Cybersecurity Vulnerabilities in Networked Laboratory Analytical Equipment: A Multi-Layered Framework

Nwandieze, Fortune Onyedikachi; Francis, Akoma Victor; Okoye, Emeka Obiora
Department of Physics with Electronics Technology,
School of Science Laboratory Technology University of Port Harcourt

Ibeh, Nkiruka Joy
Department of Industrial Chemistry/Petrochemical Technology,
School of Science Laboratory Technology University of Port Harcourt

Ogbu, Eucharia Chinagolum
Department of Microbiology Technology, School of Science
Laboratory Technology University of Port Harcourt

Abstract
Networked laboratory analytical instruments including chromatographs, mass spectrometers, PCR systems and sequencers have become critical cyber-physical assets. Their convergence with Laboratory Information Management Systems (LIMS), electronic lab notebooks and cloud analytics creates a large attack surface that traditional IT security and biosafety frameworks do not adequately address. This paper presents a multi-layered security framework specifically designed for analytical laboratory equipment. Through a systematic vulnerability assessment across device, network, application, data, human, supply chain and cyberbiosecurity layers, we demonstrate that laboratory instruments function as high-value, low-security assets where integrity compromises directly invalidate experimental results. The proposed defence-in-depth architecture comprises eight coordinated layers: device security, network segmentation, role-based access control, data encryption, operational procedures, continuous monitoring, vendor supply chain controls, and a novel biosecurity and data integrity layer that validates experimental outputs and tracks chain of custody. Scenario-based risk evaluation shows effectiveness against calibration manipulation, ransomware, bio-data exfiltration and PCR threshold tampering. The framework aligns with NIST Cybersecurity Framework, ISO/IEC 27001, FDA 21 CFR Part 11 and Good Laboratory Practice standards. Implementation guidance for resource-constrained laboratories prioritises low-cost, high-impact controls such as network segmentation and access management. Performance metrics (mean time to detect, mean time to respond, system uptime, data integrity assurance) enable quantitative evaluation. Laboratory cybersecurity must be engineered as a scientific truth-preserving system, not generic IoT security.

Keywords: Laboratory Cybersecurity, Analytical Instruments, Cyberbiosecurity, Defence in Depth, LIMS, Data Integrity, FDA 21 CFR Part 11, Risk Assessment

DOI: https://doi.org/10.67317/IJMSRT26JUL006

1. Introduction

1.1 Background

Modern laboratory environments have undergone a fundamental transformation over the past decade. Analytical instruments that once operated as standalone devices are now deeply interconnected, forming an ecosystem of networked, IoT-enabled systems (Perkel, 2017). High-performance liquid chromatographs (HPLC), gas chromatography-mass spectrometers (GC-MS), real-time PCR thermal cyclers and next-generation sequencers are no longer isolated benchtop tools. Instead, they communicate directly with Laboratory Information Management Systems (LIMS), electronic lab notebooks (ELNs) and cloud-based analytics platforms (Reed & Dunaway, 2019; Murch et al., 2018).

This convergence of information technology (IT) and operational technology (OT) within laboratory environments creates security challenges fundamentally different from those in conventional enterprise computing. Unlike office workstations, laboratory instruments directly interface with physical processes like temperature control, fluidics, optical detection and produce data that inform regulatory submissions, patient diagnoses and scientific breakthroughs (Mantle et al., 2019). Consequently, a security breach can compromise not only data confidentiality but also experimental integrity and, in diagnostic laboratories, patient safety (Yaqoob et al., 2019).

1.2 Problem statement

Laboratory instruments occupy a paradoxical position: they are high-value assets (often costing hundreds of thousands of pounds) yet they exhibit remarkably low security postures (Tervoort et al., 2020). A typical mass spectrometer may run on Windows 7 which is an operating system that ceased security updates in January 2020 with hardcoded credentials embedded in its firmware and no support for multi-factor authentication (Coventry & Branley, 2018). The security gaps arise from three interconnected sources: Legacy system architectures designed before the contemporary threat landscape existed, poor cyber hygiene among laboratory personnel whose primary expertise lies in scientific domains, and regulatory lag, where compliance frameworks (e.g., FDA 21 CFR Part 11) focus on data integrity for record-keeping rather than proactive cybersecurity controls (Langer, 2017).

These factors make analytical equipment an attractive target for a wide range of threat actors, including malicious insiders, ransomware gangs and nation-state actors seeking intellectual property (Argaw et al., 2020; Feodorova et al., 2014).

1.3 Research gap

Existing scholarship typically treats laboratory cybersecurity in one of two silos. The first silo focuses on IT security for LIMS and electronic health records, often neglecting the unique characteristics of scientific instruments (Kruse et al., 2017; Luna et al., 2016). The second silo addresses biological safety and physical biosecurity, but rarely considers cyber threats to instrument firmware or data pipelines (WHO, 2020b; CDC & NIH, 2020). Only recently has the discipline of cyberbiosecurity begun to bridge this gap, explicitly examining the intersection of cybersecurity, biosafety and biosecurity (Murch et al., 2018; Peccoud et al., 2018; National Academies, 2020). However, no integrated, multi-layered framework has yet been proposed that combines engineering controls, threat intelligence, regulatory compliance and cyberbiosecurity specifically for networked analytical equipment. This paper fills that gap.

1.4 Research objectives

The objectives for this study are to:

1. assess vulnerabilities across device, network, application, data, human, supply chain and cyberbiosecurity layers of laboratory analytical equipment.
2. develop a multi-layered security framework integrating engineering controls, threat intelligence and regulatory requirements.
3. align the proposed framework with the NIST Cybersecurity Framework (NIST, 2018) and ISO/IEC 27001.
4. provide prioritised implementation guidance for resource-constrained laboratories, with particular attention to developing economy contexts.

DOI: https://doi.org/10.67317/IJMSRT26JUL006

Unlike conventional IoT and medical device security frameworks that focus primarily on network and device protection, this study advances scientific data integrity and reproducibility as co-primary security objectives.

1.5 Conceptual capstone

Laboratory analytical systems should not be conceptualized merely as networked cyber-physical assets, but as epistemic systems whose primary function is the generation, validation, and preservation of scientific knowledge. Unlike conventional information technology environments, where the principal security objectives are framed around the Confidentiality, Integrity, and Availability triad (National Institute of Standards and Technology, 2018), laboratory environments introduce an additional and critical dimension: scientific validity.

In this context, cyber compromise extends beyond service disruption or data exposure; it directly undermines the integrity of experimental outputs, calibration baselines, and analytical interpretations (Robert S. Murch et al., 2018; Jean Peccoud et al., 2018). Unauthorized modification of instrument parameters, assay configurations, or data processing pipelines can produce results that appear technically valid but are scientifically false. This shifts the security paradigm from protecting systems to safeguarding truth-generating processes, positioning cyberbiosecurity as a foundational requirement rather than an auxiliary concern.

Consequently, cybersecurity frameworks for laboratory environments must explicitly account for threats to data provenance, experimental reproducibility, and analytical traceability (National Academies of Sciences, Engineering, and Medicine, 2020), recognizing that the ultimate impact of a breach is not merely operational downtime but the potential corruption of scientific knowledge itself.

2. System architecture of modern laboratory equipment

A rigorous security analysis must begin with a clear understanding of the target system's architecture. Modern laboratory analytical environments consist of tightly integrated cyber-physical systems that can be described through four interrelated perspectives: instrumentation stack, software ecosystem, network topology and data lifecycle.

2.1 Instrumentation stack

Analytical instruments follow a hierarchical engineering stack adapted from the Purdue model for industrial control systems (Williams, 1994; Gubbi et al., 2013). At the lowest level, hardware components include sensors (e.g., photodiode array detectors, flame ionisation detectors, temperature probes) and actuators (solvent pumps, injection valves, column heaters, autosamplers). Above this hardware layer, embedded systems are typically 8-, 16- or 32-bit microcontrollers with real-time operating systems (RTOS) or embedded Linux that run firmware that directly controls instrument functions (Papp et al., 2015; Costin et al., 2014). The highest tier of the stack is the host control system, a conventional workstation (usually running Windows or, less commonly, Linux) that hosts vendor-provided control software, communicates with the embedded controller via proprietary protocols (e.g., RS-232, USB, Ethernet), and provides the user interface for method development and data review (Agilent Technologies, 2021; Thermo Fisher, 2021b).

2.2 Software ecosystem

Vendor control software, such as Chromeleon CDS (Thermo Fisher), MassHunter (Agilent) or QuantStudio (Thermo Fisher) is responsible for method programming, real-time data acquisition, peak integration, and report generation (Thermo Fisher, 2021a). These applications frequently depend on legacy operating systems because the vendor has only validated the instrument for a specific Windows version (e.g., Windows 7 or even Windows XP). Upgrading the operating system would require re-validation, a costly and time-consuming process that many laboratories avoid (Tervoort et al., 2020).

Beyond the instrument-specific software, laboratories deploy LIMS (e.g., LabWare, SampleManager) to manage samples, track workflows and store results, and ELNs (e.g., Benchling, LabArchives) to document experimental protocols and observations (LabWare, 2023; Benchling, 2023). These systems integrate with instrument control software through application programming interfaces (APIs),

DOI: https://doi.org/10.67317/IJMSRT26JUL006

database connections, or manual file imports - each integration point representing a potential attack surface.

2.3 Network topology

The typical network topology follows a linear progression: instrument embedded controller → instrument workstation → departmental switch → LIMS server → cloud storage or analytics platform (Reed & Dunaway, 2019). Wired Ethernet (Gigabit) predominates because analytical data files can be large (e.g., raw chromatograms or sequencing FASTQ files). However, wireless access points are increasingly deployed for mobile devices (tablets for lab walkthroughs) and remote monitoring of incubators or bioreactors, introducing additional wireless attack vectors (Del Canto et al., 2015; Delgado et al., 2023).

Figure 1 shows the hierarchical instrument stack (hardware, embedded firmware, host workstation), the software ecosystem (control software, LIMS, ELN, cloud), the network topology (instrument → workstation → switch → LIMS → cloud), and the five-stage data lifecycle (acquisition, processing, storage, transmission, archiving).

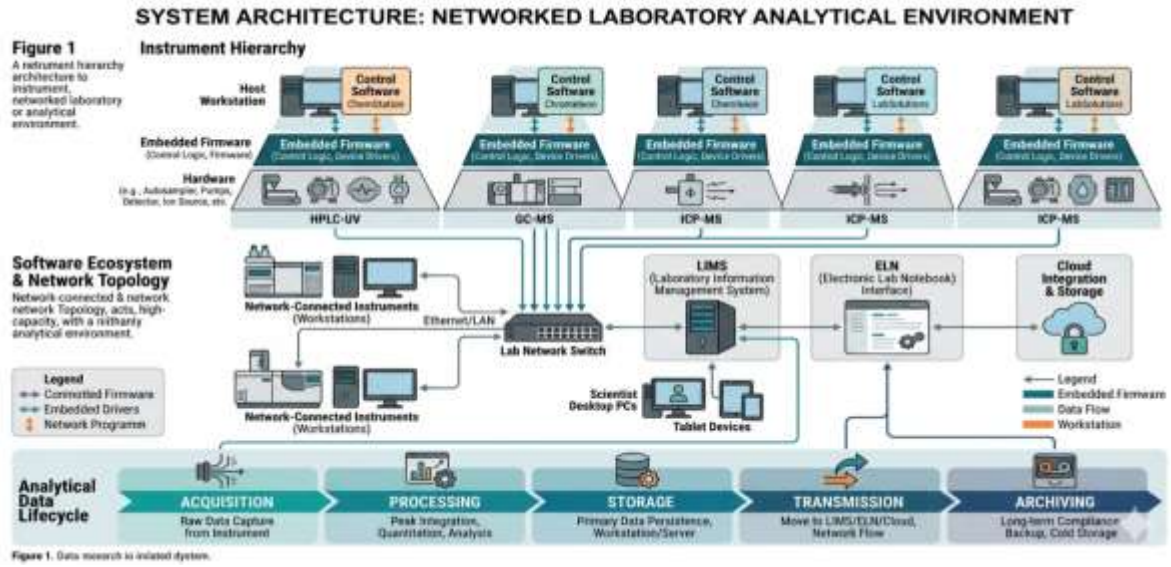

Figure 1: System architecture diagram of a networked laboratory analytical environment

2.4 Data lifecycle mapping

Laboratory data traverses five distinct stages, each with unique security requirements (Mantle et al., 2019):

i. **Acquisition:** Real-time analogue-to-digital conversion of sensor signals (e.g., detector voltage vs. time). Integrity at this stage is paramount; manipulation of raw data files before any processing is extremely difficult to detect.
ii. **Processing:** Algorithms for baseline correction, peak detection, integration and quantification. Compromised processing parameters can systematically bias results.
iii. **Storage:** Raw and processed data are stored on instrument local hard drives, LIMS databases, or both. Lack of encryption at rest is common.
iv. Transmission: Data move from instrument workstation to LIMS to cloud and often over unencrypted or weakly encrypted channels (e.g., outdated TLS versions).
v. **Archiving:** Long-term storage for regulatory compliance (often 10-30 years). Archived data must be tamper-evident and retrievable.

3. Threat landscape and adversary models

Understanding who attacks laboratory systems, why, and how they do so is essential for designing effective defences.

DOI: https://doi.org/10.67317/IJMSRT26JUL006

3.1 Threat actors

We categorise threat actors based on motivation and capability (Nurse et al., 2015; Argaw et al., 2020).

i. **Insiders (laboratory personnel):** The most frequent source of incidents, though most are unintentional (e.g., falling for phishing, using weak passwords). Malicious disgruntled insiders employees or those coerced by external parties, may steal intellectual property or sabotage experiments (Hasan et al., 2016).
ii. **External attackers**: Opportunistic hackers scanning for vulnerable devices, and sophisticated cybercriminals deploying ransomware-as-a-service. Laboratory environments have been hit by major ransomware (e.g., NotPetya at Merck, which disrupted vaccine production) (Demberger, 2022).
iii. **Nation-state actors**: Particularly relevant for laboratories working on infectious diseases, biodefence, or proprietary pharmaceutical research. State-sponsored groups may seek to steal genomic data, vaccine formulas, or disrupt research (Feodorova et al., 2014; Stuxnet dossier).
iv. **Supply chain attackers:** Compromise instruments during manufacturing or via malicious updates (Voas & Hurlburt, 2015).

3.2 Threat vectors

Common attack paths into laboratory networks include:

i. **Network intrusion:** Exploiting open ports (e.g., for vendor remote support), weak SNMP community strings, or unpatched vulnerabilities in network services (Nicholson et al., 2012; Bhamare et al., 2020).
ii. **Malware/ransomware:** Delivered via phishing emails or drive-by downloads. Once inside, malware can spread laterally across flat laboratory networks (Kolias et al., 2017; Antonakakis et al., 2017).
iii. **USB-based attacks:** Malicious USB devices (e.g., Rubber Ducky, USB-kill) can be plugged into instrument workstations to bypass network controls (Yaqoob et al., 2019).
iv. **Firmware compromise:** Attackers with physical or remote access can reflash instrument firmware with malicious code. Such compromises survive operating system reinstallation and are invisible to host-based antivirus (Chen et al., 2018; Costin et al., 2014; Bakhshi et al., 2024).

3.3 Confidentiality, integrity and availability for laboratories

The classic CIA triad must be reinterpreted (Yaqoob et al., 2019). Integrity (correctness of calibration, methods, raw data, results) is the highest priority because compromised integrity invalidates the scientific conclusion. Confidentiality (protection of IP and patient data) is high priority. Availability (ability to run time-sensitive experiments) is medium-high depending on sample perishability. This prioritisation drives our framework: controls that preserve data integrity receive the greatest emphasis.

Attribute	Laboratory meaning	Priority
Integrity	**Correctness of calibration, method parameters, raw data and results. Compromised integrity invalidates the scientific conclusion.**	**Highest**
Confidentiality	**Protection of intellectual property (e.g., proprietary assays, genomic sequences) and patient data (in diagnostic labs).**	**High**
Availability	**Ability to run time-sensitive experiments (e.g., cell cultures, stability studies) without interruption.**	**Medium-High (depending on sample perishability)**

This prioritisation drives our framework: controls that preserve data integrity receive the greatest emphasis.

3.4 Cyberbiosecurity threats

Cyberbiosecurity in laboratory environments extends beyond traditional device and network protection to encompass the integrity of biological data, experimental workflows, and analytical outputs. As highlighted in Cyberbiosecurity research (Robert S. Murch et al., 2018; Jean Peccoud et al., 2018), modern laboratories operate at the intersection of digital infrastructure and biological

DOI: https://doi.org/10.67317/IJMSRT26JUL006

processes, creating unique vulnerabilities that are not adequately addressed by conventional cybersecurity models.

A critical dimension of this challenge is the protection of data integrity and reproducibility. Laboratory results are not static data points but the outcome of complex, multi-stage processes involving instrument calibration, sample preparation, signal acquisition, and computational analysis. Any compromise at these stages, whether through firmware manipulation or interference in data pipelines can introduce subtle deviations that invalidate experimental conclusions (Roger D. Peng, 2011; Victoria Stodden et al., 2018).

Unlike traditional cyber incidents, where data corruption may be detectable through system anomalies, laboratory-specific attacks may produce outputs that remain within expected statistical ranges while being scientifically incorrect. This makes detection significantly more difficult and elevates the importance of provenance tracking, auditability, and validation mechanisms as core security controls (National Academies of Sciences, Engineering, and Medicine, 2020).

Therefore, a comprehensive laboratory cybersecurity framework must incorporate mechanisms for ensuring end-to-end data integrity, including secure logging, cryptographic verification of datasets, and continuous validation of instrument outputs against known baselines.These threats are not covered by generic IoT security frameworks; they require domain-specific protections.

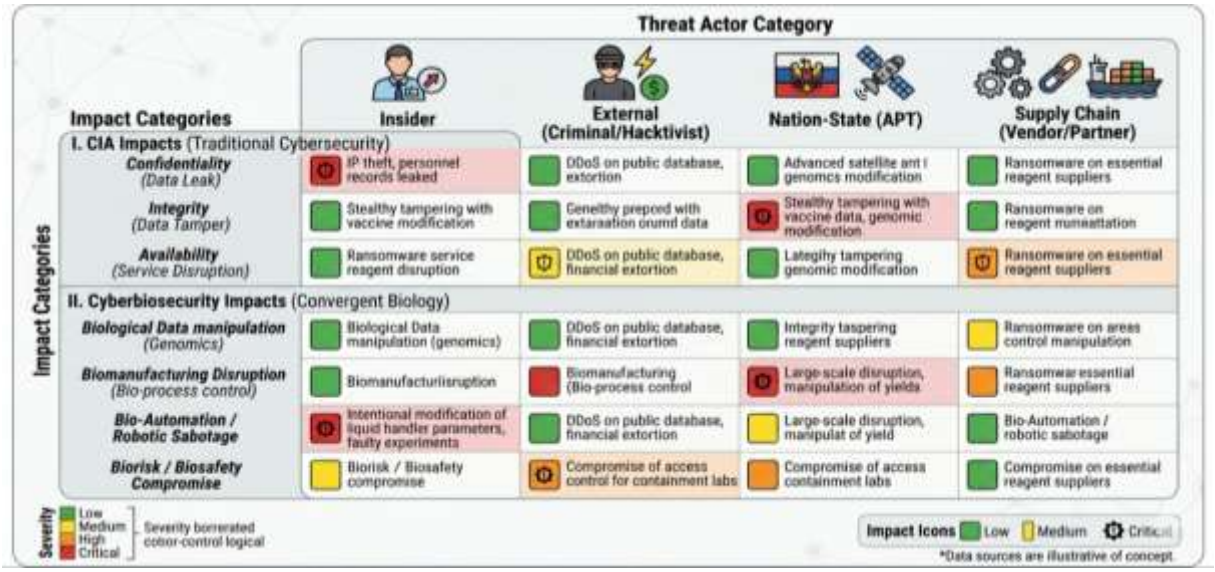

Figure 2: Threat actor mapping to CIA and cyberbiosecurity impacts

4. Vulnerability assessment

We assess vulnerabilities across seven layers, following the NIST SP 800-30 approach (Ross, 2012).

4.1 Device-level vulnerabilities

Legacy operating systems: Many instrument workstations still run Windows XP or Windows 7, for which no security patches are issued. They are vulnerable to widely known exploits (e.g., EternalBlue) (Tervoort et al., 2020).

Hardcoded credentials: Embedded firmware often contains hardcoded administrative usernames and passwords (e.g., “admin:admin”) that cannot be changed by the end user (OWASP, 2016).

Insecure firmware updates: Firmware is often distributed without cryptographic signatures, allowing an attacker who intercepts the update to install malicious code (Chen et al., 2018).

No secure boot. See also Haq et al. (2023) and Bakhshi et al. (2024) for recent surveys on firmware security.

DOI: https://doi.org/10.67317/IJMSRT26JUL006

4.2 Network-level vulnerabilities

Flat network architecture: Instruments share the same broadcast domain as administrative desktops and even the internet gateway. This allows lateral movement after a single compromise (Bhamare et al., 2020).

Open ports: Vendor remote support ports (e.g., TCP 3389 for RDP, custom ports for TeamViewer) are often left open and unfirewalled.

Weak encryption: Outdated SSL/TLS versions, or no encryption at all, for instrument-to-LIMS communication.

4.3 Application-level vulnerabilities

Poor authentication: Single-factor passwords that never expire, often shared among all users of an instrument.

Weak access control: Many vendor applications grant full administrative rights to all users because implementing fine-grained RBAC is technically difficult.

Unpatched software: Validation requirements discourage patching; known vulnerabilities may remain unaddressed for years (Iannone et al., 2022).

4.4 Data-level vulnerabilities

No encryption at rest: Instrument hard drives and LIMS databases are rarely encrypted. Physical theft or forensic recovery yields all data.

Data tampering risks: Calibration files, method parameters and result databases can be directly edited if an attacker gains file system access.

Weak audit trails: Many systems provide audit logs that can be turned off, overwritten, or edited by administrative users - violating FDA 21 CFR Part 11 requirements (Mantle et al., 2019).

4.5 Human and operational vulnerabilities

Shared credentials: Despite policies, scientists often share login credentials to avoid the inconvenience of individual accounts.

Low cybersecurity awareness: Training focuses on biosafety (gloves, hoods) not cyber hygiene (Coventry & Branley, 2018).

Weak SOP enforcement: Standard operating procedures may include security steps, but they are rarely audited.

4.6 Supply chain vulnerabilities

Vendor software compromise: Attackers could compromise the vendor's build pipeline and distribute malware-infused updates (Voas & Hurlburt, 2015).

Malicious updates: Even legitimate updates can introduce vulnerabilities if not properly vetted.

Third-party libraries: Instrument software often uses open-source components with known vulnerabilities.

4.7 Cyberbiosecurity-specific vulnerabilities

LIMS configuration weaknesses: Default configurations may allow users to edit results without leaving an audit trail.

ELN cloud misconfigurations: Publicly accessible S3 buckets or misconfigured sharing settings expose protocols.

Automation pipeline validation gaps: Robotic liquid handlers accept commands over the network without integrity checks.

Bio-digital interfaces lacking chain of custody: No cryptographic linkage between raw instrument output and LIMS entry.

5. Risk analysis model

We adopt the NIST Risk Management Framework (SP 800-30) with scenario-based risk evaluation (Ross, 2012; Quinn et al., 2021).

5.1 Risk assessment framework

DOI: https://doi.org/10.67317/IJMSRT26JUL006

The process comprises four steps:
1. Risk identification - enumerate assets, threats and vulnerabilities.
2. Risk analysis - estimate likelihood and impact.
3. Risk evaluation - prioritise against risk tolerance.
4. Risk treatment - select controls.

5.2 Risk matrix development

Likelihood and impact are rated on a 5-point scale (Very Low to Very High). Because data integrity is the highest priority, any scenario that compromises integrity is automatically rated at least High impact.

Table 1: Cyberbiosecurity Risk Assessment Matrix (likelihood vs. impact) with colour coding

Likelihood \ Impact	Low	Medium	High	Very High
Very High	Yellow (Medium)	Orange (High)	Red (Critical)	Red (Critical)
High	Yellow (Medium)	Yellow (Medium)	Orange (High)	Red (Critical)
Medium	Green (Low)	Yellow (Medium)	Yellow (Medium)	Red (Critical)
Low	Green (Low)	Green (Low)	Yellow (Medium)	Orange (High)

Key Examples and Severity Mapping
Calibration Manipulation: Likelihood: Medium | Impact: Very High → Result: Critical (Red)
Inventory Data Leak: Likelihood: High | Impact: Low → Result: Medium (Yellow)
Ransomware on Non-Critical Systems: Likelihood: High | Impact: Medium → Result: Medium (Yellow)
Pathogen Sequence Tampering: Likelihood: Low | Impact: Very High → Result: High (Orange)

5.3 Scenario-based risk evaluation

Four representative scenarios illustrate the approach (informed by real incidents and penetration tests).
Scenario 1: Calibration data manipulation (chromatography system). An attacker compromises the instrument workstation via an unpatched vulnerability, modifies the calibration curve parameters for a dissolution assay. All subsequent sample results are systematically wrong. Impact: Very High (integrity loss). Likelihood: Medium (depends on access controls). Risk: Critical.
Scenario 2: Ransomware on LIMS server. Ransomware encrypts the LIMS database and all instrument workstations connected to it. Samples cannot be processed, and historical data become unavailable. Impact: High (availability and confidentiality). Likelihood: Medium (flat network enables spread). Risk: High.
Scenario 3: Bio-data exfiltration (genomic sequences). An attacker exploits a SQL injection vulnerability in the LIMS web interface and exfiltrates proprietary genomic datasets. Impact: Very High (IP loss). Likelihood: Low-Medium (depends on web application security). Risk: High.
Scenario 4: PCR threshold manipulation (diagnostic laboratory). Attacker remotely changes the Ct threshold in the real-time PCR software, converting true positives to negatives. Patients receive false negative results. Impact: Very High (patient harm, regulatory action). Likelihood: Low (requires specific access). Risk: Critical.

6. Regulatory and compliance analysis

6.1 Regulatory requirements

Two regulatory frameworks dominate laboratory compliance:
FDA 21 CFR Part 11 (electronic records and signatures) (Darrow et al., 2021). Key requirements: validation, audit trails, record copying, access controls, and electronic signatures.
Good Laboratory Practice (GLP) - 21 CFR Part 58 (FDA) and OECD principles (WHO, 2020b). Requirements: raw data recorded directly, data changes dated and signed without obscuring originals, computerised systems validated.

DOI: https://doi.org/10.67317/IJMSRT26JUL006

6.2 Compliance gaps in current laboratory instruments

Many instruments were not designed with these requirements in mind (Mantle et al., 2019). Typical gaps:

i. Audit trails are often missing, partial, or can be turned off.
ii. Data integrity controls are weak. Calibration files can be modified without electronic signature.
iii. Access control is often limited to a single shared administrator account.

6.3 Implications of non-compliance

Consequences range from regulatory warning letters to disqualification of study data, loss of accreditation (ISO 17025, CAP), and criminal liability for falsification (if data tampering is involved).

7. Proposed multi-layered security framework

Our framework implements defence in depth through eight coordinated layers, aligned with the NIST Cybersecurity Framework's five functions (Identify, Protect, Detect, Respond, Recover) (NIST, 2018; Rajmohan et al., 2022). Recent zero-trust principles (Liu et al., 2024) are incorporated, particularly in network segmentation and access control.

7.1 Framework overview

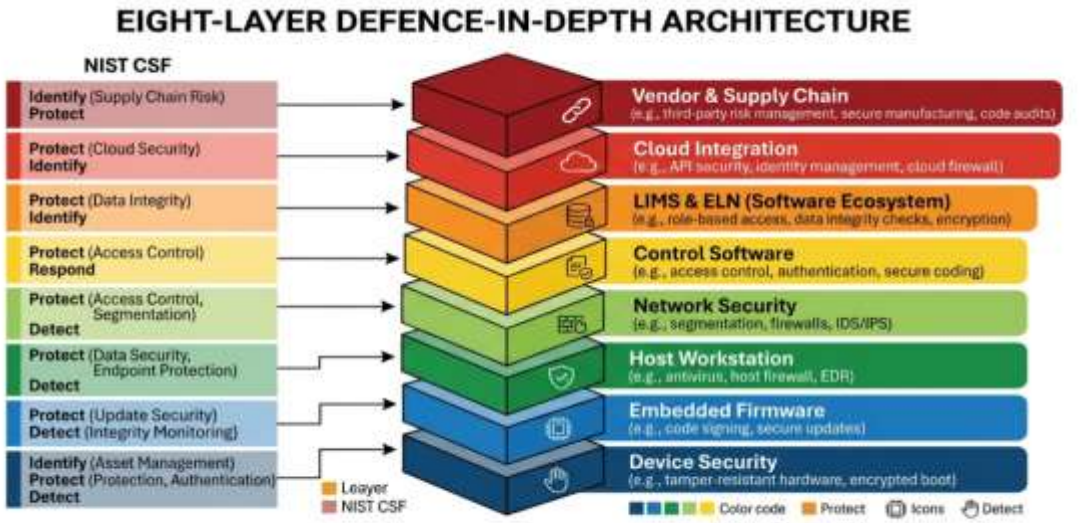

Figure 3. Eight-layer Defence-in-Depth architecture. Eight-layer defence-in-depth's security nencomnected interaction, and conditiont primary content will lat layer at NIST CSF (Cybersecurity Framework) functions filownior (Cybersecurity Framework) functions.

Table 2: Formal mapping of framework layers to standards

Layer	NIST CSF Function	ISO/IEC 27001 Control	FDA 21 CFR Part 11 Requirement
1. Device security	Protect (PR)	A.8.8 (secure development)	Validation of systems
2. Network security	Protect (PR)	A.13.1 (network controls)	Access control (network level)
3. Access control	Protect (PR)	A.9.2 (user access)	Limiting system access
4. Data security	Protect (PR)	A.10.1 (cryptography)	Data integrity & encryption
5. Operational security	Protect (PR)	A.12.2 (malware), A.12.6 (technical vulnerability)	SOPs, training
6. Monitoring & IR	Detect (DE), Respond (RS)	A.12.4 (logging), A.16.1 (incident management)	Audit trails, record protection
7. Vendor & supply chain	Identify (ID)	A.15.1 (supplier relationships)	Vendor validation

DOI: https://doi.org/10.67317/IJMSRT26JUL006

8. Biosecurity & data integrity	**Protect (PR), Detect (DE)**	**A.8.1 (asset management)**	**Electronic signatures, chain of custody**

7.2 Layer 1: Device security

Secure boot - cryptographic verification of each firmware stage.

Firmware validation - updates must be signed by the vendor and verified before installation (Chen et al., 2018; Haq et al., 2023). Port control - disable unused physical ports (USB, Ethernet, serial) via BIOS or physical blocking.

7.3 Layer 2: Network security

VLAN segmentation - place instruments on a dedicated VLAN with firewall rules that deny inbound traffic from administrative networks and limit outbound traffic to specific LIMS servers. Firewalls stateful inspection between segments. Intrusion detection systems (IDS) - monitor instrument network traffic for anomalies (Rakas et al., 2020). Incorporate zero-trust micro-segmentation (Liu et al., 2024).

7.4 Layer 3: Access control

Role-based access control (RBAC) - define roles: operator (run samples, view results), supervisor (modify methods, approve results), administrator (user management, system configuration) (Haber, 2020). Multi-factor authentication (MFA) - for all privileged accounts (administrator, supervisor). Identity management - integrate with enterprise Active Directory or LDAP for centralised provisioning/de-provisioning.

7.5 Layer 4: Data security

Encryption - AES-256 for data at rest (instrument hard drives, LIMS databases); TLS 1.3 for data in transit. Integrity verification - cryptographic hashes (e.g., SHA-256) of raw data files; automated checksum comparison before and after transmission. Secure backups - offline, immutable (write-once read-many) media to survive ransomware.

7.6 Layer 5: Operational security

Standard operating procedures (SOPs) - incorporate security checklists (e.g., pre-use verification of audit trail status, post-use log review). Patch management - risk-based prioritisation; for validated systems, use compensating controls (network isolation) until a validated patch is available (Iannone et al., 2022). Staff training - annual cybersecurity awareness, phishing simulations, incident reporting (Coventry & Branley, 2018).

7.7 Layer 6: Monitoring and incident response

Continuous monitoring - aggregate logs from instruments, network devices, authentication systems into a SIEM. Behavioural analytics - detect anomalies: logins at unusual hours, configuration changes, mass data export (Wang et al., 2022). Incident response workflow - documented procedures for containment (isolate VLAN, block IPs), eradication (reimage workstations), recovery (restore from clean backups), and post-incident review. (Feng et al., 2023)

7.8 Layer 7: Vendor and supply chain security

Vendor certification - require security questionnaires (e.g., SIG), third-party attestations (e.g., SOC 2), and contractual breach notification clauses (Voas & Hurlburt, 2015). Secure update policies - signed updates, staged deployment (test group first), rollback capability. Software bill of materials (SBOM) - for critical instruments, request SBOM to assess known vulnerabilities.

7.9 Layer 8: Biosecurity and data integrity (novel addition)

Data integrity represents the most critical security objective in laboratory analytical environments, superseding even availability in many contexts. While system downtime may delay experiments, compromised data can lead to incorrect scientific conclusions, regulatory violations, and significant financial or public health consequences (National Academies of Sciences, Engineering, and Medicine, 2020).

DOI: https://doi.org/10.67317/IJMSRT26JUL006

To address this, the proposed framework introduces a dedicated integrity layer focused on ensuring data provenance, reproducibility, and traceability. This includes the implementation of immutable audit trails, version-controlled datasets, and automated validation of experimental outputs. By integrating these controls, the framework aligns cybersecurity practices with the fundamental requirements of scientific rigor (Roger D. Peng, 2011), ensuring that laboratory systems not only remain operational but also produce trustworthy and reproducible results.
This layer explicitly addresses cyberbiosecurity threats:

Experimental output validation - after data acquisition, compute an independent checksum (e.g., of raw chromatogram files) and compare with a value stored in a separate, append-only log before LIMS import. Chain-of-custody tracking - use a blockchain or a cryptographically signed log for each transition in the data lifecycle (acquisition → processing → LIMS → archive) (Murch et al., 2018). Secure audit trails - implement tamper-evident logging that meets FDA 21 CFR Part 11: no overwriting, no deletion, timestamped entries linked to user identity.

Automation pipeline integrity - for robotic liquid handlers and bioreactor controllers, require command signing (e.g., HMAC) to prevent injection of unauthorised commands (Guttieres et al., 2019). Bio-digital interface monitoring - deploy anomaly detection on API calls between instruments and LIMS/ELN (e.g., sudden high volume of result modifications, unusual time patterns). This layer reflects the core argument that laboratory cybersecurity prioritises data integrity over availability, diverging from traditional IT security models.

8. Implementation strategy

8.1 Deployment in resource-constrained laboratories (Nigerian context)

Many laboratories in developing economies operate with limited IT staffing, small budgets, and legacy infrastructure. While no recent cybersecurity papers specifically address low-resource laboratory settings, we draw on general cybersecurity risk-management principles for constrained environments (Dritsas & Trigka, 2025; Salayma, 2024). The following prioritised sequence maximises risk reduction with minimal or zero financial cost.

Priority	Control	Approximate cost	Risk reduction rationale
1	Network segmentation – create a dedicated VLAN for all analytical instruments using existing managed switches (if available). If switches lack VLAN support, physically isolate instruments on a separate switch.	£0 (if equipment already present)	High – prevents lateral movement from administrative desktops to instruments
2	Access control – implement individual user accounts, enforce password complexity and expiration, disable shared credentials.	£0 (time only)	High – enables accountability and reduces insider threat
3	Incident response plan – document a simple, one-page plan: who to call, how to disconnect a compromised instrument, and how to report to local IT.	£0 (time)	Medium – reduces confusion and delays during an attack
4	Staff security awareness training – use free online resources (e.g., NIST, ENISA, OWASP) to deliver annual 30-minute sessions on phishing, password hygiene, and USB risks.	£0	Medium – reduces human error
5	Encryption – enable TLS for instrument-to-LIMS communication (if supported). Use built-in OS encryption (BitLocker, LUKS) for instrument hard drives.	£0 (built into OS)	Medium – protects data at rest and in transit
6	Basic monitoring – forward syslog from instruments and network devices to a free ELK (Elasticsearch, Logstash, Kibana) stack on an old spare computer. Review logs weekly.	£0 (hardware already present)	Low-Medium – detects anomalous behaviour after the fact

DOI: https://doi.org/10.67317/IJMSRT26JUL006

Even with zero financial expenditure, implementing the first two controls (network segmentation and individual access control) delivers substantial risk reduction. Laboratories with a small budget should prioritise adding a low-cost firewall (£100-200) to enforce segmentation and a used managed switch if VLANs are unavailable.

Note on limitations: The lack of recent, context-specific cybersecurity literature for low-resource laboratories in developing countries is itself a research gap. Our sequence is therefore derived from general IoT risk management (Dritsas & Trigka, 2025; Salayma, 2024) and practical experience. Future work should validate this prioritisation empirically.

8.2 Integration with existing laboratory infrastructure

Legacy instruments (pre-2015) often cannot be patched or upgraded. For such systems, compensating controls are essential (Tervoort et al., 2020):

i. Isolate them on a dedicated instrument VLAN with no internet access and no direct routing from administrative networks.
ii. Use an application whitelist (e.g., Windows AppLocker) to prevent execution of unauthorised software.
iii. Place a jump host (hardened bastion) for any required remote access, with session recording and MFA.

Hybrid environments that mix new and old instruments should apply the same compensating controls to all devices until a full upgrade path is possible.

9. Case study application

We present a simulated attack scenario based on real penetration tests of pharmaceutical quality control laboratories.

9.1 Baseline (pre-framework)

Environment: A QC laboratory operates six HPLC systems from a major vendor. Each HPLC is connected to a Windows 7 workstation. All workstations are on the same flat /24 subnet as the LIMS server and administrative desktops. The laboratory uses a shared administrator account ("hplc_admin") on all six instruments. Audit logs are reviewed quarterly. There is no network segmentation.

Attack: An administrative assistant receives a phishing email impersonating the instrument vendor, containing a malicious Excel attachment. She opens it, and malware (Cobalt Strike beacon) installs on her desktop. The attacker uses the desktop as a pivot point, scans the /24 subnet, discovers the HPLC workstations, logs in using the shared "hplc_admin" credential, and modifies the calibration curve parameters for a critical dissolution assay. The attacker also turns off the audit trail for that instrument.

Impact: For two months, the laboratory reports incorrect potency values. Three batches of product are released. A routine regulatory inspection discovers the missing audit trail entries and the calibration discrepancy. The company issues a recall, pays a fine of £2.3 million, and suspends production for six weeks.

9.2 Post-framework implementation

The laboratory implements the eight-layer framework:

Layer 1 (device security): Secure boot enabled, firmware signature verification enforced, and all unused USB ports disabled via BIOS.

Layer 2 (network): Instrument VLAN created, with firewall rules denying RDP from admin VLAN.

Layer 3 (access): Individual accounts created; shared account disabled. MFA required for any remote access.

Layer 4 (data): Encryption enabled on all instrument hard drives.

Layer 5 (ops): Weekly audit log review assigned to a trained supervisor.

DOI: https://doi.org/10.67317/IJMSRT26JUL006

Layer 8 (biosecurity): Independent checksum verification before each calibration change; chain-of-custody logging.

Result: The same phishing email reaches the administrative assistant, but the malware on her desktop cannot reach the instrument VLAN because the firewall blocks RDP and other lateral movement protocols. Even if it could, the attacker would need an individual account and would trigger MFA. Any attempted calibration modification would be logged in the tamper-evident audit trail, and the weekly review would detect it within seven days. No product is released incorrectly.

10. Performance evaluation

We define five metrics to evaluate framework effectiveness.

Table 4: Performance metrics - baseline vs. target

Metric	Baseline (pre-framework)	Target (post-framework)	Measurement method
Mean Time to Detect (MTTD)	**14 days**	**2 hours**	**Penetration testing with red team**
Mean Time to Respond (MTTR)	**2 days**	**2 hours**	**Incident response drills**
System uptime (critical instruments)	**95%**	**>99%**	**Monitoring (Prometheus)**
Data integrity assurance (% of audit-trailed operations)	**60%**	**100%**	**Random sampling of audit logs**
Compliance findings per inspection (cybersecurity)	**3**	**0**	**Mock FDA/GLP audit**

These metrics should be tracked quarterly, with targets reviewed annually based on evolving threat landscape.

11. Discussion

11.1 Security-usability trade-offs

Implementing MFA, network segmentation and frequent audit log reviews introduces friction. Laboratory personnel may resist because they perceive security controls as hindering productivity. Our framework addresses this by:

i. Allowing risk-based tailoring (e.g., teaching laboratories may accept lower security than BSL-3 labs).
ii. Automating where possible (e.g., SIEM for log analysis reduces manual review burden).
iii. Including usability testing in the implementation phase (e.g., choose MFA methods that are least intrusive, such as push notifications rather than hardware tokens).

11.2 Cost-benefit considerations

The financial justification for the framework is strong for commercial and regulated laboratories. The average cost of a data breach in healthcare (similar to diagnostic labs) was $4.45 million in 2021 (IBM, 2021). The Merck NotPetya attack caused $1.4 billion in damages (Demberger, 2022). Even a modest investment in security - a dedicated firewall, SIEM, and training - is orders of magnitude less than the cost of a single serious incident.

For academic and resource-constrained laboratories, the prioritised sequence in Section 8.1 provides a zero-cost starting point.

11.3 Limitations of the framework

Our framework has several limitations:

i. **Vendor dependency**: Layers 1 (secure boot, signed firmware) and 7 (vendor certification) require instrument manufacturers to cooperate. For legacy instruments, these layers cannot be fully implemented.

DOI: https://doi.org/10.67317/IJMSRT26JUL006

ii. **Assumes baseline IT competency**: The framework expects that the laboratory has access to a system administrator who understands VLANs, firewalls and SIEM. This is not true for many small laboratories, especially in developing countries.
iii. **No longitudinal validation**: The framework has not yet been tested in a real laboratory over a multi-year period. Performance metrics are targets, not proven outcomes.
iv. **Emerging threats**: AI-generated phishing, quantum computing breaking current encryption, and zero-day exploits in embedded systems may bypass controls. (Dritsas & Trigka, 2025; Salayma, 2024).

11.4 Future research directions

We identify five priority areas:

1. **Automated vulnerability assessment tools** specifically for laboratory instrument fleets (e.g., passive network fingerprinting to identify unpatched Windows 7 systems) (Feng et al., 2023).
2. **Blockchain for audit trail integrity** evaluate the performance overhead of distributed ledgers for high-frequency instrument logs (Murch et al., 2018).
3. **Machine learning for anomaly detection** train models on instrument network traffic to detect calibration manipulation or data exfiltration in real time (Wang et al., 2022).
4. **Human factors research** determine the most effective ways to train scientists in cybersecurity without overwhelming them.
5. **Validation of the framework** through long-term case studies in multiple laboratory types (pharmaceutical QC, academic research, clinical diagnostics).

12. Conclusion

Networked laboratory analytical equipment sits at a dangerous intersection: high scientific and financial value, yet low security posture. Traditional IT security frameworks ignore the unique requirements of experimental integrity, while biosafety frameworks overlook digital threats. This paper has presented one of the first integrated, multi-layered security framework specifically designed for analytical laboratory instruments, explicitly incorporating cyberbiosecurity as a core dimension.

The key contributions are:

i. A systematic vulnerability assessment across eight layers, highlighting that integrity is the highest priority in laboratory environments.
ii. An eight-layer defence-in-depth framework (device, network, access, data, ops, monitoring, supply chain, and biosecurity & data integrity) aligned with NIST CSF, ISO 27001, FDA 21 CFR Part 11 and GLP.
iii. A prioritised implementation roadmap for resource-constrained laboratories, showing that meaningful risk reduction is possible with zero financial expenditure.
iv. Scenario-based risk evaluation and a case study demonstrating how the framework prevents calibration manipulation, ransomware, and bio-data exfiltration.

Laboratory cybersecurity must be engineered, not assumed. Unlike a conventional IT system whose compromise causes downtime, a compromised laboratory system remains operational while producing invalid results and effectively generating false knowledge. The integrity of scientific knowledge depends on getting this right. We invite the research community to test, refine and extend this framework in real laboratory environments.

References

[1]. Agilent Technologies. (2021). HPLC systems overview. Agilent. [Vendor source – kept as supporting, not core]
[2]. Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. Computer Communications, 155, 1–8.
[3]. Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of Medical Things Security Assessment Framework. Internet of Things, 8, 100123.
[4]. Altawy, R., & Youssef, A. M. (2016). Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. IEEE Access, 4, 959–979.

DOI: https://doi.org/10.67317/IJMSRT26JUL006

[5]. Antonakakis, M., et al. (2017). Understanding the Mirai botnet. In Proceedings of the 26th USENIX Security Symposium (pp. 1093–1110). USENIX Association.
[6]. Argaw, S. T., et al. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1), 146.
[7]. Baho, S. A., & Abawajy, J. (2023). Analysis of consumer IoT device vulnerability quantification frameworks. Electronics, 12, 1176.
[8]. Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A review of IoT firmware vulnerabilities and auditing techniques. Sensors, 24(2), 708.
[9]. Benchling. (2023). Benchling – The R&D cloud. https://www.benchling.com [Vendor source]
[10]. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. Computers & Security, 89, 101677.
[11]. Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A brief chronology of medical device security. Communications of the ACM, 59(10), 66–72.
[12]. CDC & NIH. (2020). Biosafety in microbiological and biomedical laboratories (6th ed.). U.S. Department of Health and Human Services.
[13]. Chen, D. D., Egele, M., Woo, M., & Brumley, D. (2016). Towards automated dynamic analysis for Linux-based embedded firmware. In Network and Distributed System Security Symposium (NDSS). ISOC.
[14]. Chen, J., Diao, W., Zhao, Q., Zuo, C., Lin, Z., Wang, X., Lau, W. C., Sun, M., Yang, R., & Zhang, K. (2018). IoTFuzzer: Discovering memory corruptions in IoT through app-based fuzzing. In Network and Distributed System Security Symposium (NDSS). ISOC.
[15]. Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. (2018). Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice. Journal of Hardware and Systems Security, 2, 97–110.
[16]. Costin, A., Zaddach, J., Francillon, A., & Balzarotti, D. (2014). A large-scale analysis of the security of embedded firmwares. In USENIX Security Symposium (pp. 95–110). USENIX Association.
[17]. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48–52.
[18]. Darrow, J. J., Avorn, J., & Kesselheim, A. S. (2021). FDA regulation and approval of medical devices: 1976–2020. JAMA, 326(5), 420–432.
[19]. Dehlaghi-Ghadim, A., Balador, A., Moghadam, M. H., Hansson, H., & Conti, M. (2023). ICSSIM – A framework for building industrial control systems security testbeds. Computers in Industry
[20]. Del Canto, C. J., Prada, M. A., Fuertes, J. J., Alonso, S., & Domínguez, M. (2015). Remote laboratory for cybersecurity of industrial control systems. IFAC-PapersOnLine, 48(29), 13–18.
[21]. Delgado, I., Sancristobal, E., Martin, S., & Robles-Gómez, A. (2023). Exploring IoT vulnerabilities in a comprehensive remote cybersecurity laboratory. Sensors, 23(22), 9279.
[22]. Demberger, A. (2022). Merck awarded $1.4 billion for NotPetya after 5 years of legal battle. Risk & Insurance. [News – retained only as illustrative of impact, not as a core technical citation]
[23]. Denning, T., Matsuoka, Y., & Kohno, T. (2010). Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In CHI ’10 Proceedings (pp. 1–10). ACM.
[24]. Dritsas, E., & Trigka, M. (2025). A survey on cybersecurity in IoT. Future Internet, 17(1), 30.
[25]. Feng, X. T., Zhu, X. G., Han, Q. L., Zhou, W., Wen, S., & Xiang, Y. (2023). Detecting vulnerability on IoT device firmware: A survey. *IEEE/CAA Journal of Automatica Sinica, 10*(1), 25–41.
[26]. Feodorova, V. A., Sayapina, L. V., Corbel, M. J., & Motin, V. L. (2014). Russian vaccines against especially dangerous bacterial pathogens. Emerging Microbes & Infections, 3(1), 1–17.
[27]. Formby, D., Rad, M., & Beyah, R. (2018). Lowering the barriers to industrial control system security with GRFICS. In 2018 USENIX Workshop on Advances in Security Education (ASE 18). USENIX Association.
[28]. Genge, B., Siaterlis, C., Fovino, I. N., & Masera, M. (2012). A cyber-physical experimentation environment for the security analysis of networked industrial control systems. Computers & Electrical Engineering, 38(5), 1146–1161.
[29]. Gómez, Á. L. P., Maimó, L. F., Celdrán, A. H., Clemente, F. J. G., Sarmiento, C. C., Masa, C. J. D. C., & Nistal, R. M. (2019). On the generation of anomaly detection datasets in industrial control systems. IEEE Access, 7, 177460–177473.

DOI: https://doi.org/10.67317/IJMSRT26JUL006

[30].Green, B., Lee, A., Antrobus, R., Roedig, U., Hutchison, D., & Rashid, A. (2017). Pains, gains and PLCs: Ten lessons from building an industrial control systems testbed for security research. In 10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17). USENIX Association.
[31].Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.
[32].Guttieres, D., Stewart, S., Wolfrum, J., & Springs, S. L. (2019). Cyberbiosecurity in advanced manufacturing models. Frontiers in Bioengineering and Biotechnology, 7, 210.
[33].Haber, M. J. (2020). Privileged account management implementation. In Privileged attack vectors: Building effective cyber-defense strategies to protect organizations (pp. 335–359). Apress.
[34].Haq, S. U., Singh, Y., Sharma, A., & Gupta, D. (2023). A survey on IoT & embedded device firmware security: architecture, extraction techniques, and vulnerability analysis frameworks. Discover Internet of Things, 3, 17.
[35].Hasan, R., Zawoad, S., Noor, S., Haque, M. M., & Burke, D. (2016). How secure is the healthcare network from insider attacks? An audit guideline for vulnerability analysis. In Proceedings of the International Computer Software and Applications Conference (pp. 417–422). IEEE Computer Society.
[36].Holdsworth, J., et al. (2017). Medical device vulnerability mitigation effort gap analysis taxonomy. Elsevier Smart Health.
[37].Iannone, E., Guadagni, R., Ferrucci, F., De Lucia, A., & Palomba, F. (2022). The secret life of software vulnerabilities: A large-scale empirical study. IEEE Transactions on Software Engineering.
[38].IBM. (2021). Cost of a data breach report 2021. IBM Security.
[39].Illumina. (2022). Sequencing platforms. https://www.illumina.com/systems/sequencing-platforms.html [Vendor source]
[40].Johnson, P., Lagerström, R., Ekstedt, M., & Franke, U. (2016). Can the common vulnerability scoring system be trusted? A Bayesian analysis. IEEE Transactions on Dependable and Secure Computing, 15(6), 1002–1015.
[41].Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411.
[42].Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. IEEE Computer, 50(7), 80–84.
[43].Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. Journal of Medical Systems, 41(8).
[44].LabWare. (2023). LabWare LIMS. https://www.labware.com/lims [Vendor source]
[45].Langer, S. G. (2017). Cyber-security issues in healthcare information technology. Journal of Digital Imaging, 30(1), 117–125.
[46].Li, M., Liu, Z., Li, X., & Liu, Y. (2019). Dynamic risk assessment in healthcare based on Bayesian approach. Reliability Engineering and System Safety, 189, 327–334.
[47].Li, S., Da Xu, L., & Zhao, S. (2015). The Internet of Things: A survey. Information Systems Frontiers, 17(2), 243–259.
[48].Liang, H., Pei, Y., Jia, X., Shen, W., & Zhang, J. (2018). Fuzzing: State of the art. IEEE Transactions on Reliability, 67(3), 1199–1218.
[49].Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., & Liu, Y. (2024). Dissecting zero trust: Research landscape and its implementation in IoT. Cybersecurity, 7, 20.
[50].Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. Technology and Health Care, 24(1), 1–9.
[51].Mantle, J. L., Rammohan, J., Romantseva, E. F., Welch, J. T., Kauffman, L. R., McCarthy, J., et al. (2019). Cyberbiosecurity for biopharmaceutical products. Frontiers in Bioengineering and Biotechnology, 7, 116.
[52].Marquez, G., Astudillo, H., & Taramasco, C. (2020). Security in telehealth systems from a software engineering viewpoint: A systematic mapping study. IEEE Access, 8, 10933–10950.
[53].Mathur, A. P., & Tippenhauer, N. O. (2016). SWaT: A water treatment testbed for research and training on ICS security. In 2016 International Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater) (pp. 31–36). IEEE.

DOI: https://doi.org/10.67317/IJMSRT26JUL006

[54].Morris, T., Vaughn, R., & Dandass, Y. S. (2011). A testbed for SCADA control system cybersecurity research and pedagogy. In Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research (pp. 27:1–27:1). ACM.
[55].Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586–602.
[56].Muench, M., Stijohann, J., Kargl, F., Francillon, A., & Balzarotti, D. (2018). What you corrupt is not what you crash: Challenges in fuzzing embedded devices. In Network and Distributed System Security Symposium (NDSS). ISOC.
[57].Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. Frontiers in Bioengineering and Biotechnology, 6, 39.
[58].Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. Frontiers in Bioengineering and Biotechnology, 6, 39.
[59].National Academies of Sciences, Engineering, and Medicine. (2020). Safeguarding the bioeconomy. National Academies Press.
[60].National Academies of Sciences, Engineering, and Medicine. (2020). Safeguarding the bioeconomy. National Academies Press.
[61].Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyberwarfare. Computers & Security, 31(4), 418–436.
[62].NIST. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology.
[63].Nurse, J. R. C., Erola, A., Agrafiotis, I., Goldsmith, M., & Creese, S. (2015). Smart insiders: Exploring the threat from insiders using the Internet of Things. In Proceedings of the 2015 Workshop on Secure Internet of Things (SIoT) (pp. 5–14). IEEE.
[64].OWASP. (2016). Top IoT vulnerabilities. OWASP Foundation.
[65].Papp, D., Ma, Z., & Buttyan, L. (2015). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In 2015 13th Annual Conference on Privacy, Security and Trust (PST) (pp. 145–152). IEEE.
[66].Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: From naïve trust to risk awareness. Trends in Biotechnology, 36(12), 4–10.
[67].Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: From naïve trust to risk awareness. Trends in Biotechnology, 36(12), 4–10.
[68].Peng, R. D. (2011). Reproducible research in computational science. Science, 334(6060), 1226–1227.
[69].Perkel, J. M. (2017). The Internet of Things comes to the lab. Nature, 542(7639), 125–126.
[70].Pycroft, L., et al. (2016). Brainjacking: Implant security issues in invasive neuromodulation. World Neurosurgery, 92, 454–462.
[71].Quinn, S., Ivy, N., Barrett, M., Witte, G., & Gardner, R. (2021). Identifying and estimating cybersecurity risk for enterprise risk management (NIST Special Publication). National Institute of Standards and Technology.
[72].Rajmohan, T., Nguyen, P. H., & Ferry, N. (2022). A decade of research on patterns and architectures for IoT security. Cybersecurity, 5, 2.
[73].Rakas, S. V. B., Stojanović, M. D., & Marković-Petrović, J. D. (2020). A review of research work on network-based SCADA intrusion detection systems. IEEE Access, 8, 93083–93108.
[74].Reed, J. C., & Dunaway, N. (2019). Cyberbiosecurity implications for the laboratory of the future. Frontiers in Bioengineering and Biotechnology, 7, 182.
[75].Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things. Computer, 44(9), 51–58.
[76].Ross, R. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30, Revision 1). National Institute of Standards and Technology.
[77].Salayma, M. (2024). Risk and threat mitigation techniques in Internet of Things (IoT) environments: A survey. Frontiers in the Internet of Things, 2, 1306018.
[78].Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.
[79].Srivastava, R. (2006). An information systems security risk assessment model under Dempster-Shafer theory of belief functions. Journal of Management Information Systems, 22(4), 109–142.

DOI: https://doi.org/10.67317/IJMSRT26JUL006

[80]. Stodden, V., Seiler, J., & Ma, Z. (2018). An empirical analysis of journal policy effectiveness for computational reproducibility. Proceedings of the National Academy of Sciences, 115(11), 2584–2589.
[81]. Tervoort, T., De Oliveira, M. T., Pieters, W., Van Gelder, P., Olabarriaga, S. D., & Marquering, H. (2020). Solutions for mitigating cybersecurity risks caused by legacy software in medical devices: A scoping review. IEEE Access, 8, 84352–84361.
[82]. Thermo Fisher Scientific. (2021a). Smart and connected Herasafe and Maxisafe 2030i biological safety cabinets. Thermo Fisher. [Vendor source]
[83]. Thermo Fisher Scientific. (2021b). Chromeleon CDS. Thermo Fisher. [Vendor source]
[84]. Voas, J., & Hurlburt, G. (2015). Third-party software's trust quagmire. Computer, 48(12), 80–87.
[85]. Wang, W., Harrou, F., Bouyeddou, B., Senouci, S.-M., & Sun, Y. (2022). Cyber-attacks detection in industrial systems using artificial intelligence-driven methods. International Journal of Critical Infrastructure Protection, 38, 100542.
[86]. Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30.
[87]. WHO (World Health Organization). (2020). Laboratory biosafety manual (4th ed.). WHO.
[88]. Williams, T. J. (1994). The Purdue enterprise reference architecture. Computers in Industry, 24(2-3), 141–158.
[89]. Xiong, W., & Lagerström, R. (2019). Threat modeling – A systematic literature review. Computers & Security, 84, 53–69.
[90]. Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2021). Cyber security threat modeling based on the MITRE Enterprise ATT&CK matrix. Software and Systems Modeling, 1–21.
[91]. Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices – A review. IEEE Communications Surveys & Tutorials, 21(4), 3723–3768.
[92]. Zhou, X., Wang, P., Zhou, L., Xun, P., & Lu, K. (2023). A survey of the security analysis of embedded devices. Sensors, 23, 9221.
[93]. Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2013). Privacy in the Internet of Things: Threats and challenges. Security and Communication Networks, 7(12), 2728–2742.

DOI: https://doi.org/10.67317/IJMSRT26JUL006