Scientific Research Publishing

Open Journal of Applied Sciences, 2022, 12, 2124-2134
https://www.scirp.org/journal/ojapps
ISSN Online: 2165-3925
ISSN Print: 2165-3917

Flaws in the Field of Digital Security in the Workplace: Case of Companies in Burkina Faso

Yanogo Kiswendsida Jean Hermann, Ouedraogo Tounwendyam Frederic

Institute of Computer Engineering and Telecommunication Polytechnic, School of Ouagadougou, Ouagadougou, Burkina Faso
Email: yanogohermann@yahoo.fr

How to cite this paper: Hermann, Y.K.J. and Frederic, O.T. (2022) Flaws in the Field of Digital Security in the Workplace: Case of Companies in Burkina Faso. *Open Journal of Applied Sciences*, **12**, 2124-2134.
https://doi.org/10.4236/ojapps.2022.1212146

Received: November 2, 2022
Accepted: December 26, 2022
Published: December 29, 2022

Abstract

Digital in the daily life of companies undeniably leads them to use services and applications of all kinds. Companies in their permanent quest for the exchange of information devote themselves to the use of the Internet which nowadays constitutes an open door for the birth of several types of faults, some of which are unknown to certain digital professionals in the field. Corporate. The purpose of this research is to show the probable existence of digital security flaws in the daily activities carried out by companies in Burkina Faso. In companies in Burkina Faso, we seem to see a way of working that does not respect the standards and safety standards prescribed by ISO 27001. We seem to see a way of working based on the result of the gain and not on the securities measures and integrity of critical data, data confidentiality, management and prevention of possible security risks related to their activities. We seem to be witnessing in companies the immanent presence of faults which could be the work of the users of the system, of the infrastructure used which is outdated or badly configured, of software anomalies linked to programming errors, and to poor implementation of the security policy within the companies. This research is important because it exposes the handicaps that companies have in terms of digital security. The expected result is to bring out existing flaws that are not taken seriously by IT staff and propose possible solutions to overcome these security risks.

Keywords

Security Risks, Digital Security Flaws, Integrity of Critical Data

1. Introduction

The daily work in companies in Burkina Faso could be peppered with security breaches which could consciously or unconsciously hinder the smooth running

or even put the company at risk in terms of digital security. Security vulnerabilities are recurrent when the necessary measures are not taken to comply with norms and standards. IT security must be focused on protection against risks and must take into account the elements to be protected such as data, equipment, users, awareness of the risks that weigh on the company [1]. We see this while many companies do not adapt to it. In a company, it is imperative to know the bases relating to the various threats and to improve the knowledge of good practices relating to collective security [2]. It is important to emphasize that the growing interconnectivity of systems, the use of standard software or hardware, the growing outsourcing of IT services create factors for the spread of attacks and cyber disasters on a planetary scale [3]. It seems essential for IT workers in companies in Burkina Faso to look into the flaws that exist within their structure. The contribution to this research is to show the probable and unknown existence of digital faults in companies in Burkina Faso, and which are unknown to professionals in the field, and to propose anticipatory solutions for resolution. The research is essentially declined on the method used, the result obtained then a proposal for a solution, and in order to the conclusion.

2. Research Methodology Used

Our research methodology focus on the approaches used, research methods, research techniques, and the survey plan. To carry out this research wisely, we used the mixed approach which is both quantitative and qualitative. The quantitative approach allowed us to collect numerical information on the flaws, their frequency, and their management in the company.

The qualitative approach allowed us to understand the phenomenon of recurrence and persistence of faults in business, to prove that it exists by using tools such as analyses. The following methods are used.

2.1. Analytical Method

This method consisted in analyzing the information on the faults coming from each of the units surveyed. This information comes from the interviews, the difficulties experienced, that we made during our stay within the companies.

2.2. The Descriptive Method

In this method, observation allows us to explain the phenomenon of flaws by describing situations and facts experienced.

We collect data based on the description of the situation of the faults in the company, and based on observations and real facts. Before going to the field, we draw up a grid in our register to collect data.

The technique used in the research is:

The technique of the interview

During the interview, we ask a set of questions to the people in charge of managing the digital system. The answers to these questions are listed. Then we

proceed to the analysis phase which consists in analyzing the posture, the availability, the way of responding as well as the responses obtained.

2.3. Data Collection Plan

Our primary data is obtained through a questionnaire and interviews with IT professionals, as well as service providers directly involved in the company's service chain. Our secondary data is through documentation. We use the snowball method.

Table 1 shows the types of data collected and the techniques used to collect them.

2.4. Data Analysis Plan

Data analysis is done with SPSS software. We analyze the information we obtain (graphs, diagrams, parametric and non-parametric tests). Graphs and diagrams allow us to appreciate our variables, and to illustrate the results of our research:

Software used	Data analyzed
SPSS 16	- Graphics; - Diagrams; - Parametric and non-parametric tests.
SPSS 16	Results checking based on our objectives.

2.5. Cyber Threat in Companies in Burkina Faso

It is news that data thefts have become lucrative activities to such an extent that isolated people are no longer the only ones to commit criminal acts. Indeed, the threat increasingly comes from well-structured organizations. Organizations sell collected information for a business. In fact, companies in Burkina Faso, like any other country, are becoming a potential target. The scale of this traffic makes obsolete and ineffective the little protection tips that many companies apply thinking of protecting themselves but which are in reality ineffective.

All organizations face this situation of insecurity. There are two ways of hacking. We can distinguish mass piracy: this implies that the pirate does not target anyone, but digital equipment with vulnerabilities that can be exploited. This consists of recovering unprotected data on equipment, if necessary stealing identities.

In case the hack is targeted. Targeting is a function of rank, function of the person. It is essential that the user who uses the internet tool in the company

Table 1. Data collection plan.

Types of data collected	Techniques used
- Primary Data	Interviews with IT professionals
	A questionnaire
- Secondary Data	Documentation

avoids trap messages such as game winnings, prompts to configure the password of any account. Sometimes it is a question of common sense. When you use the internet and new technologies and you receive electronic gifts while you are at a certain level of decision and responsibility, vigilance becomes mandatory at this time.

Hackers are constantly on the lookout for breaking into corporate computer systems. These companies are not always aware of this, without an effective warning system. A computer hack can cause lasting disruption, and even the loss of confidential information or even espionage.

3. Sample Determination

Respondents are the people who are directly in charge of the company's IT infrastructure. The statistical unit is the person in charge of the company's IT system.

Sample Size Calculation

Sampling is the operation which consists in taking a certain number of elements to be treated or observed, that is to say that the sample is a subset of the population. For our case, we use the formula that allows us to determine the sample size using a 10% margin of error. We then apply:

$$N = Z^2 \&^* P^* Q / e^2$$

& = 0.5 implies that $Z = 1.96$;

$P = 0.5$;

$Q = 1 - p = 0.5$;

E = between 1 and 10%;

N = represents the sample size;

Z^2 = reduced center normal law;

& = represents the degree of confidence;

E^2 = represents the maximum or systematic error.

We will therefore have

$N = 1.962 \times 0.5 \times 0.5/0.12 = 0.2401/0.01 = 97$.

4. Presentation, Analysis and Interpretation of Results

The survey allowed us to collect very useful information for our analysis. Our result consists in interpreting the digraphs; the graphs that come from the data entered in SPSS.

The graphs below show the conclusions of our tests on SPSS.

4.1. Flaws Related to User Works

Are users allowed to use their own computer equipment in the network?

Table 2 shows that when asked whether users are allowed to use their own computer equipment in the network, we end up with 64.9% of companies that

Table 2. Frequency of use of personal tools in the network.

Are users allowed to use their own IT equipment in the network?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oui	63	64.9	64.9	64.9
	Non	34	35.1	35.1	100.0
	Total	97	100.0	100.0	

allow it. This shows a lack of taking security vulnerabilities seriously. However, we know that the use of personal devices in a company network constitutes a security breach within the company. Indeed, Bring Your Own Devices increases in information security vulnerabilities and risks [4]. The use of BYOD brings security risks and threats [5].

Figure 1 shows the frequency, the percent, the valid percent and the cumulative percent of use of personal tools in the network.

To the question of whether companies have a detection mechanism in case a user or any person tries to use their equipment in the network without authorization, the finding is as follows.

4.2. Flaws Related to the Misconfiguration of the System

In Table 3, we find that 94.8% of companies do not have an intrusion detection mechanism against 5.2 that use one. These figures show that companies that use digital tools in the process of their daily activities do not give enough consideration to the importance of this security flaw. We know this during the capital importance of using detection mechanisms within a company. Intrusion detection system is one of the important ways to achieve high security in computer networks and used to thwart different attacks [6]. By using that, the companies will increase their safety. The standards in term of security commend to use Intrusion detection system. Intrusion detection systems detect advanced threats and reduce false positives [7].

Figure 2 shows the frequency, the percent, the valid percent and the cumulative percent of the statistics on detection mechanisms.

4.3. Flaws Related to Equipment that Is Outdated

In Table 4 we find that 56.7% of companies renew their equipment only if the equipment is no longer usable and 17.5% do so every 10 years. However, we know the importance of renewal and the security breaches that non-renewal can cause. Indeed, technology watch must be part of the company's strategies [8]. Technological acquisition enhances its technological resources and skills within the company [9].

Figure 3 shows the frequency, the percent, the valid percent and the cumulative percent of the time taken before making a change.

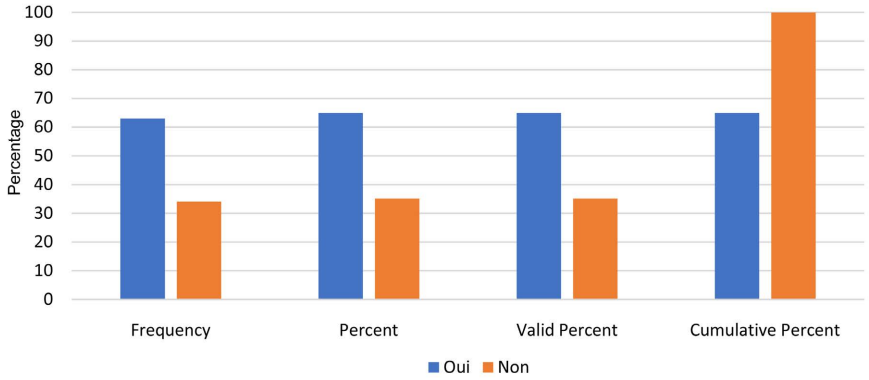

Figure 1. Frequency of use of personal tools in the network.

Table 3. Statistics on detection mechanisms.

Do you have network intrusion detection mechanisms?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oui	5	5.2	5.2	5.2
	Non	92	94.8	94.8	100.0
	Total	97	100.0	100.0	

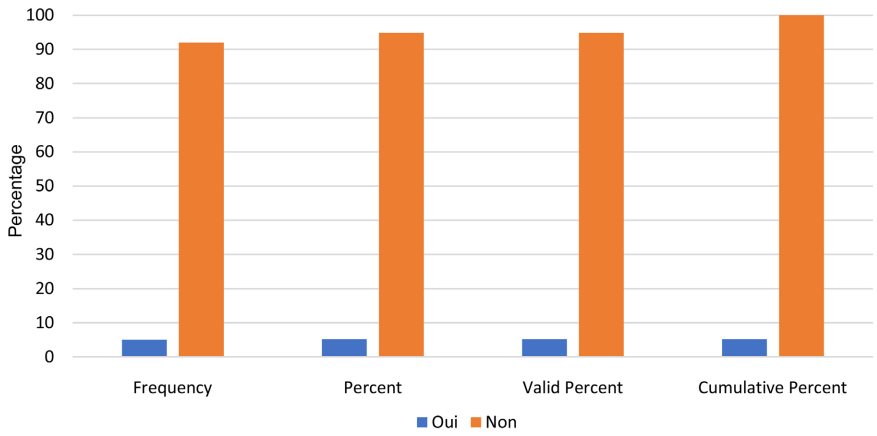

Figure 2. Statistics on detection mechanisms.

Table 4. Statistics on the frequency of changing equipment.

How often do you change your equipment?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Chaque 10 ans	17	17.5	17.5	17.5
	Chaque 5 ans	23	23.7	23.7	41.2
	Uniquement quand les équipements sont inutilisables	55	56.7	56.7	97.9
	Autres	2	2.1	2.1	100.0
	Total	97	100.0	100.0	

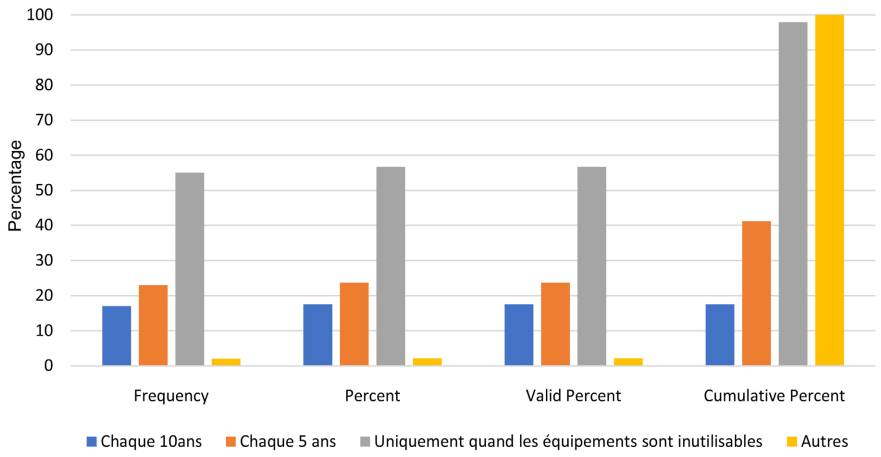

Figure 3. Time taken before making a change.

4.4. Flaws Related to the Company's Poor Security Policy

Table 5 shows the statistics on penetration testing. We know that any company must perform permanent penetration tests because it allows them to detect vulnerabilities in their security. A company that does not perform penetration testing exposes itself to security risks such as permanent attacks. Penetration testing is one such security measure that aims to uncover the security vulnerabilities in the system. Due to the dynamic aspect of cyberspace and technology, advanced or more unusual penetration testing mechanisms need to be employed to deal with the emerging vulnerabilities and security threats in cyberspace [10]. Penetration testing techniques helps to determine whether the arrangements in securing system are working properly or not by fixing those security gaps [11].

Figure 4 shows the frequency, the percent, the valid percent and the cumulative percent of penetration test frequency.

4.5. Flaws Related to Software Usage Anomalies (Non-Authentic Operating System)

Table 6 indicates that original Windows operating systems can guarantee users the quality and functionality they have come to expect, including access to all content available for download, updates and enhanced features. However, we know that updates are very important. Unlicensed systems do not provide access to all expected functionality. The licensed operating system gives an optimization, efficiency, or even profitability [12].

4.6. Flaws Linked to a Lack of Retraining of Employees

In Table 7, we find that 45.4% of companies train their staff only when there is only a budget available. 11.3% of companies do not train their IT professionals at all. 32% of companies wait until there is a new technology before training their IT professional. We know that technology is constantly changing. Therefore, if IT professionals are not up to date with this evolution, a certain number of things escape them. Training gives the best utilization of Human resources,

Table 5. Statistics on penetration testing.

Effectuez-vous des tests de pénétration permanente					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oui	4	4.1	4.1	4.1
	Non	93	95.9	95.9	100.0
	Total	97	100.0	100.0	

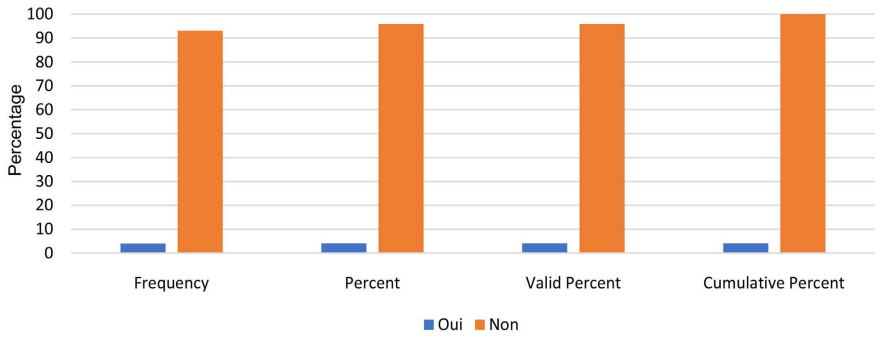

Figure 4. Penetration test frequency.

Table 6. Statistics on licensed operating systems.

Are the operating systems licensed?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oui	30	30.9	30.9	30.9
	Non	67	69.1	69.1	100.0
	Total	97	100.0	100.0	

Table 7. Statistics of IT personnel training in digital security.

Statistics of IT personnel training in digital security					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Chaque 6 mois	2	2.1	2.1	2.1
	Chaque 1 an	3	3.1	3.1	5.2
	Chaque 2 ans	2	2.1	2.1	7.2
	Autres	4	4.1	4.1	11.3
	Pas du tout	11	11.3	11.3	22.7
	Quand il y a un budget disponible	44	45.4	45.4	68.0
	Quand il y a une nouvelle technologie disponible	31	32.0	32.0	100.0
	Total	97	100.0	100.0	

upgrade capacity advancement, blast usefulness, improving hierarchical lifestyle, upgrade excellent and assurance, blast benefits, upgrading corporate ethical quality and picture [13]. Training is one of the most important investments because it enhances the knowledge, skills, attitudes and behavior of employees [14].

Figure 5 shows the frequency, the percent, the valid percent and the cumulative percent of training of professionals in digital security.

5. Determination of Support for the Vulnerabilities Found

Security practices such as Audits that often focus on penetration testing are performed to find flaws in some types of vulnerability & use tools, which have been tailored to resolve certain risks [15]. In view of the flaws observed in the companies during our research, the following solutions for handling these flaws are as follows (Table 8).

Proposals of a Model of Solutions Allowing IT Professionals to Always Be at the Forefront of the Existential Evolution of Flaws

One of the best solutions to stay at the forefront of developments would be to put in place a technology watch policy. The elements of this technology watch are listed in Table 9 below.

The following proposals (Table 10) can make it possible to anticipate and secure as to the existence of new flaws to come. The implementation of a vulnerability watch is useful.

Table 8. Vulnerability support.

Types of flaws	Recommended solutions
Authorization to use personal IT tools in the company network.	- Set up mechanisms to restrict and control the use of these tools (GPO etc…) and encourage user awareness.
Lack of intrusion detection mechanisms.	- Deploy hardware or software solutions for detecting and preventing intrusions.
Failure to change computer and digital equipment in general within a reasonable time..	- Avoid obsolete equipment by replacing it frequently (updating).
The non-implementation of penetration testing periodically..	- Encourage, include in the security policy, and conduct periodic penetration tests to detect vulnerabilities in the company.
Using non-genuine operating system.	- Use licensed operating systems (in accordance with Microsoft).
Use of outdated operating system.	- Use operating systems whose technical support is still valid with Microsoft.
Lack of recurrent training for IT professionals.	- Set up in the security policy a continuous and periodic training plan.

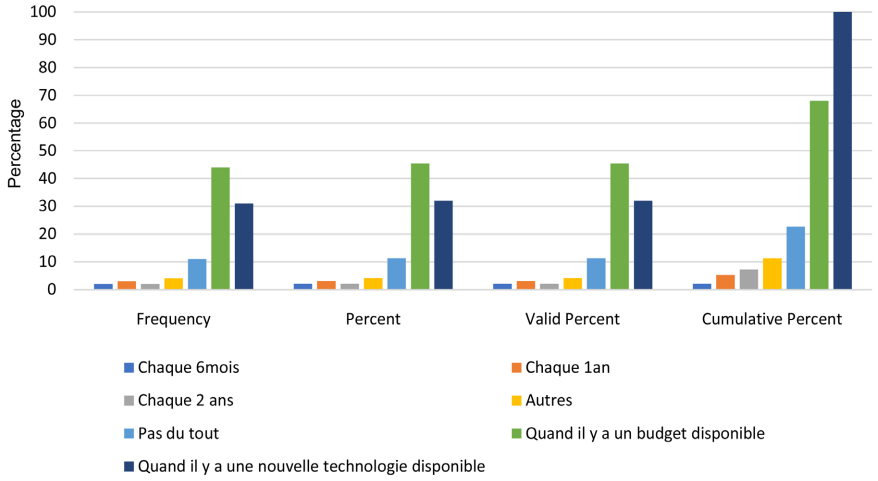

Figure 5. Frequency of training of professionals in digital security.

Table 9. Technology watch solution.

Proposal for a technology watch solution
1) Set up an internal team responsible for monitoring the technological innovations that are available on the market.
2) Use technological monitoring tools such as Google alert which allows you to be informed of news by email or the use of monitoring software such as AMI.
3) Encourage challenge within the company to get IT professionals more interested in learning.

Table 10. Proposal of anticipatory solutions.

Proposal of anticipatory solutions
1) Implementing a vulnerability monitoring policy reduces the risk of breaches and attacks.
2) Test and test the information system to ensure its robustness using certain test tools.
3) Implement a risk and vulnerability assessment approach.
4) Frequently audit the information system.

6. Conclusion

The research which relates to the study of flaws in the field of digital security in the workplace in Burkina Faso has enabled us to highlight the existing flaws which are linked to users, to a bad security policy due to a lack of setting up detection, training and awareness mechanisms, the use of unsuitable or even obsolete operating systems and equipment. This research has allowed us to provide solutions that allow IT professionals to stay at the cutting edge of technology in order to better deal with this ever-evolving situation of security breaches. It is important for businesses to make this a priority to ensure their survival and success in this growing world of technology.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Yende, R. (2018) Support de Cours de Sécurité Informatique et Crypto.

[2] Prieur, B. (2020) Fondamentaux de la sécurité informatique utilisateur. Doctoral Dissertation, IT-Akademy.

[3] Héon, S. and Parsoire, D. (2017) La couverture du cyber-risque. *Revue d'économie financière*, **2**, 169-182. https://doi.org/10.3917/ecofi.126.0169

[4] Ratchford, M., Wang, P. and Sbeit, R.O. (2018) BYOD Security Risks and Mitigations. In: Latifi, S., Ed., *Information Technology: New Generations*, Springer, Cham, 193-197. https://doi.org/10.1007/978-3-319-54978-1_27

[5] Tchao, E.T., Ansah, R.Y. and Djane, S.D. (2017) Barrier Free Internet Access: Evaluating the Cyber Security Risk Posed by the Adoption of Bring Your Own Devices to e-Learning Network Infrastructure.

[6] Manzoor, I. and Kumar, N. (2017) A Feature Reduced Intrusion Detection System Using ANN Classifier. *Expert Systems with Applications*, **88**, 249-257. https://doi.org/10.1016/j.eswa.2017.07.005

[7] Kumar, S., Viinikainen, A. and Hamalainen, T. (2016) Machine Learning Classification Model for Network Based Intrusion Detection System. 2016 11*th International Conference for Internet Technology and Secured Transactions* (*ICITST*), Barcelona, 5-7 December 2016, 242-249. https://doi.org/10.1109/ICITST.2016.7856705

[8] Lemieux, S. (2018) Évolution technologique à vitesse grand V-Comment rester dans la course? *Gestion*, **43**, 56-61. https://doi.org/10.3917/riges.434.0056

[9] Ouiddir, C. and Ouikene, N. (2020) L'innovation et le management des ressources technologiques: Cas de l'entreprise Electro-Industries Azazga. Doctoral Dissertation, Université Mouloud Mammeri, Tizi-Ouzou.

[10] Arfaj, B., Mishra, S. and AlShehri, M. (2022) Efficacy of Unconventional Penetration Testing Practices. *Intelligent Automation and Soft Computing*, **31**, 223-239. https://doi.org/10.32604/iasc.2022.019485

[11] Khera, Y., Kumar, D. and Garg, N. (2019) Analysis and Impact of Vulnerability Assessment and Penetration Testing. 2019 *International Conference on Machine Learning, Big Data, Cloud and Parallel Computing* (*COMITCon*), Faridabad, 14-16 February 2019, 525-530. https://doi.org/10.1109/COMITCon.2019.8862224

[12] Werthner, H. (2022) From Absolute Nonsense to the World's Operating System. *Electronic Markets*, **32**, 145-151. https://doi.org/10.1007/s12525-021-00508-w

[13] Haralayya, B. (2022) Employees Training and Development at Mgssk Ltd Bhalki. *Iconic Research and Engineering Journals*, **5**, 184-196.

[14] Laing, I.F. (2021) The Impact of Training and Development on Worker Performance and Productivity in Public Sector Organizations: A Case Study of Ghana Ports and Harbours Authority. *International Research Journal of Business and Strategic Management*, **2**, 438-449.

[15] Nabi, F., Yong, J., Tao, X., Malhi, M.S., Farhan, M. and Mahmood, U. (2021) Process of Security Assurance Technique for Application Functional Logic in E-Commerce Systems. *Journal of Information Security*, **12**, 189-211. https://doi.org/10.4236/jis.2021.123010