Krepitev odpornosti laboratorijev proti kibernetskim napadom

Building laboratory resilience against cyberattacks

Giuseppe Lippi
Section of Clinical Biochemistry, University of Verona

Corresponding Author:
Prof. Giuseppe Lippi
University Hospital of Verona, Section of Clinical Biochemistry, Piazzale L.A. Scuro, 10, 37134 Verona, Italy
e-mail: giuseppe.lippi@univr.it

ABSTRACT

Cyberattacks targeting healthcare facilities, including medical laboratories, have surged in recent years, threatening patient safety, data integrity, and operational continuity. Laboratories are especially vulnerable due to their reliance on interconnected systems, rapid data exchange, and uninterrupted diagnostic workflows. This article describes the personal experience garnered during and after a cyberattack on a healthcare facility, which dramatically affected the operations of the local laboratory medicine services. Effective resilience requires both robust prevention measures and practical response strategies to sustain operations during and after an incident. Immediate actions include defining a recovery plan, reverting to paper-based ordering and reporting systems, manual sample labeling, and detailed logging of incoming specimens to enable continuity of diagnostic services while digital systems are being restored. Post-attack strategies for strengthening resilience encompass the recruitment of specialized cybersecurity expertise, staff training, operating system upgrades, enhanced authentication protocols, network segmentation through multiple firewalls and antivirus solutions, secure cloud migration, and implementation of automated anomaly detection systems. Secure device policies, strict access controls, and the elimination of insecure shared folders are also advisable. Although all these interventions improve security, they can also introduce challenges, including increased workload from frequent training and authentication, slower operations, downtime from connectivity issues, and delays in instrument programming, release of test results, and technical support. Building resilience in laboratories thus requires a balanced integration of technological fortification, staff preparedness, and adaptive workflow redesign. This ensures that cybersecurity measures uphold, rather than impede, the uninterrupted delivery of accurate and timely diagnostic results.

Keywords: laboratory medicine, cyberattacks, cybersecurity

INTRODUCTION

The healthcare sector continues to face an alarming surge in the frequency and severity of data breaches. According to the last statistics of the Health Insurance Portability and Accountability Act (1), 6,759 healthcare data breaches were recorded between 2009 and 2024. These breaches involved »

at least 500 files and exposed or impermissibly disclosed the personal health information of approximately 847 million individuals. The upward trend is evident: 57 million records were compromised in 2022, 168 million records in 2023, and 276.8 million records in 2024, averaging approximately 760,000 records breached per day. These statistics underscore the vast and growing vulnerability of healthcare data, highlighting an urgent need for bolstered cybersecurity defenses, stringent response protocols, and robust resilience strategies across the sector.

Medical laboratories are critically vulnerable to cyberattacks due to their interconnected nature and strong reliance on information systems. They integrate multiple and networked diagnostic instrumentations, endpoint devices, laboratory information systems, hospital information systems, and electronic health records to facilitate patient testing and reporting. Although this interconnected digital ecosystem increases efficiency, it also exposes these facilities to a vast array of cyber threats, such as ransomware, phishing, insider threats, and supply chain attacks (2). Recently, the European Federation of Clinical Chemistry and Laboratory Medicine promoted a survey that included a vast number of clinical laboratories across Europe. The results revealed that over 34% of respondents had already been victims of one or more cyberattacks at their institution, and 65% of respondents believed they were likely to be targeted by a cyberattack in the future (3).

A successful cyberattack on a laboratory can disrupt clinical workflows, delay critical diagnostics, and jeopardize patient safety. For example, ransomware attacks typically encrypt laboratory data, blocking access to test orders and results, whereas breaches in data confidentiality may expose personal health information, violating privacy regulations and eroding public trust (4, 5). Laboratory resilience against cyberattacks must encompass prevention, responses, and mechanisms to maintain critical operations during and after incidents. To this end, this article describes the personal experience garnered during and after a cyberattack that dramatically impacted local hospital and laboratory medicine operations.

CYBERATTACKS TARGETING MEDICAL LABORATORIES

A thorough understanding of the types of cyberattacks that laboratories may face is essential for designing and implementing effective, tailored defense strategies (Table 1) (6). A threat that often targets healthcare infrastructures is ransomware, a malicious software that encrypts critical data and demands payment for decryption keys. Phishing and social engineering attacks exploit human vulnerabilities through deceptive emails or messages that lure staff into revealing credentials or clicking malicious links. Distributed denial-of-service attacks overwhelm network resources, causing system outages and service disruption. Insider threats, involving malicious or negligent insiders with authorized access, cause intentional or accidental data breaches. Supply chain attacks compromise third-party software or hardware vendors, introducing vulnerabilities into laboratory systems. Addressing these multifaceted threats requires a comprehensive cybersecurity framework that integrates technology, processes, and human factors.

Table 1: Glossary of potential threats to healthcare facilities and medical laboratories.

Term	Definition
Adware	Unwanted software that displays ads and can track user behavior.
Spyware	Software that secretly monitors user activity and collects information.
Trojan Horse	Malware disguised as legitimate software to trick users into installing it.
Malware	Malicious software (e.g., viruses, worms, trojans) designed to damage or disrupt systems.
Ransomware	Malware that encrypts data and demands payment for its release.
Distributed denial of service	An attack that floods a server or network with traffic to make it unavailable.
Phishing	A method of tricking people into giving up sensitive information via fake emails or websites.

»

IMMEDIATE RESPONSE TO CYBERATTACKS

When a cyberattack is detected, immediate and coordinated response efforts are critical to mitigate operational disruptions and safeguard patient safety, as recently underscored by the European Federation of Clinical Chemistry and Laboratory Medicine Task Force Preparation of Labs for Emergencies (7). Proactive preparedness is paramount; laboratories must develop, document, and regularly update a comprehensive and practicable cyber incident response plan prior to any attack, ensuring rapid activation when necessary. This plan should dictate prompt notification of all pertinent stakeholders, including laboratory leadership, medical directors, information technology (IT) support teams, clinical personnel, and, when appropriate, institutional cybersecurity, compliance officers, police cybercrime units, and data protection authorities (Table 2).

Table 2: Immediate responses to cyberattacks.

Action	Description
Paper-based ordering	Use printed forms from intranet-connected printers for test requests.
Manual labeling	Label tubes manually with patient identifiers.
Sample recording	Log all incoming samples on paper or offline spreadsheets.
Result reporting	Use printed instrument sheets, Excel modules, or verbal communication to report results.
Fax transmission logging	Record all sent faxes with receipts stored securely.

Upon cyberattack onset, laboratories should immediately transition to validated, secure paper-based workflows to maintain continuity of critical operations. Test requisitions should be managed manually using preprinted forms distributed via intranet-connected printers (provided network access remains functional) or stored locally on dedicated computers at sample collection sites with cable-connected printers. Specimen labeling must include multiple patient identifiers (e.g., full name, date of birth, sex, and, where available, preprinted patient ID and patient medical number) to preserve specimen integrity and chain of custody in the absence of electronic barcode systems.

Comprehensive and accurate logging of all incoming specimens on paper logs or secure offline spreadsheets within the laboratory is essential to maintain traceability and compliance with regulatory standards. Test results should be communicated to clinics via printed instrument output or preferably by emergency digital reporting tools (e.g., protected Excel modules with specific queries enabling cross-referencing patient demographic data with their corresponding reference intervals), with verification to minimize transcription errors. Fax transmissions, used as a primary communication channel over telephone notification (which should be reserved exclusively for urgent or critical test result notifications), must be rigorously documented, and transmission receipts should be retained to ensure auditability and support forensic investigations.

It is also crucial to integrate periodic staff training and simulation exercises into preparedness protocols such as simulated phishing campaigns, ensuring personnel are proficient with manual fallback procedures and understand their roles during cyber emergencies. Despite the increased labor and resource demands of paper-based contingency workflows, these measures are indispensable for preserving laboratory operational resilience, ensuring regulatory compliance, and ultimately protecting patient care quality during cyber crises.

BUILDING LONG-TERM LABORATORY RESILIENCE

Laboratories should develop and maintain comprehensive cybersecurity frameworks that integrate organizational, technical, and behavioral dimensions to ensure sustained resilience against evolving cyber threats (Table 3). Establishing clear governance structures with designated cybersecurity consultants and dedicated leadership roles is essential to foster accountability, ensure strategic alignment with established healthcare cybersecurity frameworks (such as those promulgated by the National Institute of Standards and Technology) (8), and guide the formulation of laboratory-specific risk management policies. Such cybersecurity experts play a crucial role in conducting thorough risk assessments, facilitating compliance audits, and tailoring policies that address the unique operational and regulatory challenges of laboratory environments.

Table 3: Cybersecurity measures for building long-term laboratory resilience.

Category	Measure	Description and Purpose
Governance and organizational	Clear governance structures	Designated cybersecurity consultants and leadership ensure accountability and strategic alignment with frameworks (e.g., the National Institute of Standards and Technology), guiding lab-specific risk policies.
	Risk assessments and compliance audits	Regular evaluations to identify vulnerabilities, ensure regulatory compliance, and tailor security policies to lab-specific operations.
	External expert collaboration and information sharing	Engage cybersecurity experts and join threat intelligence networks to stay up to date on emerging threats and best practices.
Staff awareness and training	Mandatory, recurring cybersecurity training	Focus on phishing identification, secure password management, and incident reporting to build a strong human firewall and security-aware culture.
	Embedding security awareness	Promote proactive security behaviors, early threat detection, and immediate reporting among laboratory personnel.
Technical measures	System modernization and patch management	Upgrade legacy systems to the latest operating systems (e.g., Windows 11+) and apply timely patches to decrease exploitable vulnerabilities.
	Multi-factor authentication (MFA) and strong password policies	Enforce MFA and regular updates of complex, unique passwords to strengthen account security beyond passwords alone.
	Network segmentation and firewalls	Use dedicated firewalls and segment networks to isolate critical lab subsystems, limiting lateral threat movement in case of breach.
	Endpoint security and anti-malware	Deploy advanced antivirus and endpoint detection and response platforms to detect and mitigate sophisticated malware and zero-day exploits.
	Encryption at rest and in transit	Encrypt sensitive data stored locally or in the cloud and during transmission to protect confidentiality and integrity.
	Secure cloud usage	Use encrypted, access-controlled cloud environments for scalable and resilient data storage and processing.
	Access control policies and the principle of least privilege	Restrict user/device permissions strictly to necessary access levels to mitigate insider threats and external exploitation.
	Elimination of insecure shared resources	Remove or secure network shared folders to prevent unauthorized data access and propagation of malware.
	AI (artificial intelligence)-based automated threat detection	Implement AI and machine learning tools for real-time anomaly detection, enabling rapid incident identification and containment.

»

Category	Measure	Description and Purpose
Testing and plans	Regular penetration testing and vulnerability assessments	Conduct proactive testing to identify and fix security weaknesses before adversaries exploit them.
	Incident response and business continuity plans	Develop, update, and rehearse procedures for cyber incident management and fallback operations to ensure the continuity of critical lab functions.
	Backup and disaster recovery	Maintain frequent, encrypted backups stored offsite/in a cloud with tested recovery plans to restore data and operations after incidents.
Access controls and monitoring	Role-based access control and privilege management	Enforce access controls tailored by role to ensure only authorized personnel have access to sensitive data or systems.
	Continuous monitoring and audit trails	Log and audit all access events and system changes; use security information and event management to promptly alert to any anomalies.
	Device security protocols	Enforce rigorous device management standards, including endpoint protection, patching, and use controls.

Staff awareness and digital proficiency constitute critical pillars of cybersecurity resilience. Mandatory, recurrent training programs focusing on cybersecurity best practices, including phishing identification, secure password protocols, and timely incident reporting, significantly strengthen the human firewall. Embedding a pervasive culture of security awareness empowers personnel to adopt proactive behaviors, quickly identify threats, and promptly report suspicious activities, thus mitigating potential breaches at the earliest stage.

From a technical standpoint, laboratories must prioritize modernization efforts by upgrading legacy systems, such as migrating to the most recent operating systems (e.g., Windows 11 or later), which offer enhanced security features and improved compatibility with enterprise-grade cybersecurity solutions. The implementation of multi-factor authentication significantly decreases the risk of unauthorized access by requiring multiple independent forms of verification, thereby strengthening account security beyond reliance on passwords alone. Complementary policies that enforce regular password updates, promote the use of complex passwords, and mandate unique credentials across different platforms further enhance credential integrity and mitigate the risks associated with password reuse and compromise.

Robust network segmentation, which can be achieved using dedicated firewalls that isolate critical laboratory subsystems, limits lateral threat propagation and contains potential breaches within confined network zones. Employing multi-layered security solutions, including advanced antivirus software and endpoint detection and response platforms, provides dynamic defense against a vast array of malware and sophisticated zero-day exploits. Additionally, transitioning data storage and processing to secure cloud infrastructures with strong encryption standards and specific access management enhances data protection and improves system resilience and scalability.

The integration of automated threat detection systems based on artificial intelligence and machine learning algorithms enables real-time monitoring and identification of anomalous behaviors or unauthorized access patterns, facilitating rapid incident containment and minimizing operational impact. Eliminating insecure shared network folders, enforcing stringent access control policies based on the principle of least privilege, and maintaining rigorous device security protocols are imperative measures to mitigate risks posed by both insider threats and external adversaries. »

Laboratories should then incorporate regular penetration testing and vulnerability assessments into their cybersecurity programs to identify and remediate emerging weaknesses proactively. Developing and routinely updating incident responses and business continuity plans, including well-rehearsed procedures for fallback operations during cyber events, ensures that laboratories can maintain critical functions and comply with regulatory requirements under adverse conditions. Collaboration with external cybersecurity experts and participation in information-sharing networks further strengthen laboratory defenses by providing timely threat intelligence and best practice guidance.

POTENTIAL CHALLENGES AND ADVERSE CONSEQUENCES OF CYBERSECURITY MEASURES

Although the benefits of the abovementioned cybersecurity measures are well-established, their implementation can present significant operational challenges within laboratory settings (Figure 1). Staff may encounter increased workload and cognitive fatigue resulting from frequent training sessions and the repetitive use of multi-factor authentication protocols. This cumulative burden can contribute to security fatigue, potentially prompting employees to engage in unsafe workarounds that inadvertently undermine cybersecurity defenses.

Stringent system restrictions and multi-layered security checks, although essential for protecting sensitive data, can introduce latency in routine laboratory workflows, thereby decreasing overall operational efficiency. Temporary system downtimes can result from factors such as virtual private network failures, network segmentation configurations, firewall rules, and antivirus software interference. These issues can disrupt critical workflows, including instrument programming, data transfer to laboratory information systems, validation of test results, and remote vendor technical support, thereby impacting instrument uptime and the reliability of laboratory results.

Financial constraints further complicate cybersecurity efforts. The financial investments required for hiring specialized cybersecurity personnel, acquiring software licenses, and upgrading IT infrastructure are often limited by laboratory budgets, potentially diverting resources away from core diagnostic functions and innovation initiatives. Additionally, rigorous access control policies, although indispensable for securing data, may inadvertently hinder timely collaboration and communication with external partners, vendors, and clinical teams, thereby impacting integrated care pathways and supply chain management.

To this end, achieving an optimal balance between robust cybersecurity and operational feasibility necessitates continuous monitoring and iterative refinement of policies. Incorporating structured feedback mechanisms from laboratory staff enables the identification of workflow bottlenecks and user experience challenges. Adaptive policy adjustments that align security protocols with real-world laboratory practices are critical to sustaining both resilience against cyber threats and uninterrupted delivery of high-quality patient care.

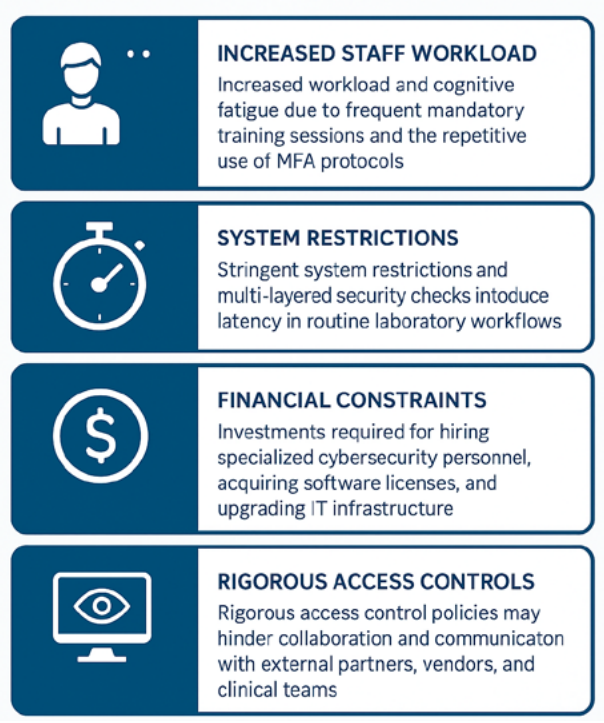

Figure 1: Potential challenges and adverse consequences of cybersecurity measures.

BROADER IMPLICATIONS AND FUTURE DIRECTIONS

With the accelerating digitalization of laboratory operations, the sector faces increasingly sophisticated, targeted, and persistent cyber threats. As diagnostic workflows, patient data management, and inter-laboratory communication become more interconnected, vulnerabilities in digital infrastructure can directly compromise clinical service delivery and patient safety. Emerging technologies, including artificial intelligence for anomaly detection, blockchain for secure and immutable data exchange, and zero-trust architectures for access control, offer substantial potential to strengthen the resilience of cybersecurity and accuracy of threat detection.

Nevertheless, technology alone is insufficient. Effective cyber defense requires sustained collaboration among laboratory leadership, IT security teams, technology vendors, and regulatory authorities to establish harmonized security standards, validated protocols, and real-time threat intelligence sharing. Integrating cyber resilience into broader disaster recovery and business continuity strategies is essential, given the critical role of laboratories within wider healthcare ecosystems. The adoption of emerging cyber insurance models specifically tailored to medical laboratory operations can also help offset the financial impact of cyber incidents, incentivize compliance with best practices, and facilitate rapid recovery. Finally, cybersecurity in laboratory medicine must be treated as a core component of quality management and patient safety, with continuous investment in workforce training, risk assessment, and system upgrades to anticipate and neutralize evolving digital threats.

CONCLUSIONS

Strengthening healthcare and laboratory resilience against cyberattacks is a complex yet essential component of healthcare quality and patient safety (8-12). This imperative is emphasized by the World Health Organization in its "Global Strategy on Digital Health 2020–2025", which underscores that digital health must be ethical, reliable, equitable, sustainable and, most importantly, safe and secure (12). Modern laboratories must adopt an integrated cybersecurity framework that combines proactive prevention, rapid and effective incident responses, and continuous risk governance (13). Preventive measures should include regular system upgrades, network segmentation to contain breaches, and comprehensive workforce training to address human-factor vulnerabilities. Incident response strategies must incorporate well-rehearsed fallback procedures, including manual operations, to ensure diagnostic continuity during digital disruptions. Continuous monitoring, supported by advanced analytics and centralized governance, is critical for early threat detection and a robust security posture.

Although implementing such measures may impose operational and financial burdens, the risks associated with cybersecurity breaches, ranging from patient harm and diagnostic delays to data loss, regulatory sanctions, and reputational damage, far outweigh these costs (14). Effective defense depends on sustained leadership commitment, interdisciplinary collaboration (between laboratory, IT, and clinical teams), and the cultivation of a pervasive security-aware culture. Cybersecurity must be recognized not as a peripheral technical function but as an integral component of quality management in laboratory medicine. Overall, cybersecurity is essential to safeguarding the uninterrupted delivery of accurate, timely, and reliable diagnostic information for supporting patient care, which remains the core mission of medical laboratories.

REFERENCES

1. Health Insurance Portability and Accountability Act. Healthcare Data Breach Statistics [Internet]. [accessed on 9. 8. 2025]. Available from: https://www.hipaajournal.com/healthcare-data-breach-statistics/.
2. Patel AU, Williams CL, Hart SN, Garcia CA, Durant TJS, Cornish TC, McClintock DS. Cybersecurity and Information Assurance for the Clinical Laboratory. J Appl Lab Med 2023;8:145-61.
3. Lippi G, Cadamuro J, Danese E, Favaloro EJ, Favresse J, Henry BM, et al. EFLM Task Force Preparation of Labs for Emergencies (TF-PLE) survey on cybersecurity. Clin Chem Lab Med 2024;63(1):e1-2.
4. Lippi G, Ferrari A. Lessons learnt in medical laboratories during a disruptive cyber-attack. J Lab Precis Med 2024;9:1.
5. Al Haddad C, Boutros T, Finianos P, Germanos M. When code crashes the lab: Operational resilience in clinical laboratories amid a cyberattack - A case study from a university hospital. Ann Biol Clin (Paris) 2025;83(4):414-24.
6. Niki O, Saira G, Arvind S, Mike D. Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. Digit Health 2022;8:20552076221104665.

7. Lippi G, Akhvlediani S, Cadamuro J, Danese E, García de Guadiana Romualdo L, Delacour H, et al. EFLM Task Force Preparation of Labs for Emergencies (TF-PLE) recommendations for reinforcing cyber-security and managing cyber-attacks in medical laboratories. Clin Chem Lab Med 2024;63:27-34.
8. National Institute of Standards and Technology (NIST). Cybersecurity Framework [Internet]. [accessed on 9. 8. 2025]. Available from: https://www.nist.gov/cyberframework.
9. Sendelj R, Ognjanovic I. Cybersecurity Challenges in Healthcare. Stud Health Technol Inform 2022;300:190-202.
10. Aldosari B. Cybersecurity in Healthcare: New Threat to Patient Safety. Cureus 2025;17:e83614.
11. Freyer O, Jahed F, Ostermann M, Rosenzweig C, Werner P, Gilbert S. Consideration of Cybersecurity Risks in the Benefit-Risk Analysis of Medical Devices: Scoping Review. J Med Internet Res 2024;26:e65528.
12. World Health Organization. Global strategy on digital health 2020–2025. Geneva: World Health Organization; 2021.
13. De Micco F, Di Palma G, Giacomobono F, De Benedictis A, Cingolani M, Tambone V, et al. Laboratory medicine between technological innovation, rights safeguarding, and patient safety: A bioethical perspective. Open Med (Wars) 2025;20(1):20251153.
14. Lee J, Kim H, Choi SJ. Do hospital data breaches affect health information technology investment? Digit Health 2024;10:20552076231224164.