European Journal of Business and Management
ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online)
Vol.14, No.18, 2022

Strategies for Ensuring the Safety of Digital Documents in Office Systems Management

Phoebe Tega Agbamu (PhD)[1] Abigail O. Ofume[2]
Department of Vocational and Technical Education
University of Delta, Agbor, Nigeria[1]
Email: tegapheobe@gmail.com[1] Tel: 08035050720[1]
Email: sonnyofume@yahoo.com[2] Tel: 08033422368[2]

Abstract
The today's office is shifting to a paperless office (automated office) where the computer is employed in carrying out general office work and documents are managed electronically. Organizations are currently faced with the problem of securing these documents from loss, hackers, malware and unauthorized users. Hence this study sought to find out the strategies for ensuring the safety of digital documents in Office Systems Management. The population of the study comprised of 118 administrators and secretaries selected from organizations that operate automated offices in the six State capitals of the States in South-South Nigeria. Four research questions were raised and four corresponding research hypotheses were raised and tested at 0.05 level of significance. The result of the study revealed that the administrators and secretaries viewed all backup, password, file level and share level security, as well as encryption strategies as ensuring safety of digital documents to a high extent. It was concluded in this study that backup, password, encryption, file level and share level security strategies does ensure safety of digital documents in Office Systems Management. Therefore, it was recommended that these strategies be employed by organizations operating automated offices to ensure safety of their digital documents.
Keywords: Backup, encryption, file level, share level, safety, strategies, Office, Systems Management
DOI: 10.7176/EJBM/14-18-05
Publication date: September 30th 2022

Introduction

The office is the information and records hub of any organization and advances in office systems has brought about a serious shift from paper-based processes to electronic processes in records and documents management. Offices had hitherto been characterized by paper- based processes in records management which involve the handling of physical documents ranging from typed letters and documents, photocopied materials, receipts and files, archiving and retrieving physical documents from a file cabinet (kissell, 2013). The traditional paper based processes have been found to be inefficient, costing valuable office space and posing risk of losing valuable documents, due to lose, damage, misfiling or getting into wrong hands (Mills Senn,2014) .The challenges and problems posed by paper based processes are minimized if not totally eliminated when organizations go digital.

Digitization or paperless trend is fast becoming the norm in Office Systems Management. Currently, organizations are offering their clients the convenience of mobile application and the option to receive electronic invoices (Chao, 2015). Stratton noted that electronic files allow for better access to information sharing, cost less in terms of physical space and personnel, and can increase productivity.

The concept of paperless office or digitization may bring to mind an office without papers. However in reality, a paperless office or paper free office is a work environment in which the use of paper is greatly reduced. This is done by converting document and other papers into a digital form, a process known as digitization. A paperless environment closely resembles an office utilizing integrated information system with multiple software tools to reduce paper consumption and improve efficiency in retrieving electronic documents (Dykman and Davis, 2012). Organizations that offer a variety of options such as mobile application, electronic billing and electronic payment benefit by not having to send out paper invoices while their customers enjoy the convenience of performing tasks such as transferring funds, paying bills and checking account balances from anywhere regardless of time and space. Some problems associated with paper payments such as, cash counterfeiting and signature forgery are eliminated when organizations go digital (Aigbe and Akpojaro, 2014).

Statement of Problem

In the electronic office instead of heaps of files which are consulted often to retrieve information and volumes of paper sent here and there, you find computers, laptops intranet and internet connections. This has led to the need for Electronic Document Management System (EDMS), Electronic Records Management System (ERMS) and a combination of the two systems Electronic Data and Records Management System (EDRMS). A system in which the records life circle which range from creation, storage, retrieval, transmission to protection are done electronically.

Although a lot can be said for the paperless office or digitization, it is not foolproof. Frear, (2014) identified some factors inhibiting the spread of digitization, one of which is the fear of losing electronic documents. If digitization is to be considered best practice in documentation then the fear of losing vital documents if controlled electronically, need to be allayed. Organizations need to stay one step ahead of those with malicious intent, like hackers, unauthorized users and software that interfere with the computers normal function. The contention then is to seek for well-established strategies that can ensure the safety of digital documents. Therefore this study seeks to determine the safety measures or strategies companies or organizations can put in place to ensure the safety of their digital documents.

Purpose of the Study

The major purpose of the study was to identify strategies for ensuring the safety of digital documents in Office Systems Management. Specifically, the study sought to identify

1. The backup strategies that ensures safety of digital documents in Office Systems Management.
2. The password strategies that ensures safety of digital documents in Office Systems Management.
3. The encryption strategies that ensure safety of digital documents in Office Systems Management
4. The file level and share level security strategies that ensure safety of digital documents in Office Systems Management.

Significance of the Study

The findings of this study revealed the strategies that organizations adopt to ensure safety of their digital documents. This would in turn erase the fear of digitization from the minds of managers of office systems. It will gradually lead to widespread digitization, which translates to best practices in document management. With an efficient and safe document management system, office workers, secretaries and administrators would find it easy to retrieve information thereby leading to increased productivity in the office.

Research Questions

The study was guided by the following research questions:

1. To what extent do backup strategies ensure safety of digital document in Office Systems Management?
2. To what extent do passwords strategies ensure safety of digital documents in Office Systems Management?
3. To what extent do encryption strategies ensure safety of digital documents in Office Systems Management?
4. To what extent do file level and share level security strategies ensure safety of digital documents in Office Systems Management?

Research Hypotheses

The following null hypotheses were tested at 0.05 levels of significance.

1. There is no significant difference in the mean ratings of administrators and secretaries on the extent to which backup strategies ensure safety of digital documents.
2. The administrators and secretaries do not differ significantly in their mean ratings on the extent to which password strategies ensure safety of digital documents.
3. There is no significant difference in the mean ratings of administrators and secretaries on the extent to which encryption strategies ensure safety of digital documents.
4. The administrators and secretaries do not differ significantly in their mean ratings on the extent to which file level and share level security strategies ensure safety of digital documents.

Methodology

The population of the study comprised of 118 administrators and secretaries from organizations in south-south Nigeria that operate automated offices. No sampling was done since the population was manageable. A 4 point Likert rating scale questionnaire titled: Strategies Ensuring Safety of Digital Documents (SESODD) was used for data collection. It was scored 1-4 weighed scale. It contained 41 questionnaire items based on the research questions raised for the study. The instrument was validated by 4 experts - two are in Vocational and Technology Education, and the other two are in Educational Foundations. The reliability of the instrument was determined by use of Cronbach Alpha technique and yielded a reliability of 0.78. Of the 118 questionnaire distributed with the help of six (6) research assistants who were properly briefed, only 100 were correctly filled and returned. Mean and standard deviation were used to answer the research questions while t-test was used to test the null hypotheses at 0.05 levels of significance. Mean ratings above 2.5 were regarded as high extent and below 2.5 were regarded as low extent. For the null hypotheses, anyone with a p-value lower than the alpha level was rejected while, anyone with a p-value higher than the alpha level was retained.

Results

The results of the study are presented and analyzed in the following tables:

Research Question One

To what extent do backup strategies ensure safety of digital documents in Office Systems Management?

Table 1:

Respondents' Mean Ratings on the Extent to which Backup Strategies Ensure Safety of Digital Documents

S/N	Item Statement	X	SD	Remark
1	Backup early	3.63	.520	High Extent
2	Backup often	3.48	.565	High Extent
3	Backup with centres having multiple points	3.51	.580	High Extent
4	Store documents offsite	3.52	.580	High Extent
5	Use cloud computing to update the document as you work	3.36	.632	High Extent
6	Use flash and memory for storage as you work	3.38	.611	High Extent
7	Use CD ROMS for storage backup	3.44	.605	High Extent
8	Use hard disk for storage backup	3.17	.726	High Extent
9	Use compact disk for storage backup	3.39	.612	High Extent
10	Use magnetic tape for backup	3.38	.595	High Extent
	Grand mean	3.43		

Source: Survey Data 2022

The data in table 1 indicate the mean and standard deviation of administrators and secretaries in South-South Nigeria on the extent to which backup strategies ensure the safety of digital documents in office systems management. It can be deduced from the table that all the item statements were responded to as useful to a high extent for ensuring safety of digital documents. Items 1-10 which are: backup early 3.63, backup often 3.48, backup with centres having multiple points 3.51, store documents offsite 3.52, use cloud computing to update the document as you work 3.36, use flash and memory for storage as you work 3.38, use CD ROMS for storage backup 3.44, use hard disk for storage backup 3.17, use compact disk for storage backup 3.39 and use magnetic tape for backup 3.38. The grand mean of 3.43 showed that backup strategies ensure safety of digital documents to a high extent.

Research Question Two

To what extent do password strategies ensure safety of digital documents in Office Systems Management?

Table 2:

Respondents' Mean Ratings on the extent to which Passwords Strategies Ensure Safety of Digital Documents

S/N	Item Statement	X	SD	Remark
1	Use password that has never been written down	3.18	.594	High Extent
2	Use password that has never been stored online	3.00	.810	High Extent
3	Use password that is not a word in any language or slang	3.37	.687	High Extent
4	Use password that contains at least fifteen alphanumeric characters	3.32	.568	High Extent
5	Use password that cannot be found in a dictionary	3.28	.735	High Extent
6	Use password that is not a computer term or command	3.17	.714	High Extent
7	Use password that is not a date or other personal information	2.95	.754	High Extent
8	Use password that is not a company name	3.01	.761	High Extent
9	Use password that has a combination of upper and lower case characters	3.18	.694	High Extent
10	Use password that has number, symbols and letters.	3.20	.681	High Extent
	Grand mean	3.17		

Source: Survey Data 2022

The data in table 2 shows the mean and standard deviation of administrators and secretaries in South-South Nigeria on the extent to which password strategies ensure the safety of digital documents in office systems management. It can be deduced from the table that all the item statements were responded to as useful to a high extent for ensuring safety of digital documents. Items 1-10 which are: use password that has never been written down 3.18, use password that has never been stored online 3.00, use password that is not a word in any language or slang 3.37, use password that contains at least 15 alphanumeric characters 3.32, use password that cannot be found in a dictionary 3.28, use password that is not a computer term or command 3.17, use password that is not a date or other personal information 2.95, use password that is not a company name 3.01, use password that has a combination of upper and lower case character 3.18 and use password that has number symbols and letters 3.20.

The grand mean of 3.17 showed that password strategies ensure safety of digital documents to a high extent.

Research Question Three

To what extent do file level and share level security strategies ensure safety of digital documents in Office Systems Management?

Table 3:

Respondents' Mean Ratings on the Extent to which File Level and Share Level Strategies Ensure Safety of Digital Documents

S/N	Item Statement	X	SD	Remark
1	Set permission on data files and folder	3.43	.561	High Extent
2	Use of share level permissions	2.90	.864	High Extent
3	Use file level permissions	3.07	.695	High Extent
4	Define level of access	3.12	.773	High Extent
5	Use read only access	3.21	.809	High Extent
6	Use full control access	3.58	.630	High Extent
7	Use set time limits for accessing files	3.39	.677	High Extent
8	Use new technology file system (NTFS)	3.27	.683	High Extent
9	Operate a user level permission	3.09	.830	High Extent
10	Use change permission	3.25	.748	High Extent
	Grand mean	3.23		

Source: Survey Data 2022

Data in table 3 revealed that items 1-10 were highly rated as a means of ensuring safety of digital document. The items are: set permission on data files and folders 3.43, use of share level permission 2.90, use of file level permission 3.07, define level of access 3.12, use read only access 3.21, use full control access 3.58, use set time limits for accessing files 3.39, use new technology file system (NTFS) 3.27, operate a user level permission 3.09 and use change permission 3.25. The grand mean of 3.23 indicated that the administrators and secretaries, view file level share level security strategies as a means of ensuring safety of digital documents to a high extent.

Research Question Four

To what extent do encryption strategies ensure safety of digital documents in Office Systems Management?

Table 4:

Respondents' Mean Ratings on the Extent to which Encryption Strategies Ensure Safety of Digital Documents

S/N	Item Statement	X	SD	Remark
1	Use encryption file system (EFS)	3.38	.597	High Extent
2	Use disk encryption	3.17	.726	High Extent
3	Never store a plain text	3.04	.793	High Extent
4	Store only cipher text	3.24	.810	High Extent
5	Use cryptographic method data	3.06	.843	High Extent
6	Encrypt with a public key infrastructure (PKI)	3.13	.829	High Extent
7	Encrypt with the stenography software	3.02	.739	High Extent
8	Use encapsulating security payload (ESP)	3.58	.528	High Extent
9	Use secure wireless transmission	3.44	.632	High Extent
10	Use right management system (RMS)	3.36	.671	High Extent
11	Send and store data only on wireless network that uses encryption	3.03	1.010	High Extent
	Grand mean	3.55		

Source: Survey Data 2022

The data in table 4 showed that items 1-11 were all rated to a high extent. These items include: use encryption file system (EFS) 3.38, use disk encryption 3.17, never store a plain text 3.04, store only cypher text 3.24, use cryptographic method data 3.06, encrypt with a public key infrastructure (PKI) 3.13, encrypt with the stenography software 3.02, use encapsulating security payload 3.58, use secure wireless transmission 3.44, use right management system (RMS) 3.36 and send and store data only on wireless network that uses encryption 3.03. The grand mean of 3.55 indicated that the administrators and secretaries view encryption strategies as means of ensuring safety of digital documents.

Hypothesis 1

There is no significant difference in the mean ratings of administrators and secretaries on the extent to which backup strategies ensure safety of digital documents.

Table 5:
T-test Analysis of Difference in the Mean Ratings of Administrators and Secretaries on the Extent to which Backup Strategies Ensure Safety of Digital Documents

Group	N	X	SD	DF	t	P-value	Alpha Level	Decision
Administrators	60	3.40	.393					Not Sig
Secretaries	40	3.44	.381	118	-.566	.576	0.05	p>0.05

Source: Survey Data 2022

The result in table 5 showed t-test analysis of the difference in mean rating of administrators and secretaries on the extent to which backup strategies ensure safety of digital documents in Office Systems Management. It can be discerned from the table that the observed probability value (p-value) or sig at 0.05 level of significance with degree of freedom 118 is .576 which is greater than the chosen alpha level t(118)= -.566 p>0.05. Since the p-value is higher than the chosen alpha level, the null hypothesis is therefore upheld. This implies that there is no significant difference between the mean ratings of administrators and secretaries on the extent to which backup strategies ensures the safety of digital documents in Office Systems Management.

Hypothesis 2
The administrators and secretaries do not differ significantly in their mean ratings on the extent to which password strategies ensure safety of digital documents.
Table 6
T-test Analysis of Difference in the Mean Ratings of Administrators and Secretaries on the Extent to which Password Strategies Ensure Safety of Digital Documents

Group	N	X	SD	DF	t	P-value	Alpha Level	Decision
Administrators	60	3.05	.389					Sig
Secretaries	40	3.28	.368	118	-3.374	.001	0.05	p<0.05

Source: Survey Data 2022

Table 6 revealed t-test analysis of difference in the mean rating of administrators and secretaries on the extent to which password strategies ensure safety of digital documents in Office Systems Management. It can be deduced from the table that the observed probability value (p-value) or sig at 0.05 level of significance with degree of freedom 118 is .001 which is less than the chosen alpha level t(118)= -3.374 p,<0.05. Since the p-value is less than the chosen alpha level, the null hypothesis is rejected, and the alternate hypothesis retained. This implies that administrators and secretaries differ significantly in their rating on the extent to which password strategies ensures the safety of digital documents in Office Systems Management. This difference is in the level of ratings and does not in any way negate the fact that password strategies ensure the safety of digital documents

Hypothesis 3
There is no significant difference in the mean ratings of administrators and secretaries on the extent to which file level and share level security strategies ensure safety of digital documents.
Table 7:
T-test Analysis of the Difference in the Mean Ratings of Administrators and Secretaries on the Extent to Which File Level and Share Level Security Strategies Ensure Safety of Digital Documents

Group	N	X	SD	DF	t	P-value	Alpha Level	Decision
Administrators	60	3.14	.417					Sig
Secretaries	40	3.32	.440	118	-2.384	.019	0.05	p<0.05

Source: Survey Data 2022

The result in table 7 showed t-test analysis of difference in the mean rating of administrators and secretaries on the extent to which file level and share level security strategies ensure safety of digital documents in Office Systems Management. It can be seen from the table that the observed probability value (p-value) is .019 which is less than 0.05, the chosen alpha level t(118)= -2.384 p<0.05. Since the p-value is less than the chosen alpha level, the null hypothesis is therefore rejected. This implies that there is a significant difference in the mean ratings of administrators and secretaries on the extent to which file level and share level security strategies ensures the safety of digital documents in Office Systems Management, the difference being in the level of rating.

Hypothesis 4
The administrators and secretaries do not differ significantly in their mean ratings on the extent to which encryption strategies ensure safety of digital documents.

Table 8
T-test Analysis of Difference in the Mean Ratings of Administrators and Secretaries on the Extent to which Encryption Strategies Ensures Safety of Digital Documents

Group	N	X	SD	DF	t	P-value	Alpha Level	Decision
Administrators	60	3.14	.481					Sig
Secretaries	40	3.32	.438	118	-2.218	.028	0.05	p<0.05

Source: Survey Data 2022

Table 8 showed t-test analysis of the mean ratings of administrators and secretaries on the extent to which encryption strategies ensures the safety of digital documents in Office System Management. It can be deduced from the table that the observed probability value (p-value) or sig at 0.05 level of significance with degree of freedom 118 is .028 which is less than the chosen alpha level t(118)= -2.218 p>0.05. Since the p-value is less than the chosen alpha level, 0.05 the null hypothesis is rejected. This implies administrators and secretaries differ significantly in their mean rating on the extent to which encryption strategies ensure the safety of digital documents in Office Systems Management. Again this is in the level of rating since all the strategies were rated as ensuring safety of digital documents.

Discussion of Findings

The findings in table 1 showed the backup strategies that can be employed by organizations to ensure safety of their digital documents. The grand mean of 3.43 gives clear evidence that back-up strategies ensures the safety of digital documents. The use of backup strategies for safety of documents or records was supported by the study of Ibezim (2018) who opined that hard disk or tapes should be used for storage backup to secure documents. Such disks should be stored in safes that can withstand fire and floods.

The study also revealed that password strategies ensure the safety of digital documents with a grand mean of 3.17. Good password practices are critical to the security of documents. Charoen (2014) identified password as an important strategy for ensuring the safety of records. McDonald's (2001) also added that the most common way of access control is through the use of passwords. He however warned that organizations need to note that in times of employee turnover, there have been reported cases of former employees accessing the organizations system to distort data and cause damage to databases because they know the password. Hence, changing passwords regularly is also very important.

Further revelations from this study are that file level and share level strategies including encryption strategies are ways in which companies can ensure the safety of their digital documents. This was evidenced with grand means of 3.23 and 3.55 respectively.

Nasieku (2012) listed data encryption by use of a key to prevent unauthorized users from accessing data as a safe security practice. According to Nova and Nova (2013) authentication through file level and share level security strategies ensures that only legitimate users are allowed to gain access into a system or a network.

Conclusion

The development of strategies for ensuring safety of digital documents is a challenge to most organizations. It was concluded in this study that backup, passwords, encryption, file level and share level security strategies can ensure safety of digital documents in Office Systems Management. Therefore, organizations should apply these strategies to ensure safety of their digital documents.

Recommendations

Based on the findings of this study, the following recommendations are made:

1. Organizations should secure their digital documents through the use of passwords with lower/upper case characters including numbers and symbols.
2. That organization should create backups for their digital documents
3. That organizations should use file level and share level security to ensure safety of digital documents.
4. Organization should use data encryption to prevent unauthorized users from accessing their documents.

References

Aigbe, P., & Akpojaro, J. (2014). Analysis of security issues in e-payment systems. International Journal of Computer Applications, 108 (10), 10-14. Retrieved from http://dx.doi.org/10.5120/18946-9993

Chao, C. (2015). Implementing a paperless system for small and medium sized businesses (SMBs): A master's thesis presented to the interdisciplinary studies programme, University of Oregon

Charoen, D, (2014). Password security. International Journal of Security (IJS), 8 (1). Retrieved from https://online library.wiley.com

Dykman, C. A., & Davis, C. K. (2012). Addressing Resistance to workflow automation. Journal of Leadership,

Accountability and Ethics, 9 (3), 115-123.

Frear, H. (2014). Fear of filing? EDM can help with paper overload and building customer relationship. *Credit Control,* 35(314): 87 – 89. Http://connection.ebscohost.com/c/articles/98709811/fear-filing-edm-can-help-paper-overload-building-customer-relationships.

Ibezim, N.C (2018) Assessment of Electronics management practices adopted in tertiary institutions in Rivers state, Nigeria. An unpublished M.Sc.project, Department of Business Education, University of Nigeria, Nsukka

Kissel, J. (2013). Embracing the nearly paperless future. Macworld 30(10) 76 – 77 Http://connectionebscohost.com/c/articles/901833419/embracing-nearlypaperless-future

McDonalds, B. (2001). E-commerce. Retrieved from http://www.zdnet.com

Mills-Senn, P. (2014). How safe are digital documents? University business.com/article/how-safe-are-your-digital documents

Nasieku, A.P. (2012). A frame work for managing electronic records The case of MOI University presented at SCESAL, 20th Conference, Kenya. Retrieved from Shttp://www.scesai.edu.au/.org on may, 21st 2018.

Nova, S.M. and Nova,Y.L. (2013). Complex passwords: How far is too far? The role of cognitive load employee productivity *Online Journal of Applied Knowledge of Management1(1).*