



INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND INNOVATIVE STUDIES

ISSN: 2820-7157

Advancing Knowledge, Inspiring Innovation

www.ijsrisjournal.com



PEER REVIEWED
Rigorous & Transparent

DOI: CROSSREF
Member

OPEN ACCESS
For Global Visibility

BI-MONTHLY
Timely Publication

WIDE READERSHIP
High Impact & Visibility

AUTHOR FRIENDLY
Fast | Supportive | Reliable

RECEIVED
17 August 2026

ACCEPTED
09 September 2026

PUBLISHED
1 October 2026

Pages from:

October 2026

Volume 5

Number 5

543 to 551

The severity of cyberattacks in the healthcare sector in the Democratic Republic of Congo

ETUMANGELE TSHITAKA Gabriel¹, BANYAKWA BABINGWA Christophe¹

¹Assistant Lecturer, Department of Computer Science, Higher Pedagogical Institute of Gombe, Kinshasa, Democratic Republic of the Congo (DRC); gabrieletums2015@gmail.com; +243 817 851 599

²Researcher, Department of Computer Science, Higher Pedagogical Institute of Gombe, Kinshasa, Democratic Republic of the Congo (DRC); cbanyakwa@gmail.com; +243 997 756 095

LICENSE



This article is licensed under the
**Creative Commons Attribution
4.0 International License (CC BY 4.0).**

<https://creativecommons.org/licenses/by/4.0/>



PREFIX :

10.63883

— IJSRIS JOURNAL —

OPEN ACCESS



This is an open access article
distributed under the terms of
open access.

ABSTRACT

Information system security is a key issue for digital and technological sovereignty for any entity, organisation or even country that is ambitious and aware of the potential risks and threats arising from a constantly changing environment. The

widespread and gradual digitalisation of our societies is leading us towards a world that is certainly increasingly interconnected, but which also harbours real vulnerabilities in the face of malicious actors. Whilst some organisations have taken the initiative on this issue, the fact remains that, as far as the Democratic Republic of the Congo is concerned, much

remains to be done, particularly in the health sector, where the attention of digital experts has so far been largely absent.

Through this article, we aim to make our contribution to the healthcare sector, and we hope that the proposed cybersecurity measures will be implemented on a case-by-case basis in the various hospitals.

Keywords: Network security – system security, cyber security – cyber threats, healthcare.

1. Research question and significance

Our work focuses, on the one hand, on issues related to cybersecurity as a new strategic challenge for public organisations, particularly healthcare organisations and structures, encompassing both state and non-state actors. On the other hand, we outline the measures and countermeasures to be adopted in the face of potential cyber threats.

In the digital age, the control and management of information are essential tools for responsible governance and resilience in the face of the threats that abound in the digital ecosystem. The use of new technologies (**ICT**) lies at the heart of digital transformation; any organisation worthy of the name in this century should comply with international standards regarding information system security. As in the health and social care sectors, new ways of working have emerged, such as telemedicine, remote diagnostics and operations, remote working, and online social security declarations. In light of these changes, it is imperative that we have confidence in the reliability of the hardware and software resources we use.

1.1. Issue

Our key question is: how can we effectively protect public health organisations, such as hospitals and university hospitals, from cyber threats? What role can the **Chief Information Officer (CIO)** or the head of information systems play in a healthcare setting? What role should the state play in regulating and ensuring a safer and more reliable digital ecosystem?

We will focus on developing countries (with particular attention to the case of the Democratic Republic of the Congo, abbreviated to **DRC**), and we will seek to understand how the implementation of measures and counter-measures can be a significant advantage in the commitment to cybersecurity.

Our observation is that, whilst the Democratic Republic of the Congo has been somewhat slow to establish its position in the field of cybersecurity, as have certain other African countries in the sub-region, we believe that, with the various measures

proposed to combat information system hacking, the implementation of these measures will go a long way towards minimising the risks and cyber-threats that continue to place a heavy strain on information systems and those responsible for them, thereby strengthening the security of information systems through the use of appropriate measures and counter-measures.

1.2. Research methodology

For our research topic, we employed a **documentary and participatory** approach. The documentary method was based on the type of data available, drawing on the vast amount of data found on the internet. We adopted a participatory approach as, throughout the writing process, we conducted interviews with medical staff to gather their views on the issue of cybersecurity in the healthcare sector, thereby identifying useful potential solutions that address the specific network security needs of large hospital centres. We gathered a substantial and reliable volume of information, which we scrutinised in order to analyse it in the light of international cybersecurity standards. This led us to a number of factual observations regarding the digital ecosystem of healthcare organisations in the DRC. Firstly, we laid the foundations by outlining the key aspects of cybersecurity; we also examined what constitutes an information system. We then proposed measures and countermeasures to effectively combat potential cyber threats.

2. Analysis of the current situation

2.1. Regulatory framework

We can state that the African continent is currently experiencing considerable growth in information and communication technologies. This transformation brings with it a host of significant vulnerabilities in the face of cyber threats.

The Congolese government, like other nations around the world, has responded strongly to these cyber threats by prioritising the development of a cybersecurity strategy designed to address this dark side of new information and communication technologies.

In the absence of an appropriate response underpinned by structural governance commensurate with the scale of the challenges, by legislation that is tailored and adaptable to the changing nature and form of illicit practices, and by synergistic collaboration with the private sector, a framework of trust between stakeholders and cooperation at all levels, an immense challenge remains to be overcome. Although significant progress has been made to date, the development

of cybersecurity in Africa remains limited and cybercrime is gaining ground.

In order, therefore, to tackle this daunting array of cyber threats and challenges, the Congolese government has, like many other countries, committed itself to implementing cybersecurity strategies that foster collaboration and trust between state and private-sector actors in the security sectors in the face of the ever-changing landscape of cybercrime. Given its size – the second-largest country in Africa by area, surrounded by nine neighbours – and its potential in terms of natural resources, the Democratic Republic of the Congo, which has only just begun its digital transformation, risks becoming a prime battleground in cyberspace. ***The creation of a resilient, proactive and tailored cybersecurity ecosystem to ensure the protection of citizens, public institutions and enterprises, partnerships, diplomacy, intelligence and so on is therefore essential.***

But how can this be achieved?

First and foremost, let us examine the landscape of hardware and software infrastructure.

2.2. Current state of hardware and software

Whilst in certain sectors (such as banking and telecoms) cybersecurity is more or less regulated, the vast majority of activities – including those in the public service sector – are not subject to even the most basic security regulations, despite having exposure to cyberspace in some cases.

We therefore note that even for hospitals and university teaching hospitals, apart from manual archiving, very few healthcare facilities have switched entirely to electronic systems, with a few exceptions – notably hospitals funded by foreign sources such as **the MOKOLE Hospital Centre**, the **HJ Clinic**, and, very recently, the Kinshasa Referral Hospital (formerly **Maman YEMO**).

These public institutions and healthcare organisations lack secure and reliable information systems. There is a lack of data sharing between these various healthcare organisations. This precarious situation, which falls far short of modern standards, poses a significant challenge to the implementation of information systems (IS); although not yet widespread, such systems could help address potential threats from other digital actors.

The first step towards addressing this shortfall:

- **Is the training of competent staff;**

- **The allocation of financial resources;**
- **The deployment of software infrastructure** such as data centres, etc., to ensure digital sovereignty;
- **The maintenance of information systems.**

Protecting hospitals (where the term ‘hospital’ is used here to refer, in a narrow sense, to any form of healthcare organisation) against cyber risks and future threats involves assessing the current situation and potential threats. The aim is not to pinpoint the risks faced by the information system with absolute precision, but to strategically factor in the significance of the various threats and anticipate how they might evolve. In addition to the threat landscape, another key factor affecting the status quo is the current level of protection afforded to the Democratic Republic of the Congo against cyber risks.

3. Digitalisation of the healthcare sector in the DRC

3.1. The case of digital health

The decentralised government public service, the National Agency for Clinical Engineering, Information and Health Informatics (ANICiiS), is tasked with promoting and developing digital health in the DRC. This involves establishing a strategic technical framework enabling:

- The identification,
- The development,
- The management,
- The roll-out and the maintenance of it applications.

The aim is to promote health informatics in various fields:

- Telemedicine,
- Telehealth,
- Medical robotics,
- Big data and/or open health data,
- Health mapping,
- The use of drones in the healthcare supply chain,
- Maintenance of biomedical equipment,

- Bioinformatics,
- Predictive medicine, etc.

3.2. Experimentation with digital health in the DRC

From a digital perspective, an analysis of the situation within the DRC's healthcare system reveals the following findings:

- There is no operational structural management of the IT equipment stock within the Ministry of Health. In most cases, there is a shortage of electricity supply, particularly in outlying areas.
- As regards applications, several types of software are used at different levels of the healthcare hierarchy, from the central to the peripheral levels. This includes both general-purpose and specialist software designed to meet the specific needs of users, without any consideration of interoperability issues.
- Internet and intranet connectivity varies greatly. However, the central offices of health zones have the potential for internet connectivity via a VSAT network or, in some cases, the 2G or 3G signal from certain communication networks; this still allows for the electronic entry of data.

3.3. Challenges of digital transformation in the healthcare sector

- Lack of standardisation, normalisation and regulation;
- Problems relating to data availability, security and poor data quality;
- Highly variable timeliness in the provision of information and insufficient completeness;
- Operational failures in most of the IT equipment supplied and in ICT infrastructure;
- Unregulated and poorly adapted implementation of business solutions, and a lack of ICT skills;
- Few business applications (office automation, reporting and analysis solutions);
- Difficult and fragmented dissemination of information.

4. Information systems

4.1. Definition

An information system (IS) can be defined technically as a set of interdependent components that collect, process, store and distribute information to support decision-making and control within an organisation.

Information systems can be considered to have **five main components**: *hardware, software, data, people and processes*. The first three are **technological**. The last two components – people and processes – distinguish the concept of information systems from more technical fields, such as computer science. To fully understand information systems, you will need to understand how all these components work together to deliver value to an organisation.

4.2. Types of information systems (IS)

There are several types of information systems; here we list a few, though the list is by no means exhaustive.

Database management systems (DBMS):

These enable data to be stored, organised and managed in a structured manner.

Content Management Systems (CMS):

These facilitate the creation, editing and publication of content on websites.

Customer Relationship Management (CRM) systems:

These systems enable organisations to manage interactions with customers, track sales and manage customer databases.

These systems play different roles within an organisation and are used to meet specific information management needs.

N.B.: The IT system forms part of the technical infrastructure of an information system. Generally speaking, this comprises hardware and software.

5. Terminology

To read and understand this article effectively, it is important to have a better grasp of the key concepts in cybersecurity; we will begin by defining security and its basic properties.

5.1. Security

In computing, the word ‘security’ can have several meanings. More precisely, the concept of security corresponds to the English word ‘security’ and refers to the ability of a computer system to withstand external physical threats (fire, flooding, bombs, etc.) or logical threats (data entry errors, intrusions, hacking, malicious code, etc.).

This is, in fact, the meaning adopted by security audit specialists when they are required to assess IT-related risks for a given organisation.

5.1.1. Fundamental properties of security

Availability: ensuring the IT system continues to function properly.

Integrity: ensuring that data is indeed what it is claimed to be.

Confidentiality: making information unintelligible to anyone other than the parties involved in a transaction.

Although security encompasses other complementary properties, these can be effectively summarised by the first three.

Other examples include: privacy, authenticity, auditability and non-repudiation.

5.1.2. The diversity of security requirements

Security requirements vary depending on the field of application for which cybersecurity standards are to be implemented. Let us recall the three key objectives of cybersecurity: integrity, availability and confidentiality.

For example, in the banking, military and education sectors – to name but a few – the requirements are not necessarily the same across these three primary properties.

By contrast, SICSS systems are characterised in particular by their stringent, and often simultaneous, requirements for confidentiality, integrity and availability, and to a certain extent also for auditability.

In the medical field, integrity (of diagnoses, for example) and availability (urgency) can sometimes be vital, in the strictest sense of the word, but confidentiality is more than just a legal obligation: access to medical information can have significant financial implications for an employer or insurer, but can also be a source of blackmail. The property of auditability is also

very important for strengthening the accountability of healthcare staff.

Similarly, in the social sector, the confidentiality of data relating to individuals and businesses, the integrity of online declarations and payments, the availability of Net-entreprises’ online services (particularly regarding deadlines for declarations and payments), as well as accountability for actions (such as payment by the due date), are all crucial issues

5.2. Cybersecurity

Cybersecurity refers to a set of measures and techniques designed to ensure the protection and integrity of an entity’s data, whether that entity is an individual, a business or, in this case, a healthcare organisation.

Also known *as information systems security*, it helps to safeguard computer networks against the risks of cyberattacks, guarantee the confidentiality and integrity of medical data, and improve the authentication of individuals accessing this data.

IT security also involves providing training for users, to equip them with the knowledge and tools needed to minimise risks.

5.3. Cyberattack

A cyberattack is defined as ‘an attack on IT systems carried out with malicious intent’. It targets various IT devices: computers or servers, whether stand-alone or networked, connected to the internet or not; peripheral equipment such as printers; or communication devices such as mobile phones, smartphones or tablets. There are four types of cyber risks with varying consequences, affecting individuals, public authorities and businesses either directly or indirectly: cybercrime, damage to reputation, espionage and sabotage.”

The constant increase in the frequency, scale and sophistication of these cyberattacks serves as a constant reminder that the fight against cybercrime is now vital.

There are various types of cyberattack, such as those targeting the DNS (DDoS, DNS cache poisoning, DNS spoofing, man-in-the-middle attacks) or attacks aimed directly at users with the aim of obtaining confidential information to commit identity theft (phishing)...

5.4. The different forms of cyberattacks in the healthcare sector

5.4.1. Ransomware

Ransomware is one of the most common forms of cyberattack in the healthcare sector: a hacker encrypts an organisation's data and demands a ransom payment to decrypt it.

The consequences can be disastrous for patient care if medical records are encrypted or rendered inaccessible.

It can also lead to long-term financial losses as the organisation struggles to pay the ransom and recover the data.

5.4.2. Phishing

Phishing is another common form of cyberattack in which hackers use social engineering techniques to gain access to sensitive information or take control of a system.

To do this, they typically send emails containing malicious links or attachments which, once opened, allow them to access the victim's computer or take control of a system.

In the US, 88 per cent of healthcare workers have opened phishing emails.

5.4.3. Theft of personal data

The theft of personal data is a major concern in the healthcare sector. According to the US Department of Health and Human Services, more than 400 incidents involving the theft or loss of unencrypted health information have been recorded since 2009. These incidents have affected a total of nearly 30 million people.

Furthermore, a recent survey revealed that nearly three-quarters of healthcare organisations have suffered a data breach in the past year.

5.4.4. DDoS attacks

A distributed denial-of-service attack involves a flood of fake connection requests directed at a targeted server, forcing it to go offline. During such an attack, numerous endpoints and IoT devices are used as part of a botnet via a malicious infection to participate in this coordinated attack.

DDoS attacks do not carry the same risks of data exfiltration as a ransomware attack, but they have the same operational disruption effects.

The significant advantage of DDoS attacks is that they can cause the same disruption without having to compromise a network, making it easier to deploy them on a much larger scale.

The speed and potential devastation of these attacks have led to their adoption of the ransom model. Now, DDoS attackers could force a healthcare organisation offline and only cease their attack if a specified ransom is paid.

6. What are the current cybersecurity challenges in the healthcare sector?

The healthcare and social care sectors are easy prey for cybercriminals, due to the relative weakness of their IT infrastructure. Hospitals, in particular, are a prime target, as they store large quantities of sensitive data and need constant access to a digital system that operates around the clock.

But it is also a veritable cash cow: medical data is highly lucrative and its value has been rising steadily for several years.

Another aggravating factor is that hospital IT systems are quite difficult to protect against cyberattacks. This is due to:

- The presence of poorly secured connections between hospitals' IT systems and those of their service providers;
- The proliferation of software and applications;
- The development of connected medical devices;
- The installation of software not approved by the IT department;
- Low levels of IT security awareness amongst staff.

7. The consequences of cyberattacks in the healthcare sector

Cyberattacks can have serious consequences for the healthcare sector:

7.1. Risks to patient confidentiality

These attacks can jeopardise patient confidentiality by compromising their personal data, such as their name, address, National Insurance number or medical history. Cybercriminals can then use this information to commit fraud or identity theft.

7.2. Risks to the quality of care

Cyberattacks can also affect the quality of care provided to patients. If the IT systems of hospitals or doctors' surgeries are compromised, this can lead to a disruption in healthcare services, preventing healthcare professionals from accessing medical records or prescribing treatments. **This can have serious consequences for patients' health, particularly in an emergency.**

7.3. Financial risks

They can also have significant financial consequences for healthcare organisations. The costs of recovering and replacing IT systems can be very high, and revenue losses can be substantial if healthcare services are disrupted for an extended period.

8. Measures to prevent and protect against cyberattacks in the healthcare sector

Staff must be trained in the correct use of technology, including security policies and best practices. They must also understand the potential risks associated with cyberattacks and know how to identify suspicious activity. Furthermore, they should be encouraged to report any incidents to management as soon as possible so that appropriate action can be taken.

8.1. Securing IT systems

IT systems must be regularly updated with the latest security patches and antivirus software to prevent cyberattacks. Organisations should also implement firewalls, encryption technologies and other security measures to protect their networks against malicious activity.

8.2. Back-up systems

Healthcare organisations should put a plan in place to ensure that their data is backed up regularly, so that in the event of a cyberattack, they can restore their systems quickly and minimise any disruption to their operations.

8.3. Risk management strategies

Organisations must put in place a risk management strategy to identify potential threats and vulnerabilities in their IT infrastructure and to develop procedures for responding quickly and effectively in the event of an incident.

9. Countermeasures against cyberattacks in the healthcare sector?

There are therefore two possible types of response: one relating to the configuration of security mechanisms, and the other to policy and these same configurations.

We propose a number of countermeasures:

9.1. First countermeasure

Prioritise the configuration of security mechanisms:

Protection systems must react automatically or at least reconfigure themselves to prevent attacks from spreading. Mechanisms currently in place allow, for example, the automatic closure of a port on a firewall (to block a source of attack) or the termination of a system process (again, to halt an attack in progress via that process).

9.2. Second countermeasure

Implement a configuration policy:

If an attack has succeeded, it is because the configuration of the preventive tools was incorrect, in which case this configuration must be reviewed. Typically, the security policy itself was incorrect or incomplete, in which case this policy must be amended and new configurations of the preventive security mechanisms deployed. There are therefore two possible types of response: one relating to the configuration of security mechanisms, the other to the policy and those same configurations.

To strengthen the cybersecurity of healthcare organisations and prevent the risk of cyber-attacks, there are various technological solutions that can be implemented on a day-to-day basis, including:

- The installation of a robust security system, including a firewall, antivirus software and a VPN;
- Using a remote monitoring service;
- Securing passwords;
- Carrying out regular backups;
- Securing Wi-Fi access;
- Setting up automatic logout to protect access to workstations;

- Using a secure healthcare email service.

Furthermore, it is essential to disseminate best security practices to all healthcare professionals. This involves three types of measures:

Awareness campaigns, urging all users of the IT system to be vigilant and reminding them of the main risks to which they are exposed.

Training initiatives, to teach staff how to use IT tools more effectively and to impart best practice.

Mandatory measures: these include, for example, requiring the use of secure messaging, regular password changes or banning the use of USB sticks.

Conclusion

In this article, we have seen just how critical data protection is within the healthcare system. Unfortunately, we have also seen the interest that hackers take in healthcare organisations.

It is therefore essential to take measures to secure IT systems, raise staff awareness of cybersecurity risks, back up data regularly and develop a risk management plan to minimise the risk of cyberattacks.

The Democratic Republic of the Congo, with its socio-economic challenges and fragile healthcare system, faces a growing threat from cyberattacks, particularly within the healthcare sector. These attacks can have serious consequences, not only for the confidentiality and security of patient data, but also for the continuity of care and medical research.

To address this reality, it is imperative that the Congolese authorities, in collaboration with healthcare stakeholders and international partners, implement robust cybersecurity strategies. This includes drawing up clear regulations, investing in secure infrastructure, and providing ongoing training for healthcare staff to strengthen their resilience in the face of these threats.

Raising awareness of the challenges posed by cyberattacks in the healthcare sector in the Democratic Republic of the Congo is essential to protect critical infrastructure and ensure patient safety. The development of tailored cybersecurity solutions, combined with staff training and appropriate government support, is vital to mitigate the risks associated with these threats.

References

1. <https://theses.hal.science/tel-00012162>
2. <https://www.ipac-traductions.com/blog/la-cybersecurite-dans-le-secteur-de-la-sante-quels-sont-les-enjeux>
3. <https://fr.quora.com/Quelle-est-la-diff%C3%A9rence-entre-un-syst%C3%A8me-informatique-et-un-syst%C3%A8me-dinformation>
4. <https://www.nameshield.com/ressources/lexique/cyberattaque/>
5. <https://pressbooks.pub/methodes/chapter/surete-de-fonctionnement/>
6. http://strategique.free.fr/archives/textes/hacking/archives_hacking_05.htm
7. https://www.memoireonline.com/04/12/5679/m_Mise-en-place-dun-systeme-de-securite-base-sur-lauthentification-dans-un-reseau-IP-Cas-d9.html
8. <https://www.iro.umontreal.ca/~salvail/securite/notes/2014/securite10-2014long.pdf>
9. <https://www.cnil.fr/fr/securite-chiffre-garantir-lintegrite-ou-signer>
10. <https://webhost.laas.fr/TSF/deswarte/Publications/02447.pdf>
11. <https://lipn.univ-paris13.fr/~poinot/save/INFO%203/Cours/Cours%202.pdf>
12. <https://www.ifri.org/sites/default/files/atoms/files/ticetsystemesdesanteenafrique.pdf>
13. <https://archipel.uqam.ca/3373/1/M9724.pdf>
14. <https://iotindustriel.com/cybersecurite/cyberattaques-dans-le-secteur-de-la-sante/>
15. National_Digital_Plan_HORIZON_2025 DRC
16. National Cybersecurity Strategy DRC
17. System security mechanisms

18. Kianpour, M., Kowalski, S., & Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey
19. Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice (2nd ed.). Syngress
20. Sharma, D. P., Lashkari, A. H., & Parizadeh, M. (2024). Understanding Cybersecurity Management in Healthcare: Challenges, Strategies and Trends. Springer.