doi: http://dx.doi.org/10.11606/issn.1679-9836.v104i6e-236087 Rev Med (São Paulo). 2025 Nov-Dec;104(6):e-236087.

Review Article

Cyberbiosecurity in medicine: protecting data and patients in the digital age

Ciberbiossegurança na medicina: protegendo dados e pacientes na era digital

Enrico Jardim Clemente Santos[1], Angela Mazzeo[2]

Santos EJC, Mazzeo A. Cyberbiosecurity in medicine: protecting data and patients in the digital age */ Ciberbiossegurança na medicina: protegendo dados e pacientes na era digital* / Rev Med (São Paulo). 2025 Nov-Dec;104(6):e-236087.

ABSTRACT: Technological innovation has become an inherent aspect of our society's existence, since practically every item relevant to our daily lives has at least one cyber component associated with it. These include personal computers, computer networks, information technology and virtual reality. Now the life sciences are establishing an interface with information technology and cybersecurity, giving rise to a discipline whose scope is biosecurity, cyber-physical security and cybersecurity, which has been called cyberbiosecurity. This involves the understanding, protection, mitigation, investigation, surveillance, intrusions and malicious and harmful activities that can occur within or at the interfaces of the medical sciences and can affect the competitiveness and resilience of institutions. This paper will address issues related to cybersecurity in medical institutions such as clinics, hospitals and laboratories.

KEYWORDS: Cyberbiosecurity; Medicine; Health system; Cyber attack; Social engineering.

RESUMO: A inovação tecnológica tornou-se um aspecto inerente à existência de nossa sociedade, uma vez que praticamente todos os itens relevantes para nossa vida diária possuem pelo menos um componente cibernético associado a ela. Dentre estes, podemos ressaltar os computadores pessoais, as redes de computadores, a tecnologia da informação e a realidade virtual. Agora, as ciências da vida vêm estabelecendo uma interface com a tecnologia da informação e a segurança cibernética, dando origem a uma disciplina que tem por escopo a biossegurança, segurança ciberfísica e cibersegurança, a qual foi denominada de ciberbiossegurança. Esta envolve a compreensão, proteção, mitigação, investigação, vigilância, intrusões e atividades maliciosas e prejudiciais que podem ocorrer dentro ou nas interfaces das ciências médicas, podendo afetar a competitividade e a resiliência das instituições. Neste trabalho abordaremos questões relacionadas à ciberbiossegurança nas instituições médicas, como clínicas, hospitais e laboratórios.

PALAVRAS CHAVE: Ciberbiossegurança; Medicina; Sistema de saúde; Ataque cibernético; Engenharia social.

[1.] Instituto de Pesquisas Energéticas e Nucleares, São Paulo, SP. Brasil. ORCID: https://orcid.org/0000-0003-0869-3342 E-mail: enrico.j@ipen.br
[2.] Universidade de São Paulo, São Paulo, SP. Brasil. ORCID: https://orcid.org/0000-0001-8483-5002 E-mail: amazzeo@usp.br
Correspondence: Enrico Jardim Clemente Santos, Rua José Piragibe, 228/11a, Vila Indiana, São Paulo. Brasil. CEP: 05585-040, enrico@celltrotec.com.br

INTRODUCTION

Cyber vulnerabilities are a reality today, posing significant risks to individuals, organizations, governments, and economies. However, the challenges associated with cybersecurity vulnerabilities are not insurmountable, as they require careful consideration by equipment designers, software and control system developers, and end users.

Risks related to the biological sciences have been managed through the implementation of standard biosafety practices (protection of valuable biological material from misuse or damage) and cybersecurity (protection of computer systems from theft and damage to their hardware, software, or information, as well as from interruption or misdirection of the services they provide). This association has been called cyberbiosecurity, an effort to safeguard the bioeconomy, the result of a revolution of innovations based on the biological sciences, culminating in the development of more sustainable products, processes, and services[1].

Cyberbiosecurity is an emerging and innovative field that addresses vulnerabilities and threats arising from the intersection of cyberspace and biotechnology, based on the intersection of three sectors: cybersecurity, biosecurity, and cyberphysical security. Cybersecurity aims to protect computer systems against breaches, loss, and damage to their hardware, software, information, and data, as well as the interruption of applications and other related services. Biosecurity aims to reduce risks related to the misuse of tools, data, and/or knowledge related to biological material. Cybersecurity addresses risks related to the security of technologies such as industrial control and operation systems, as well as Internet of Things and Internet of Bodies sensors, which interact with and affect the physical world and human life in real time[2].

Although cybersecurity encompasses the protection of any electronic data, systems, networks, etc., cyberbiosecurity is one of its most important applications. It is especially focused on implementing corrective measures, preventing illegal intrusions, and protecting data, information, processes, valuable materials, and other online resources belonging to the medical sciences[3].

Currently, threats of malicious destruction, misuse, or exploitation of valuable process information and materials at the interface between life sciences and the digital world tend to be identified and mitigated through training and the implementation of security processes, which are being periodically improved. These include the implementation of a data backup system on a separate server that is not connected to the internet; a robust and reliable security firewall; cybersecurity protocols implemented in the event of a data breach; and regular audits and anti-malware checks.

Healthcare institutions, such as clinics, hospitals, and laboratories, have been targeted by biohackers (hackers who specifically target the healthcare sector) who have obtained thousands of dollars in ransoms due to the critical nature of the information (ransomware)[4]. In particular, the challenges to be considered are the privacy and integrity of databases of physicians, patients, and healthcare institutions, defense against cyberattacks, and laboratory and hospital automation. The integrity of public bioinformatics databases, such as those maintained by the NCBI (The National Center for Biotechnology Information), and the protection of intellectual property are of fundamental importance[5].

This study aims to analyze the importance of cybersecurity in the context of medical institutions, such as clinics, hospitals, and laboratories, with regard to medical equipment and data belonging to patients and healthcare professionals.

METHODOLOGY

This study was based on exploratory and descriptive bibliographic research using scientific databases indexed in Google Scholar, Scientific Electronic Library Online (Scielo), Latin American and Caribbean Health Sciences Literature (LILACS), Researchgate, and Medical Literature Analysis and Retrieval System Online (MEDLINE). For the search, publications from 2006 to 2025 were selected using the following keywords: cybersecurity; cyberbiosecurity; biosecurity; cyberattack; medicine; cybersecurity.

RESULTS AND DISCUSSION

The first article related to cyberbiosecurity was published by Peccoud et al. in 2018. The article focused mainly on issues related to the security of the biotechnological interface with cyberspace and the need to make users aware of the risks involved. The article contributed significantly to the future scope of cyberbiosecurity[6]. The term cyberbiosecurity was established by Murch et al., who described the vulnerabilities that exist between cybersecurity, cyberphysical security, and biosecurity (Figure 1)[1]. According to Murch, cyberbiosecurity can be defined as "the development of an understanding of vulnerabilities to unwanted surveillance, intrusions, malicious and harmful activities that may occur within or at the interfaces of upcoming life sciences, cyber, cyber-physical, supply chain, and infrastructure systems, and developing and instituting measures to prevent, protect, mitigate, investigate, and attribute such threats with regard to security, competitiveness, and resilience"[1].

Cybersecurity is a discipline that has a significant impact on digital operations carried out in clinics, hospitals, and laboratories. Data obtained through a bibliographic survey conducted in the Medical Literature Analysis and Retrieval System Online (MEDLINE), based on the period between January 2017 and August 2025, and using the term cyberbiosecurity, resulted in 33 scientific publications (Graph 1). During this period, the year 2019 had the highest number of publications (15 in total), while in 2022 no publications were identified, as was the case from January to August 2025. These data prove that cybersecurity is an extremely new field.

Scientific, mathematical, computational, and engineering advances integrated with regenerative biology, genetics, reproductive technologies, plant-derived vaccines, animal therapies, biological design, and test automation and other activities are resulting in the rapid development of relevant biotechnological applications[7].

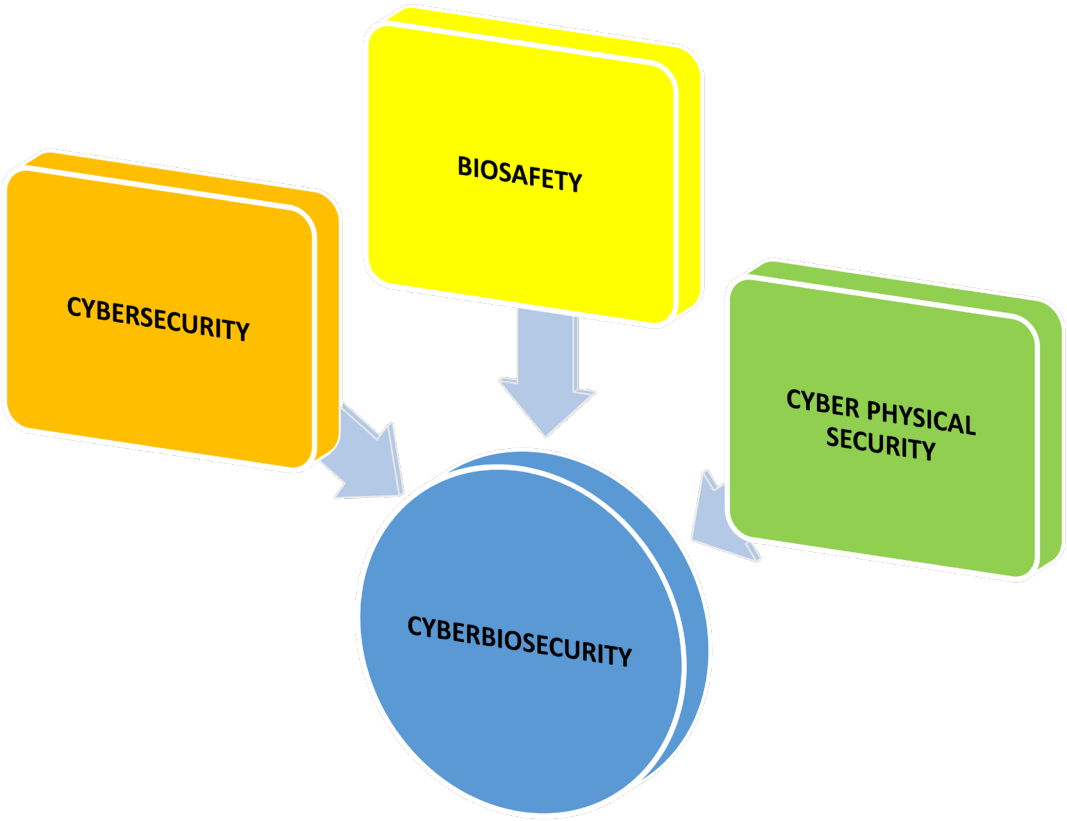
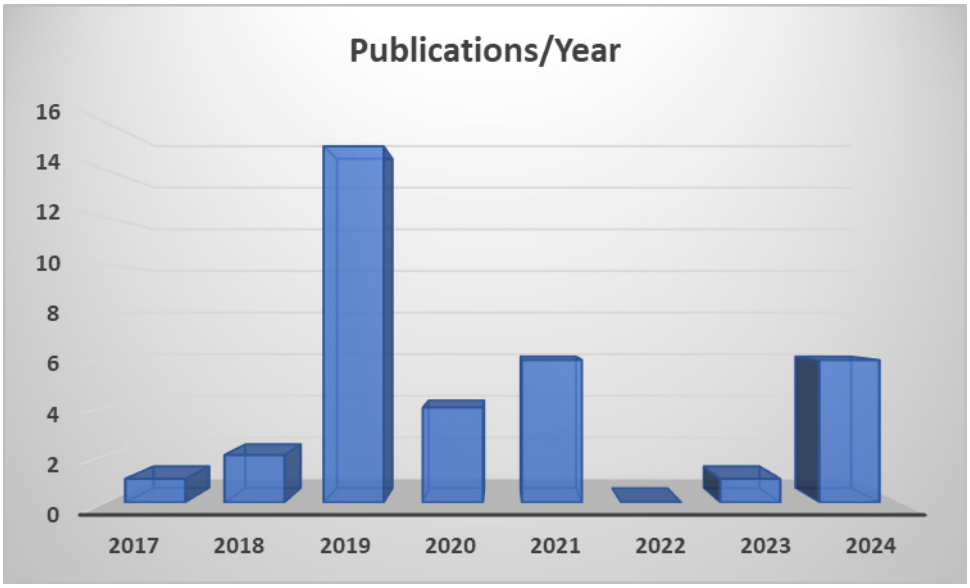


FIGURE 1 – Areas that comprise the term cyberbiosecurity

GRAPHIC 1 – Number of publications in the Medical Literature Analysis and Retrieval System Online using the term cyberbiosecurity



As the world becomes increasingly dependent on computer interconnectivity, whether professionally or socially, there has been a growing development of malware, malicious software intentionally designed to cause damage to computers or networks. Due to the vulnerability of the cybersecurity sector, the healthcare industry is facing significant challenges, as it has been the target of various types of cyberattacks, such as those carried out through online applications and platforms.

With the onset of the COVID-19 pandemic in early 2020, millions of people began working from home, making

videoconferencing a reality. In the medical field, online consultations, computer-assisted rehabilitation, and remote monitoring emerged as extremely interesting resources for the healthcare system[8]. This was mainly due to the inaccessibility of traditional healthcare services, given the high risks of exposure during in-person consultations[9]. However, barriers such as trained personnel, high costs, broadband access, and digital literacy among patients proved to be a reality in the daily lives of the global population.

This was mainly due to the inaccessibility of traditional healthcare services, given the high risks of exposure during in-person consultations[7]. However, barriers such as trained personnel, high costs, broadband access, and digital literacy among patients proved to be a reality in the daily lives of the global population.

The growing use of medical devices connected via the Internet, such as ventilators, infusion pumps, radiological imaging equipment, surgical tables, anesthetic devices, stimulation devices, pacemakers, surgical robots, monitoring equipment, implantable devices, and organ support, is already a reality. These interconnections bring with them great benefits, such as rapid data collection and transmission, which assist the medical team in decision-making[10]. In addition, they enable early intervention due to the possibility of predicting potential clinical complications, improving patient engagement, real-time monitoring leading to better patient care, greater therapeutic options, monitoring patient compliance with the treatment plan, remote monitoring, and alerting to unsafe situations, thereby speeding up patient care by the medical team[10]. The interruption or invasion of any of these devices can delay or alter the care protocol, causing irreparable damage to a patient, as well as tarnishing the institution's reputation, inflicting significant moral and financial losses[11].

Cyberattacks can have significant consequences for the healthcare system, as valuable and confidential data used, for example, to create medicines and carry out treatments can be easily accessed by malicious agents if stored on an unsecure operating system (system vulnerabilities). A good example is implantable medical devices that enable wireless connections to update, collect data, and report information to the provider in order to monitor the patient's health and progress. However, there are enormous risks regarding the security of these devices if they are not protected, since cyberattacks have the potential to sabotage the devices, causing damage or erroneous treatment, or even data theft for potential illegal activity[4].

The main reason why medical institutions are such a target is because they have a wealth of patient data at their disposal. Cyberattacks allow hackers to access information, steal it, and then sell it on the black market for considerable sums of money. A medical record contains a variety of information, such as identification and contact documents, demographic and financial information, as well as confidential medical data and prescription requests for the patient[4]. Medical records are part of a person's identity and are therefore extremely difficult to alter. The details contained in medical records can be used to create fraudulent documents for illicit financial gain, obtain controlled medications, and even for bribery or coercion, especially in the case of high-profile individuals[12]. It is now known that medical information can be worth ten times more than credit card numbers on the deep web[13]. Credit card data thefts can be quickly reported to banks, which can take immediate action, while patients tend to discover that their credentials have been stolen long after fraudsters have used them to impersonate them.

One of the main problems faced is ransomware attacks, i.e., malicious software used for extortion through the hijacking of digital data using encryption. Ransomware is a cybercrime in which hackers hold the victim's personal files hostage, demanding a ransom to restore access to these files. Although ransomware has only recently been recognized as a cybersecurity risk in healthcare, these attacks are seen as challenges for information security teams working in the healthcare system. These teams, in turn, must manage the availability, integrity, confidentiality, and authenticity of information, as well as protect healthcare technology systems[14].

Inevitably, cyberattacks result in a return to the use of analog telephones, fax machines, local printing, and handwritten notes, which can cause several problems due to the fact that younger doctors, nurses, and healthcare professionals have no experience practicing medicine without the use of electronic health records[15]. Thus, we can see that the healthcare system has a deficient infrastructure in terms of adopting effective guidelines against cyber attacks, surviving long periods of downtime, and implementing a plan for recovery and return to normal operations.

In addition to the financial cost, there is a direct and indirect impact on the health of the population served by the healthcare system compromised by a ransomware attack. The direct impact includes reduced access to healthcare, cancellation of medical appointments, cancellation of surgeries, and even the closure of emergency rooms. Indirect impacts include worsening patient health due to delayed treatments and missed diagnoses, as well as canceled appointments and procedures[16]. From the network's point of view, the greatest risk is data loss if the ransom is not paid, i.e., the process requires little effort on the part of the hacker with high potential for gain. Attacks on medical equipment, although less common, aim to challenge or cause disruption or deliberate damage, without necessarily presenting any financial gain. These attacks aim to cause erroneous monitoring due to changes in device settings. It has been proven that anesthesia machines and infusion pumps can be hacked and their settings changed without the doctor's knowledge[12].

One of the major problems with security systems is the public networks that can be found in various establishments. These are, in most cases, extremely vulnerable, since hackers can access an unencrypted device without any type of verification[17]. Although passwords are required in many establishments, they can be requested, which renders them useless. One security option when using this type of system is to establish a Virtual Private Network (VPN) connection. When accessing these networks, the VPN provides end-to-end encrypted wireless and wired connections, making it extremely challenging and time-consuming to obtain the data[18].

With the implementation of a universal paperless information system, healthcare data is being shared between hospitals around the world to provide adequate patient care. This makes the use of an encrypted system vitally important. Because servers are constantly online and therefore exposed to cyberattacks from hackers or ransomware, it is essential to back up all data frequently, securely, and regularly. These backups should be stored on a separate server that is not connected to the internet, so that the system can be restored safely and effectively if necessary. This system, also known as air-gapped, can be considered perfectly secure since it is isolated from the network, with no remote access to the system. In addition, issues related to the privacy of patients' clinical and financial data, the integrity of diagnostic test data, the integrity of biological databases, as well as the security of information that may give rise to patents, are extremely relevant issues.

In recent decades, social engineering, a manipulation technique that exploits human errors to gain access to private and valuable information, has become an extremely relevant factor in the daily lives of the world's population. In this context, the increase in cyberattacks reflects the use of social engineering by hackers who, through psychological manipulation, lead an unsuspecting recipient to perform an action to expose data, disclose confidential information, spread malware infections, or give access to restricted systems. This approach often takes the form of an email or some other form of communication with malicious links or attached malware that exploits the individual's weaknesses, causing the recipient to click on the link or attachment. In a phishing attack, the hacker produces fraudulent communications that can be interpreted as legitimate by the victim because they claim to come from trusted sources[19].

Certain guidelines should be adopted to prevent potential cyber attacks based on social engineering. These include not responding to or clicking on links sent by email that ask for personal or financial information; never disclosing confidential or even seemingly non-confidential information about yourself or your institution, either by phone or online, unless you can first verify the identity of the person requesting it and their need for that information, since attacks using deepfake, an artificial intelligence resource used to simulate people's voices, have become increasingly common; keeping your computer's security devices, such as antivirus, spyware, and browsers, up to date by running regular system checks and using browsers that have phishing filters[19].

Nowadays, it is essential that the workforce operating in the healthcare system undergoes a change in mindset to become cyber-aware, understanding that even with the best cybersecurity systems in place, they can still be targets of attacks through phishing, for example, which can compromise all connected devices, both inside and outside hospital environments. Therefore, the implementation of a "zero trust" culture is of fundamental importance for the healthcare system. Through this, professionals begin to view emails or web calls with zero trust, instead of the implicit trust that is often assumed today. Therefore, it is of fundamental importance to spare no effort to ensure that the "zero trust" culture is implemented throughout the healthcare system[20].

Although clinics, hospitals, and laboratories are investing significant amounts in implementing security measures, implementation has proven to be flawed, as modern cybersecurity providers lack experience with software used in healthcare. This is especially true with software used in laboratories, clinics, and hospitals, which ranges from highly standardized to customized for each patient. The implementation of a preventive security system is extremely important for healthcare institutions[21].

The healthcare sector has been the target of increasingly frequent and global cyber threats such as Cross-Site Scripting, Distributed Denial of Service (DDoS), Eavesdropping Attacks, Insider Threats, Internet Protocol (IP) Spoofing, IoT Attacks, Malware, Man in the Middle (MitM), Phishing, Ransomware, Session Hijacking, Smishing, Spear phishing, Spyware, Trojan (Trojan Horse), Virus, Vishing, Whaling, Worm, and Zero-Day Exploit (Table 1)[11]. Although a breach of the security system has the potential to paralyze an entire healthcare system in minutes, the effects can linger for years, as reputation recovery and legal proceedings tend to be inevitable.

Companies such as Neuralink have been developing devices designed to interact with various regions of the brain, aiming to create a new therapeutic approach for debilitating diseases that affect the brain and central nervous system. This technology, called Brain-Machine Interface (BMI), aims to bring numerous benefits to the world population through the implantation of a chip in brain tissue, including enabling an active brain to perform functions while ignoring a sick body or treating cases of certain brain diseases, such as motor neuron disease, epilepsy, sclerosis, Parkinson's disease, amyotrophic lateral sclerosis, spinal cord injuries, depression, blindness, deafness, and chronic pain. In addition, this neural interface opens up the possibility of amplifying inherent human abilities, such as concentration and memory[22]. A good example of this was the experiments carried out on pigs, which, after receiving instructions, were able to control their legs to perform movements instructed by a computer to the chip implanted in the animals' spinal cord[21]. Another very interesting experiment was conducted on a monkey that had a chip implanted in its brain, so that, through instructions issued by the computer, the animal began to play video games[23,24].

Although this approach may bring hope for a cure for ailments that medicine has so far been unable to reverse, some relevant questions arise. Among these is what will happen if a hacker accesses the computer and begins to give orders to control your thoughts by implementing new values and ideals, totally compromising people's actions, such as instructing a specific person to transfer significant amounts of money to a secret account in Switzerland or altering the settings of the surgical robots used in the process of implanting the chips in the cortex safely and effectively near the neurons of interest, since they are thin and flexible in nature, which makes their manipulation impractical.

TABLE 1 – Types of cyber threats

AMEAÇAS	DEFINIÇÃO
CROSS-SITE SCRIPTING	These are malicious codes inserted into trusted web pages or applications.
DISTRIBUTED DENIAL OF SERVICE	Makes it difficult for users to access a target system or services, overloading the network with traffic
EAVESDROPPING ATTACKS	Executed by attackers using weak or insecure (unencrypted) network connections
INSIDER THREATS	Originating from within the targeted organization, intentionally or unintentionally, by those who have or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems.
INTERNET PROTOCOL SPOOFING	An attacker modifies the source IP address in order to disguise their identity so that they can impersonate a computer on a legitimate network, tricking the receiving system into thinking that the modified IP address is from a trusted source.
IOT ATTACKS	Vulnerabilities in network-connected medical devices that can be exploited to gain access to confidential data
MALWARE	Software intentionally designed to exploit network vulnerabilities through automated and unauthorized access, compromising user privacy and computer usability through data theft and/or data destruction.
MAN IN THE MIDDLE	Data interruption through third-party interception
PHISHING	A social engineering method used to deceive users into disclosing confidential information by transmitting legitimately disguised fraudulent communications.
RANSOMWARE	Denies access to the victim's data by locking or encrypting the target user's system with the aim of publishing or destroying data unless a ransom is paid, usually in the form of untraceable cryptocurrency.
SESSION HIJACKING	Acquisition of an internet session by stealing a valid session ID from a legitimate user, so that hackers can assume the user's identity to steal data and gain unauthorized access to the system.
SMISHING	Uses SMS text messages to reach victims (communication between patients and providers)
SPEAR PHISHING	Phishing attempts targeting specific individuals or groups within an organization.
SPYWARE	It spreads without the user's knowledge by recording and transmitting activities, data, and information to unauthorized third parties.
TROJAN	It mimics legitimate software by tricking the user into running a program that will cause damage; it does not spread automatically and remains within the infected host.
VIRUS	Malicious program or code designed to alter the way a computer works and developed to spread from one computer to another.
VISHING	Uses voice features, such as calls from supposed internet telephone services, to deceive victims and extract personal and confidential information, such as bank passwords, credit card details, and social security numbers.
WHALING	A method used by cybercriminals to disguise themselves as high-ranking members of an organization and directly target other important individuals, with the aim of stealing money and confidential information or gaining access to their computer systems for criminal purposes.
Worm	Self-replicating malware is a type of virus that enters networks by exploiting vulnerabilities, moving quickly from one computer to another.
Zero-Day Exploit	Method used by hackers to attack systems, programs, and networks with vulnerabilities that have not yet been identified and corrected by developers.

FINAL THOUGHTS

As biotechnology keeps evolving, putting a cyberbiosecurity system in place is super important. Being aware of and spotting weaknesses are key steps in developing and implementing security measures against possible cyberattacks. Professionals in this field will be responsible for developing governance guidelines and standards, which will require adherence to and compatibility with defensive strategies for the healthcare system.

CONTRIBUTION AUTHOR´S: Enrico Jardim Clemente Santos - Bibliographic content survey and article writing. Angela Mazzeo - Bibliographic content survey and article writing.

REFERENCES

1. Murch R, DiEuliis D. Editorial: Mapping the Cyberbiosecurity Enterprise. Front Bioeng biotechnol. 2019;7:235. Doi: https://doi.org/10.3389/fbioe.2019.00235
2. Mazzeo A, Santos EJC. Integration of biomedical devices and the internet of bodies revolution. Res Soc Develop. 2025;14(5):e11814548921. Doi: https://doi.org/10.33448/rsd-v14i5.48921
3. Osborne C. US Hospital Pays $55,000 to Biohackers After Ransomware Attack. ZDNet. https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/
4. Dameff C, Tully J, Chan TC, Castillo EM, Savage S, Maysent P, Hemmen TM, Clay BJ, Longhurst CA. Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. JAMA Netw Open. 2023;6(5):e2312270. Doi: https://doi.org/10.1001/jamanetworkopen.2023.12270
5. Peccoud J, Gallegos JE, Murch R, Buchholz WG, Raman S.

Cyberbiosecurity: From Naive Trust to Risk Awareness. Trends Biotechnol. 2018;36(1):4-7. Doi: https://doi.org/10.1016/j.tibtech.2017.10.012

6. Murch RS, So WK, Buchholz WG, Raman S, Peccoud, J. Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy. Front Bioeng Biotechnol. 2018;6:39. Doi: https://doi.org/10.3389/fbioe.2018.00039

7. Santos EJC, Mazzeo A. Cyberbiosecurity in biointelligent environments: Integrating artificial intelligence, synthetic biology and automation in vital sectors. Res Soc Develop. 2025;14(6):e5714648937. Doi: http://dx.doi.org/10.33448/rsd-v14i6.48937

8. Tukur M, Saad G, AlShagathrh FM, Househ M, Agus M. Telehealth interventions during COVID-19 pandemic: a scoping review of applications, challenges, privacy and security issues. BMJ Health Care Inform. 2023;30(1):e100676. Doi: https://doi.org/10.1136/bmjhci-2022-100676

9. Jalali MS, Landman A, Gordon WJ. Telemedicine, privacy, and information security in the age of COVID-19. Journal of the American Medical Informatics Association: JAMIA. 2021;28(3):671-2. Doi: https://doi.org/10.1093/jamia/ocaa310

10. DeFord D. Sustainable Digital Health Demands Cybersecurity Transformation. Front Health Serv Manag. 2022;38(3):31-8. Doi: https://doi.org/10.1097/HAP.0000000000000137

11. Mazzeo A, Santos EJC. Integrating Cybersecurity into Veterinary Medicine: Protecting Animal Health Data and Systems. Res Soc Develop. 2025;14(5):e7414547190. Doi: https://doi.org/10.33448/rsd-v14i5.47190

12. Sendelj R, Ognjanovic I. Cybersecurity Challenges in Healthcare. Studies Health Technol Inform. 2022;300:190-202. Doi: https://doi.org/10.3233/SHTI220951

13. Onyango S, Steenvoorden E, Scholten J, Jansen S. Assessing the Health of the Dark Web: An Analysis of Dark Web Open Source Software Projects. In; Gregory, P., Kruchten, P., Eds.; Lecture Notes in Business Information Processing; Springer International Publishing: Cham, 2021;426:125-34. Doi: https://doi.org/10.1007/978-3-030-88583-0_12

14. Kanter GP, Rekowski JR, Kannarkat JT. Lessons From the Change Healthcare Ransomware Attack. JAMA Health Fórum. 2024; 5(9):e242764. Doi: https://doi.org/10.1001/jamahealthforum.2024.2764

15. Patel AU, Williams CL, Hart SN, Garcia CA, Durant TJS, Cornish TC, McClintock DS. Cybersecurity and Information Assurance for the Clinical Laboratory. J Appl Labor Med. 2023;8(1):145-61. Doi: https://doi.org/10.1093/jalm/jfac119

16. Abbou B, Kessel B, Ben Natan M, Gabbay-Benziv R, Dahan Shriki D, Ophir A, Goldschmid N, Klein A, Roguin A, Dudkiewicz M. When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. Front Dig Health. 2024;6:1321485. Doi: https://doi.org/10.3389/fdgth.2024.1321485

17. Bheevgade P, Saha C, Nath R, Dabhade S, Barot H, Junare SO. The Rise of Public Wi-Fi and Threats. In: Patel, S.J., Chaudhary, N.K., Gohil, B.N., Iyengar, S.S. (eds) Information Security, Privacy and Digital Forensics. ICISPD. Lec Notes Elec Engin. 2024. Doi: https://doi.org/10.1007/978-981-99-5091-1_13

18. Kabachinski J. Virtual private networks can provide reliable IT connections. Biom Instrument Technol. 2006;40(1):51-4. Doi: https://doi.org/10.2345/0899-8205(2006)40[51:VPNCPR]2.0.CO;2

19. Breda F, Barbosa H, Morais T. Social engineering and cyber security. In IATED. 2017:4204-4211. Doi: https://doi.org/10.21125/inted.2017.1008

20. Wang Z, Yu X, Xue P, Qu Y, Ju L. Research on Medical Security System Based on Zero Trust. Sensors. 2023;23(7):3774. Doi: https://doi.org/10.3390/s23073774

21. Bhuyan SS, Kabir UY, Escareno JM, Ector K, Palakodeti S, Wyant D, Kumar S, Levy M, Kedia S, Dasgupta D, Dobalian A. Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. J Med Syst. 2020;44(5):98. Doi: https://doi.org/10.1007/s10916-019-1507-y

22. Parikh PM, Venniyoor A. Neuralink and Brain-Computer Interface-Exciting Times for Artificial Intelligence. South Asian J Câncer. 2024;13(1):63-5. Doi: https://doi.org/10.1055/s-0043-1774729

23. Singh A. Kumar V. Neuralink: Spearheading the Point of Interaction among Brain and Machine. Int J Sci Res. 2023;12(9):1263-6. Doi: https://doi.org/10.21275/SR23910185406

24. Sailaja M, Dharani NV. A Study of Neuralink: The Brain Machine Interface. Int J Adv Res Comp Commun Eng. 2021;10(7):128-31. Doi: https://doi.org/10.17148/IJARCCE.2021.10723

Received: 2025, Mayo 06
Accepted: 2025, October 02