Scientific Research Publishing

Journal of Information Security, 2022, 13, 76-84
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Study on the Instability of Information Systems and Security Risks in the Public Administration: Case of Burkina Faso Public Administration

Yanogo Kiswendsida Jean Hermann

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. (2022) Study on the Instability of Information Systems and Security Risks in the Public Administration: Case of Burkina Faso Public Administration. *Journal of Information Security*, **13**, 76-84.
https://doi.org/10.4236/jis.2022.132005

Received: January 2, 2022
Accepted: April 22, 2022
Published: April 25, 2022

Abstract

The purpose of this research is to show the instability and the security risks of the information system in Burkina-Faso public administration. In this paper, witnessing unsatisfactory services such as government messaging (mailer.gov.bf) as well as G-cloud services which are the government cloud were studied. The behavior of user agents on the administration's IT infrastructures which could expose the information system to security risks was also studied. The expected result shows evidence of the weakness of the public administration information system and provides some recommendation.

Keywords

Mailer.gov.bf, Resina Network, G-Cloud, Burkina-Faso Public Administration

1. Introduction

The research is carried out in Burkina Faso which is a Sahelian country with Ouagadougou as a capital. The research focused more on public services located in the capital Ouagadougou and in the economic capital Bobo Dioulasso. Previous research pointing to the weakness of the IS has been raised such as the case of attacks on public administration websites which caused a downtime for a while. The problems that I want to find a solution concern the problems related to the messaging (mailer.gov.bf), to the G-cloud, as well as to the problems related to the misuse of the IT infrastructure by the agents.

The information system of Burkina Faso public administration can be defined as a set of resources which are stored, then processed and distributed through a computer network. The public administration information system is the strong

link in productivity and business growth. We can also say that information system (IS) is the study of networks of hardware and software that organizations use to collect, filter, and process, create, and distribute data [1]. The same source indicates that Information systems are combinations of hardware, software, and telecommunications networks that companies build and use to collect, create, and distribute useful data [1]. When the IS data is not available on time, it causes an availability problem. However, we seem to see continued instability in the Burkina Faso administration's Webmail and G-cloud services.

Cyber-attacks are defined as an exploitation of cyberspace for the purpose of accessing unauthorized or secure information, spying, disabling of networks, and stealing both data and money [2]. The same source indicates that it consists of Operations, whether in offence or defence, intended to alter, delete, corrupt, or deny access to computer data or software for the purposes of (a) propaganda or deception; and/or (b) partly or totally disrupting the functioning of the targeted computer, computer system or network, and related computer-operated physical infrastructure [2]. Burkina Faso public administration is interconnected by the Résina network which is the local administration network on the one hand as well as the G-cloud which is the cloud of Burkina Faso's government.

The availability of information is crucial for proper functioning and decision making. When information is not available at the right time, decision making and continuity of service are difficult and constitute an economic loss. The question arises as to whether the problems of instability in information systems and the consequences that this generates are perceived and measured by decision-makers?

Indeed, information system unavailability can lead to disastrous consequences ranging from delays and cancellation to a loss of millions of dollars [3].

It is important to consider that the complexity of information system protection against related threats and their implementation ways (attacks) is significant. Everyday new vulnerabilities of software could be identified and therefore new ways for attackers appear and this could serious damages [4]. The mismanagement of system users, the lack of technological watch, and the lack of sharp and seasoned practical skills of a good number of IT (information technology) managers could lead to cyber-attacks. Indeed, the cyber-attack on Georgia in the USA was launched against the governmental agencies, state bodies, courts, academia, NGOs, as well as commercial and private financial targets. Many of the affected websites were defaced [5].

Are the webmail and the G-cloud of the public administration of Burkina-Faso unstable?

The system users in view of their management, the lack of extensive practical skills of the actors in charge of the management of the information system would not constitute a potential source of vulnerabilities?

2. Research Methodology Used

According to JM de Ketele and x.ROEGIERS (1996: 139) consider a research

method as a more or less structured and coherent whole of principle supposed to be oriented with the stages of the process with which it is inscribed.

For our research, we will use the quantitative and qualitative method.

2.1. The Quantitative Method

The quantitative method is a method that shows objective measurements and the statistical, mathematical, or numerical analysis of data collected using different way such as polls and questionnaires. This method allowed us to quantify and quantify the results of the research. It helps us to present the results in the form of graphs, tables. This method turned out to be important because we were able to determine in what exact proportion the results of the research are brought. The software used is SPSS.

2.2. The Qualitative Method

The qualitative method is a method that does not involve measurement, Statistics or numerical analysis. It's a research based on existing documentation.

The objective of the qualitative research is to develop concepts which will make it possible to apprehend social situations in natural contexts. The qualitative method does not seek to quantify or measure, it most often consists of collecting data such as documentaries facilitating an interpretative process

2.3. Sample Determination

Our sample concerns the employees (users) of the Webmail, G-cloud system of Burkina-Faso public administration. To this end, a questionnaire is sent to the users of the system.

According to Alain Bouchard, for a population of more than 1000 individuals, for a margin of error of 10% with an accuracy of 95%, 94 is taken as a sample. 94 represents our sample.

3. Presentation of the G-Cloud and Webmail of Burkina Faso Public Administration

The objective of the public administration's G-cloud of Burkina-Faso is to accelerate and facilitate the development of solutions and services in the field of e-education, e-government, telemedicine, e-commerce, e-services for the benefit of the rural world, for citizens of the administration and the private sector. It is managed by ANPTIC (the national agency for the promotion of ICT). This objective seems not to be reached probably due to the recurring instabilities of the system. It seems that the architecture of the system is not well designed. This shared infrastructure for hosting services to ensure its digital sovereignty that Burkina Faso has acquired does not seem to achieve these objectives and seems to be giving a hard time, as evidenced by the many complaints about the instability of the system. Also, the Webmail supposed to facilitate the communications between agents of the administration seems to have difficulty in respecting

the standards of availability that this infrastructure should have. Indeed, we would ask ourselves the question whether the ICTs intended to lead production in the administration would not constitute a factor causing the slowness of decision-making and a setback of the targeted objectives which would consist in digitizing the public administration. We seem to see that in the case of G-cloud, resources are not permanently available to users.

4. Presentation, Analysis and Interpretation of Results

4.1. Point of View on the Stability of the Web Mail Services

When asked if users find that the services of mailer.gov.bf are unstable (regular failures, emails sent and not transmitted etc...) we obtain the following results:

Statistics		
Do you find that the mailer's services are unstable with frequent breakdowns, emails sent and not transmitted etc...?		
NOT	Valid	94
	Missing	0

Table 1. Do you find that the mailer's services are unstable with frequent breakdowns, emails sent and not transmitted etc...?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	YES	80	85.1	85.1	85.1
	NO	14	14.9	14.9	100.0
	Total	94	100.0	100.0	

The table was obtained based on the questionnaire result that we entered on the software spss.

It gives us a result of frequency, percent, and valid percent of 94 persons that have answered the questionnaire. As we can see the number of people that confirmed by the Yes answer is respectively 80, 85.1, for frequency and percentage. The number of people that confirmed by the No answer is respectively 14 and 14.9. We can conclude that most that ore that 85 percent is agreed that the mailer's services are unstable.

Figure 1 was obtained based on Table 1. It shows clearly the proportion on which people recognized the mailer's problems.

We find that 85.1% of the people questioned affirm that the services of the mailer are unstable compared to 14.9%. This could not be without consequences for the public administration. It is characterized by the permanent non-availability of data, hence slowness in decision-making and economic losses. Indeed, Unavailability can be seen as the time during which the user can no longer work efficiently due to a malfunction of the computer system. Since this tool is at the heart of the majority of organizations, the delay inevitably leads to a loss of turnover and

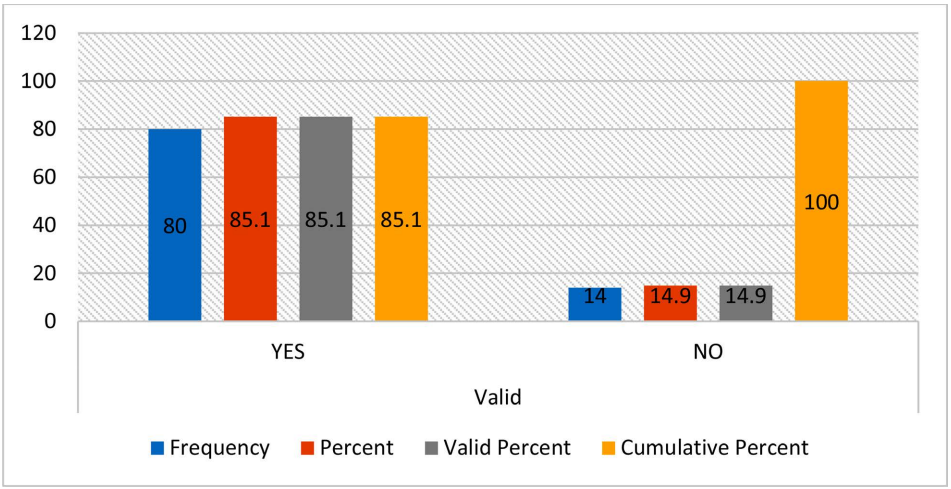

Figure 1. Statistic on mailer's services.

destroy the institution credibility.

4.2. Situation of Non-Deactivated E-Mail Accounts

When asked whether the public administration agents managed to communicate with other agents who left the public administration and still have their accounts active on the.gov.bf mailer, we obtain the following results:

Statistics		
Do you ever communicate by email with people who have left the public administration and who still use their.gov.bf email accounts?		
NOT	Valid	94
	Missing	0

Table 2. Do you ever communicate by email with people who have left the public administration and who still use their.gov.bf email accounts?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	YES	85	90.4	90.4	90.4
	NO	9	9.6	9.6	100.0
	Total	94	100.0	100.0	

Table 2 is also the result of the 94 persons' answers that we introduced on SPSS software one by one in other to fully see the proportion on how people communicate with other people that left the public administration. We see that 85% recognize to still communicate with people that are not still in the administration through the domain.gov.bf. It means that their accounts are still active on the servers even those they're not administration's workers again compare to 9%.

As we can see in Figure 2, an agent who leaves the public service should have his account deactivated. We note that some agents who are no longer in office still have the possibility of communicating via their.gov.bf mail account and this

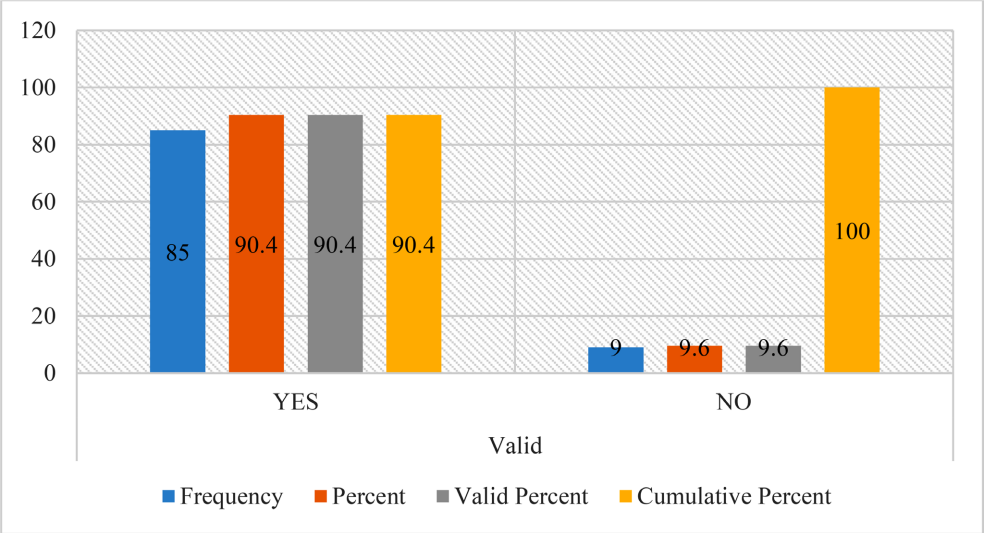

Figure 2. Statistic of email communication with outsider.

is not without risk. He could initiate a hoax and wreak havoc on the administration. Indeed, Ransomware is software that takes data hostage, encrypts it and then demands a ransom from its owner. The administration mail server could be attacked by agents who are no longer in the public service. Most of attacks are done via phishing email or on social networks.

4.3. Government Cloud Satisfaction Opinion

We can see in Table 3, when asked whether public administration officials are satisfied with the government cloud, the following results are obtained:

Statistics Are you satisfied with the government cloud services?		
NOT	Valid	94
	Missing	0

Table 3. Statistic on the government cloud.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	YES	18	19.1	19.1	19.1
	NO	76	80.9	80.9	100.0
	Total	94	100.0	100.0	

When asked if users are satisfied with G-cloud services, we find that 80.9% of people surveyed are not satisfied. The problem of satisfaction could be the fact that they are not able to use the cloud all the time. In other word the availability is not permanent and it's not without consequences. Indeed, the service unavailability leads to a major disruption affecting the business environment and the company goals. Hence, utmost care should be taken to scale the availability of

services [6]. This table that we got through the spss software by entering the data we have collected shows that 80.9 percent are satisfied compared to 19.1.

4.4. Point of View on IT Infrastructure Management

When asked whether public administration officials manage the infrastructure put at their disposal well, the following results are obtained:

Statistics		
What do you think of the behavior of administration officials with regard to their use and management of the IT infrastructure made available to them?		
NOT	Valid	94
	Missing	0

Table 4. Statistic on point of view.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Good	9	9,6	9,6	9,6
Risk	23	24,5	24,5	34
Imprudent	30	31,9	31,9	66
Not worried	32	34	34	100
Total	94	100	100	

In Table 4, we find that 31.9% of imprudent behavior and 34% of not worried behavior of the usage of IT infrastructure and this is not without possible consequences. Human acts and errors are the direct and/or indirect cause of the majority of security incidents including both intentional and unintentional misbehaviors. In other word the companies' data breaches are due to exploitation of human weaknesses [7]. This table is based on the data that we have collected and analyzed it through spss to get a broad view based on the frequency and the percentage.

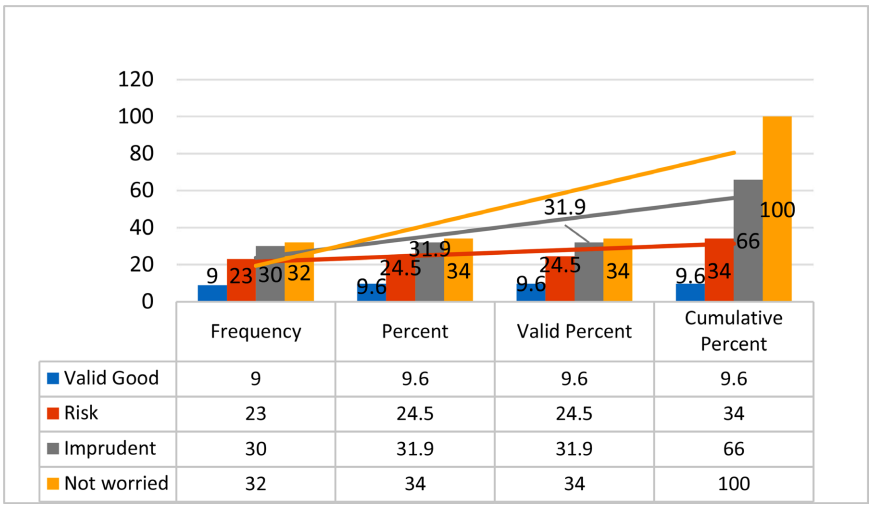

Figure 3. Comparative statistic.

Figure 3 shows the improper use of the system infrastructure that is increasing with a frequency from 9 to 32. The percentage of the improper use is also increasing from 9.6 to 34. The valid percentage goes from 9.6 to 34. We can conclude that there is a risk of security due to the improper usage of the system. The bad usage of the computer infrastructure can be considered as a security risk. Indeed, the actions that workers do deliberately or accidentally can impact the security, the failure of hardware, software, and information systems [8].

The actions that people do in their office describe a class of operational risk characterized by problems caused by the action taken or not taken by those people in a given situation [9].

5. Conclusion and Recommendations

At the end of our study, we found that major difficulties exist in the information system of the public administration and the following proposals can be made.

Proposal of solutions

Instability of mailer.gov.bf services	Audit the architecture and the necessary configurations in order to adapt it to the platform's requirements and security standards
Mail accounts still active for agents who are no longer from the public administration	Set up an email account deactivation policy for any agent who has left the public administration
The behavior of administration officials with regard to their use and management of the IT infrastructure made available to them	Set up a system for monitoring the actions taken by each user and take firm sanctions

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Bourgeois, D. and Bourgeois, D.T. (2014) Information Systems Security. In: *Information Systems for Business and Beyond*. https://ecampusontario.pressbooks.pub/infosysbus/chapter/chapter-6-information-systems-security

[2] Kadivar, M. (2014) Cyber-Attack Attributes. *Technology Innovation Management Review*, **4**, 22-27. https://doi.org/10.22215/timreview/846

[3] Ebad, S.A. (2018) The Influencing Causes of Software Unavailability: A Case Study from Industry. *Software: Practice and Experience*, **48**, 1056-1076. https://doi.org/10.1002/spe.2569

[4] Stetsenko, I.V. and Savchuk, V. (2020) Information System Penetration Testing Using Web Attack Automated Simulation. *International Conference on Computer Science, Engineering and Education Applications*, Springer, Cham, 396-406. https://doi.org/10.1007/978-3-030-55506-1_36

[5] Roguski, P. (2020) Russian Cyber Attacks against Georgia, Public Attributions and Sovereignty in Cyberspace. https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/153044/roguski_russian_cyber_attacks_against_georgia_2020.pdf?sequence=1&isAllowed=y

[6] Cebula, J.L. and Young, L.R. (2010) A Taxonomy of Operational Cyber Security Risks. Carnegie-Mellon University Software Engineering Institute, Pittsburgh.

[7] Khando, K., Gao, S., Islam, S.M. and Salman, A. (2021) Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review. *Computers & Security*, **106**, Article ID: 102267. https://doi.org/10.1016/j.cose.2021.102267

[8] Cebula, J.J., Popeck, M.E. and Young, L.R. (2014) A Taxonomy of Operational Cyber Security Risks Version 2. Carnegie-Mellon University Software Engineering Institute, Pittsburgh. https://doi.org/10.21236/ADA609863

[9] Cérin, C., Coti, C., Delort, P., Diaz, F., Gagnaire, M., Gaumer, Q. and Ville, A. (2013) Downtime Statistics of Current Cloud Solutions. International Working Group on Cloud Computing Resiliency, Tech.Rep. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.601.1031&rep=rep1&type=pdf