of assimilation, initiation, acceptance, or implementation. Second, the offer of an understanding of the connection and strength between variables (Field, 2009). Table 4 summarizes the results of multinomial logistic regression, including the significance level, β-coefficient (B) and the Experimental β-coefficient Exp (B). The related advantage, complexity, board approval, and IT competencies out of the seven independent variables are closely linked to the decision for HEI's adoption for security innovation.

In the model, based on Wald statistics, Relative Advantage, board approval, complexity, and IT competencies were defined as the only significant factors which can be established on the basis of the sign of the coefficient (B). Relative Advantage (β=.290, p<0.05), Complexity (β=-.168, p< 0.05.) Board Approval (β=161, p< 0.05.) and IT Competencies (β=-.248, p< 0.05) which is positive with the value of Exp (B > 1).

Table 4. Parameter estimates for multinomial logistic regression

	First Model Initiation Verses Adoption-decision			Second Model Adoption-decision verses Implementation			Third Model Initiation Verses Implementation		
	B.	Exp(B).	Sig.	B.	Exp(B).	Sig.	B	Exp(B)	Sig
Intercept	-4.899		.052	3.856	-	-	1.042	-	-
Relative Advantage.	.198	1.219	0.58	0.92	1.097	.367	.290	1.079	.008
Complexity.	-.134	.874	0.76	-0.34	.967	.663	-.168	.723	.035
Board Approval	0.22	1.022	.727	.139	1.149	0.27	.161	1.039	.010
Pressure from Rivals	-0.33	.967	.696	.149	1.160	0.88	.116	.947	.183
Compatibility	.092	1.097	.373	-.213	.808	0.46	-.121	.716	.266
IT Competencies	0.82	1.085	.398	-.330	.719	.001	-.248	.648	.009
Regulatory Compliance	.120	1.128	.212	.100	.905	.309	0.20	.844	.833

Table 5 summarizes the major findings with regard to the stated hypothesis and each factor is discussed in relation to the context of technology, organization and environment exhibited throughout the study model.

Table 5. Findings from the hypothesized model

Hypothesis	First Model Initiation Verses Adoption-decision	Second Model Adoption-decision verses Implementation	Third Model Initiation Verses Implementation
Ho1 Relative Advantage	Not Supported	Not Supported	Supported**
Ho2 Compatibility	Not Supported	Not Supported	Not Supported
Ho3 Complexity	Not Supported	Not Supported	Supported*
Ho4 Board Approval	Not Supported	Not Supported	Supported*
Ho5 IT Competencies	Not Supported	Supported**	Supported**
Ho6 Pressure from Rivals	Not Supported	Not Supported	Not Supported
Ho7 Regulatory Compliance	Not Supported	Not Supported	Not Supported

*Significant level at 0.05, **Significant level at 0.01

5. Discussion

5.1 The Technological Context

This study posits that complexity; relative advantage and compatibility will encourage the adoption of DPC security at HEIs. The findings related to the constructs under the technological context are analyzed below.

5.1.2 Relative Advantage

The result shows that the relative advantage and use of DPC security innovation is in a significant positive relationship as it can be observed in Table 5, relative advantage is significant in model 3. This implies that HEIs perceived benefit of innovating with security are more prevalent at the stage of implementation in comparison to the stage of initiation and adoption. It can be explained that the benefits of data security mechanisms may not be evident at onset. However, they will be able to harness the full potential of security innovation technologies when they are fully implemented. These findings are supported by Studies that have found relative advantages as drivers (Oliveira et al., 2014; Alshamaila et al., 2013; Borgman et al., 2013) for innovation adoption. However, this finding contrasts other studies (Small et al., 2011), which indicated that relative advantage had a negative impact on the development of innovation in Taiwan's high-tech industry, and had no support for the relative advantage.

5.1.3 Compatibility

Rogers (2003) reports that technology innovation is typically rapid if organizations realize that innovation is compatible with their requirements and established practices. Decision-makers at HEIs therefore prefer to make sure new ICT utilities are compatible with employee responsibility and worldviews. The results indicated that compatibility is not an influence on DPC security innovation as illustrated in Table 5. This result is different from other publications (Alshamaila et al., 2013; Chen et al., 2015; Verma & Bhattacharyya, 2017) as it has suggested that compatibility is an integral component of Information System innovation and hence there is a greater likelihood of innovation adoption by HEIs if they are compatible with current working practices. This inconsistent result is consistent with former research in the area of innovation adoption (Borgman et al., 2013; Alshamaila et al. 2013). The insignificance of compatibility may arise from the fact that HEIs expect existing standalone systems to be simply replaced by similar systems. Again, the level of conformity between innovation and the desires of potential adopters may not always be sufficiently obvious before adoption.

5.1.4 Complexity

Scholars have suggested that when firms eventually acquire an innovation, it is perceived to be significantly more complex than expected, which inhibits its implementation in turn. This study found complexity to be significant in implementation as it is illustrated in table 5 in line with (Acheampong & Moyaid, 2016; Pan & Pan, 2019; Ghobakhloo & Ching, 2019) who achieved similar results but contrasts with the findings of Yoon et al. (2014), who discovered inconsistent outcomes with complexity. These results can be exacerbated by the fact that various HEIs have real worries concerning how convenient such systems can function because they are not simple to use, adopt, and implement. This means that HEIs consider DPC security technology more difficult to comprehend and use during adoption decision-making than during the implementation phase. Another plausible explanation for this outcome could be that HEIs underestimate the function of complexity before their adoption at the initiation stage and are overconfident about technological usability. As a result, when they ultimately acquire the technology, they consider it to be much more complex than anticipated, thereby inhibiting implementation. According to this analysis, the initial misconception about the complexity of innovative security technology can lead to an assimilation gap if the widespread technology acquisition does not follow with the widespread implementation.

5.2 Organizational Context

The institutional metrics that affect DPC security innovation at HEIs in terms of its adoption and implementation are deliberated in the organizational context. Board approval and IT competencies form the major characteristics of the organizational context

5.2.1 Board Approval

Management involves executive leadership incorporation because organizational policies and processes can indeed be influenced by the top management of a respective organization. The approval from HEIs board of management is liable for improved corporate strategy leading to advantageous contexts and innovation. This is essential since decision-making on security innovation depends not only on the views of IT personnel, but on the need to persuade the board or management for their approval. The results from table 5 are congruent with earlier studies which demonstrated that senior management had an indirect effect on innovation acceptance (Alshamaila et al., 2013; Dubey et al., 2016; Lautenbach et al., 2017; Gangwar, 2018; Khan et al., 2020; Najib & Fahma, 2020). The ability of the board or management of HEI to allocate or assign resources in the procurement of cutting-edge security technologies is one potential explanation for the significant findings.

5.2.2 IT Competencies

Knowledge and skills are essential for technological adoption, which requires that organizations fully understand the underlying technology and alignment with the ambitions and specifications of the organization. More efforts need to be made to provide the expertise to run this technology at the workplace level. From Table 5, it can be observed that IT competency were significant in model 2 and model 3, that is, at the phases of adoption decision and implementation. The availability of resources in the form of infrastructure and staff at various HEIs that can accommodate security advances when the necessity arises may be one explanation for this finding. This shows that additional talents and resource availability expedite the decision to adopt and implement security innovations.

Alternatively, these outcomes suggest that insufficient IT competencies act as a barrier for implementing security innovation. This implies that HEIs may be postponing adoption decision and implementation, rather than acquisition, until they are sufficiently ready in terms of technology. This is congruent with previous research which has shown that technological-competent organizations are more likely to embrace emerging technology (Olexova, 2014; Pan & Pan, 2019; Najib & Fahma, 2020). Furthermore, empirical evidence exists that supports the view that organizations with staff with previous Information Systems knowledge will use innovative technology more frequently.

5.3 Environmental Context

Competitive pressure and regulatory compliance are the major constructs discussed under the environmental context. The study posited that both constructs determine the acceptance of DPC security innovation of HEI and are discussed below.

5.3.1 Pressure from Rivals

Security innovations can transform organizations to be more competitive and simplify the development process that matches rivals. The results from Table 5 indicate that competitive pressure inhibits the adoption of security innovation in HEIs. Previous studies had significance outcomes for competitive pressure (Borgman et al., 2013; Lautenbach et al., 2017; Igwe et al., 2020). This outcome is consistent, however, with other studies (Jeon et al., 2006; Alshamaila et al. 2013) that also discovered that competitive pressure in small to medium-size businesses was not a significant determinant for cloud computing innovation. One of the possible explanations for the insignificant result is the lack of competition among HEIs, which may require restructuring and updating of security protocols to gain a competitive edge over rivals. This implies that the competitive pressure is not stronger enough for HEIs to feel compelled to adopt innovations in DPC security preemptively to avoid a future disadvantage in competition. In this regard, DPC security technology cannot be seen as a strategic need by HEIs. Again, a potential reason can be attributed to the fact that the percentage of innovating in security in Ghanaian universities is low and is still at an early stage.

5.3.2 Regulatory Compliance

Standards and government regulations may have an adverse effect on the environment for the implementation of HEI security technologies. Table 5 indicates that there was no support for regulatory compliance in regard to DPC innovative security adoption. A possible explanation for this finding is the substantial transaction costs incurred when HEIs wish to properly comply with security benchmarks. Since many institutions have limited resources, finding additional funding to address security issues may be a difficult undertaking for them. Another possible reason for this outcome is that in difficult times the use of security technology and practices is not supported by rules or regulations from the government. In addition, government support is required to establish appropriate regulations or review their operating regulations in order to conform to the requirements of recommended practices in security. These outcomes were in line with previous studies, in which the factor has no direct effect on the use of innovative technology (Borgman et al., 2013; Igwe et al., 2020).

6. Conclusion and Recommendations

This study examined the determinants of security innovation in HEI data processing centers. Specifically, the study spelled out to; predict and explain the elements affecting the acceptance of security innovations of data processing centers by HEI. The theoretical framework for research has been the Technology Organization and Environment theory because of its appropriateness in explaining the constructs under study. Valid arguments were made for a deductive approach and its suitability for positivist research. The survey strategy was used with justification for its appropriateness for the study. The Quantitative stance was chosen due to the argument made against other methods. The study population was made up of management staff and IT support staff at selected HEIs in Ghana. 300 participants made up the study's sample, which was gathered using the probability sampling technique. The research instrument employed was a questionnaire which was adapted from innovation adoption researchers and previously published papers. The questionnaire was administered consisting of 25 items.

Data analysis was performed using SPSS version 23 and the questionnaires were checked for reliability (Cronbach's alpha was above 0.7). As the research is a predictive one, the hypothesis was tested using a multinomial logistic regression analysis. The research model showed a good fit, with Cox and Snell(0.508) and Nagelkerke(0.618) with 76.3 percent accuracy predictability.

6.1 Research Limitations

A few constraints, in particular regarding the research methodology and results, can be identified from this study. Due to the limited scale of research, it was difficult to integrate all variables of security innovation presented in previous literature.

Secondly, the methods used to achieve the research objectives have been confined to quantitative (survey) methods due to the limited time and costs. Even though this study analyzed the data through a powerful multivariate tool, other studies may use alternative methods, such as case studies, through the conduct of interviews with individuals within the same organization. Finally, this study was mainly confined to Ghana's public universities. It may therefore not be suitable that the entire population is generalized to all cycles of education in Ghana.

6.2 Implications for Theory and Practice

Many studies suggested different adoption frameworks, although very few studies addressed the adoption of security innovations across multiple contexts by offering a model for organizational security innovation. This study endeavored to fill both gaps by proposing a general security innovation model highlighting the important role organizations play in adopting innovative security technology, particularly for HEIs. While there is a need for further research into security innovation at HEIs, this research work has taken the first step to filling that gap through tangible and practical literature contributions. This model may also by coincidence be applied to other innovations rather than security. This is achieved by developing the model from a widely used framework for technology adoption, such as the TOE found in literature.

Organizations that want to adopt security innovations can implement the model with all factor-specific considerations, making decisions on innovation more easily and quickly. In addition, organizations can use the model and findings from this study after initially adopting innovative security technologies to mitigate potential problems which may arise during the innovative process.

6.3 Recommendations

Additional research is required to determine the factors influencing security innovation at other higher education institutions to deliver numerous contextual views due to the wide variety of DPCs they deploy in the performance of their primary functions of teaching, learning, and research. Again, there are additional factors that can be considered as drivers for innovative adoption decisions, thereby extending the seven factors used in this study. This will give the adoption of innovations a wider perspective while also giving the phenomenon a concrete understanding.

In addition, the results of this study indicate that more research on the adoption of security innovation within HEIs is urgently needed. The model can then be improved on the basis of its application results. Furthermore, it can develop and explain the adoption of other innovations by a streamlined or adapted model.

References

Acheampong, O., & Moyaid. S., A. (2016). An integrated model for determiningbusiness intelligence systems adoption and post-adoption benefits in banking sector. *Journal of Administrative and Business Studies* 2(6): 84–85.

Ahmad, M., & Siraj, S. (2018). A systematic review and analysis of determinants impacting adoption and assimilation of e-commerce in small and medium enterprises. *International Journal of Electronic Business* 14: 326–51.

Alexei, A., & Alexei, A. (2021). Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. *International Journal of Scientific & Technology Research.* 10(5). 128-133.

Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework. *Journal of Enterprise Information Management, 26(3)*, 250–275

Ashrafi, A., Zareravasan, A., Rabiee Savoji, S., & Amani, M. (2020). Exploring factors influencing students' Continuance intention to use the learning management system(LMS): A multi-perspective framework. *Interactive Learning Environments, Taylor & Francis, 0(0*), 1–23

Binyamin, S., Rutter, M. and Smith, S. (2017). Factors influencing the students' use of learning management Systems: A case study of King Abdulaziz University. *Proceedings of the International Conference on ELearning, ICEL*, pp. 289–297.

Braganza, A., Brooks, L., Nepelski, D., Ali, M., & Moro, R. (2017). Resource management in big data initiatives: Processes and dynamic capabilities. *Journal of Business Research*, 70, 328–337

Borgman, H.P. (2013). Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework. *In 2013 46th Hawaii International Conference on System Sciences.* Ieee, 4(5),44-35.

Chen, D. Q., Preston, D. S., & Swink, M. (2015). How the use of big data analytics affects value creation in Supply chain management*. Journal of Management Information Systems, 32(4),* 4–39

David G. S. S. & Anbuselvi, R. (2015). An architecture for Cloud computing in Higher Education. *International Conference on Soft Computing and Networks Security* (ICSNS), 1–6

Dubey, R., Gunasekaran, A., Childe, S. J., Wamba, S. F., & Papadopoulos, T. (2016). The impact of big data on world-class sustainable manufacturing*. The International Journal of Advanced Manfacting Technology, 84(1–4),* 631–645

Dutta, D., & Bose, I. (2015). Managing a big data project: the case of ramco cements limited. *International Journal of Production Economics*, 165, 293–306

Field, A. (2009) *Discovering Statistics Using SPSS. 3rd Edition*, Sage Publications Ltd., London.

Gangwar, H. (2018). Understanding the determinants of big data adoption in India: An analysis of the manufacturing and services sectors. *Information Resources Management Journal, 31(4)*, 1–22

Ghasemaghaei, M., Ebrahimi, S., & Hassanein, K. (2018). Data analytics competency for improving firm decision making performance. *The Journal of Strategic Information Systems, 27(1),* 101–113

Ghavifekr, S. & Rosdy, W. A. W. (2015). Teaching and learning with technology: effectiveness of ICT integration in schools. *International Journal of Research in Education and Science (IJRES)*, *1*(2), 175–191. https://www.ijres.net/index.php/ijres/article/view/79

Ghobakhloo, M., & Ching, N., T. (2019). Adoption of digital technologies of smart manufacturing in SMEs. *Journal of Industrial Information Integration* 16, doi:10.1016/j.jii.2019.100107

Hansen, R. J., Talmage, C. A., Thaxton, S. P., & Knopf, R. C. (2020). Enhancing older adult access to lifelong learning institutes through technology-based instruction: A brief report. *Gerontology & Geriatrics Education*, *41*(3), 342–351. https://doi.org/10.1080/ 02701960.2019.1618852

Hisrich, R., D., Michael P. P., & Dean, A., S. (2017). *Entrepreneurship*. New York: McGraw Hill Education

Igwe, S., R.., Ebenuwa, A., & Otite W., I. (2020). Technology adoption and sales performance of manufacturing small and medium enterprises in Port Harcourt. *Journal of Marketing* 5: 44–59.

Jeon, H., M., Sung H., J., & Young, K., H. (2020). Customers' acceptance intention of self-servic technology of restaurant industry: Expanding UTAUT with perceived risk and innovativeness. *Service Business* 14: 533–51

Khan, A., Satish K., & Jithesh A. (2020). The Role of ICT Laws and National Culture in Determining ICT Diffusion and Well-Being: A Cross-Country Examination. *Information Systems Frontiers* 22: 1–26.

Kim, J., & Park E. (2020). Understanding social resistance to determine the future of Internet of Things (IoT) services. *Behaviour & Information Technology* 39: 1–11.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, *30(15)*, 607-610

Kusuma, H., Muafi M., AJI Hendy M., & Sigit P. (2020). Information and Communication Technology Adoption in Small- and Medium-Sized Enterprises: Demographic Characteristics. *Journal of Asian Finance, Economics and Business* 7: 969–80.

Lautenbach, P., Kevin Johnston, and Tejumade Adeniran-Ogundipe. 2017. Factors influencing business intelligence and analytics usage extent in South African organisations. *South African Journal of Business Management* 48: 23–33

Lai, Y., Huifen, S., & Jifan, R. (2018). Understanding the determinants of Big Data Analytics (BDA) adoption in logistics and supply chain management. *International Journal of Logistics Management; Ponte Vedra Beach, 29*(2), 676-703.

Miah, S. J., Miah, M., & Shen, J. (2020). Editorial note: Learning management systems and big data technologies for higher education*. Education and Information Technologies, 25(2),* 725–730

Nam, D., Lee, J., & Lee, H. (2019). Business analytics adoption process: An innovation diffusion perspective. *International Journal of Information Management*, 49, 411–423.

Najib, M, & Fahma.F. (2020). Investigating the Adoption of Digital Payment System through an Extended Technology Acceptance Model: An Insight from the Indonesian Small and Medium Enterprises. *International Journal on Advanced Science Engineering Information Technology* 10: 1702–1708

Narwane, V. S., Raut, R. D., Gardas, B. B., Kavre, M. S., & Narkhede, B. E. (2019). Factors affecting the adoption of cloud of things: The case study of Indian small and medium enterprises. *Journal of Systems and Information Technology, 21(4),* 397–418. https://doi.org/10.1108/JSIT-10-2018- 0137

Olexova, C. (2014). Business Intelligence Adoption: A Case Study in the Retail Chain. *WSEAS Transactions on Business and Economics* 11: 95–106

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the Determinants of Cloud Computing Adoption: An Analysis of the Manufacturing and Services Sectors. *Information & Management, 51(5*), 497–510

Pan, M., & Pan, W. (2019). Determinants of adoption of robotics in precast concrete production for buildings. *Journal of Management in Engineering* 35: 05019007

Panchal, D., & Krishnamoorthy, B. (2019). Developing an instrument or business model dimensions: exploring linkages with firm competitiveness. *International Journal of Global Business and Competitiveness, 14(1),* 24–41. https://doi.org/10.1007/s42943-019-00004-1

Pegu UK (2014) Information and communication technology in higher education in india: Challenges and opportunities. *International Journal of Information and Computation Technology 4(5)*:513–518

Pinho, C., Franco, M., & Mendes, L. (2018). Web portals as tools to support information management in higher education institutions: A systematic literature review. *International Journal of Information Management,* 41(May 2017), 80–92 Elsevier.

Pinto, M., Souza, F., Nogueira, F., Balula, A., Pedro, L., Pombo, L., Ramos, F., et al. (2012). Tracing the use of communication technology in higher education: a literature review, *Proceedings of INTED2012-International Technology, Education and Development Conference*. 2012
Porter, M. (1990). *The Competitive Advantage of Nations*, Macmillan, London

Puklavec, B., Oliveira, T., & Popovič, A. (2018). Understanding the determinants of business intelligence system adoption stages. *Industrial Management and Data Systems*, *118(1),*236–261.

Raguseo, E. (2018). Big data technologies: An empirical investigation on their adoption, benefits and risks for companies. *International Journal of Information Management, 38(1)*, 187–195

Raja, R., & Nagasubramani, P. C. (2018). *Impact of modern technology in education* [Paper presentation]. *Conference on Recent Trend of Teaching Methods in Education, Sri Sai Bharath College of Education Dindigul-624710*, Tamil Nadu, India. http://dx.doi.org/10.21839/jaar. 2018.v3iS1.165

Ramanathan, R., Philpott, E., Duan, Y., & Cao, G. (2017). Adoption of business analytics and impact on performance: a qualitative study in retail. *Production Planning and Control, 28(11–12*), 985–998

Rogers, E. M. (1983). "*Diffusion of Innovations," Third Ed*., The Free Press, New York

Rogers, E.M. (1995). *Diffusion of innovations, Fourth Edition ed*., Free Press, New York

Sakala, L. C., & Chigona, W. (2020). How lecturers neutralize resistance to the implementation of learning management systems in higher education. Journal of Computing in Higher Education. *Springer US*. 32(2), 365–388

Saunders, M. N. K., Lewis, P. & Thornhill, A. (2009). *Research Methods for Business Students (5th Edition)*. London: Pearson Education.

Singar A. V. & Akhilesh, K. (2020). 'Role of cyber-security in higher education', in Smart Technologies, *Springer*, 2020, pp. 249–264.

Tatili, S., Treska, T., & Mero, B. (2016). How does technology influence on education in nowadays? *European Journal of Multidisciplinary Studies*, *1*(4), 138–141. https://dx.doi.org/10.26417/ ejms.v1i4.138-141

Tabachnick, B. G., & Fidell, L. S. (2001). *Using multivariate statistics* (4th ed.). Needham Heights, MA: Allyn and Bacon.

Tornatzky, L. G., & Fleischer, M. (1990). *The Process of Technological Innovation.* Lexington, Mass: Lexington books.

Tornatzky, L.G. & Klein, K. (1982). Innovation characteristics and innovation adoption implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management, 29(1),* 28-43

Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet* 2021, 13, 39. https://doi.org/10.3390/fi13020039

Utomo, H., Bon, A., & Hendayun, M. (2017). Academic information system support in the era of education 3.0., IOP Conference Series: *Materials Science and Engineering*, 226. https://doi.org/10.1088/1757-899 X/226/1/012190

Verma, S., & Bhattacharyya, S. S. (2017). Perceived strategic value-based adoption of big data analytics in emerging economy: A qualitative approach for Indian firms. *Journal of Enterprise Information*

Management, 30(3), 354–382

Viswanathan, M., & Sreekumar, Arun. (2019). Consumers and technology in a changing world: The perspective from subsistence marketplaces. *European Journal of Marketing*. 53. 1254-1274. 10.1108/EJM-11-2017-0826.