LabLynx

Guide to Lab Security with a Laboratory Information Management System

Author: Chris Casper October 2022

Cybercrime is so pervasive that new data breaches seem to scatter personal information across the internet every day. An attack can hit any organization at any time. Laboratories face a particular challenge as they balance security with collaboration. Should hackers breach a laboratory's systems, the resulting data loss can have severe financial, legal, and reputational consequences. This guide provides an overview of the cybersecurity landscape and explains how a laboratory information management system (LIMS) can:

- Help close security gaps,
- Control access to data and systems more granularly,
- Protect laboratory data and reinforce data integrity, and
- Support cybersecurity incident response and recovery efforts.

We will illustrate how a LIMS improves lab security by describing the security features in LabLynx's software solutions. Clients worldwide use our informatics solutions to improve laboratory productivity while protecting lab data within a secure cloud platform.

1. An evolving laboratory security landscape

Security is always a concern for laboratory managers, but the security landscape's rapid changes make many lab security policies obsolete shortly after being introduced. Effective security no longer solely protects networks from external threats: risks now come from every direction. A careless click on an email will breach a lab's defenses from within. Consider these recent examples:

Eurofins Scientific provides pharmaceutical, food, and environmental testing services and operates more than eight hundred laboratories around the world. Its security team seemed to have everything in order, including using an enterprise-grade malware scanning service. In June 2019, however, a brief window opened between the appearance of a new type of malware and the scanning service's fix.[1] The new malware slipped through unrecognized and spread through Eurofins' networks. Shutting everything down contained the breach but also took many labs offline. Before the attack, the United Kingdom's police force sent half of its forensic samples to Eurofins laboratories for testing. The shutdown led to a 20,000-sample backlog for a single customer that took four months to clear.[2]

In October 2020, an employee of the University of Vermont Medical Center (UVMC) used a hospital laptop away from work to check their personal email.[3] Opening a malicious email attachment led to a ransomware attack that kept UVMC's network down for three weeks.[4] This attack did not directly target the hospital's anatomic pathology lab, but its impact was immediate. Dependent upon UVMC's infrastructure, the lab instantly lost access to its LIMS and patient records. The lab had to implement manual analytical and reporting processes almost overnight without compromising patient safety.[5]

Laboratories can also be vulnerable to attacks that never touch their systems. American Medical Collection Agency (AMCA) once provided billing services for America's largest medical laboratories. A breach went undetected for nearly a year until security researchers saw patient credit card data for sale on the dark web.[6] Although the researchers notified AMCA, the company did not publicly disclose the breach until after the 60-day notification window required by patient privacy regulations.[7] Initially thought to impact seven million patients, the full scope now exceeds 20 million people. Many AMCA

clients, including Quest Laboratories and LabCorp, have been drawn into the resulting class-action lawsuits.[8]

Whether targeted directly or impacted by failures at a parent organization or third-party vendor, laboratories are particularly vulnerable to cyberattacks. Labs often possess sensitive information, from patient records to intellectual property. Security practices such as simple password controls may have worked before the internet connected lab networks to the outside world. Today's rapidly-changing threat landscape makes adopting security best practices imperative.

1.1 Expanding cyberthreats

You only have to read the headlines to see how common cybersecurity attacks have become. The non-profit Identity Theft Resource Center (ITRC) reported [9] that in 2021:

- Data breaches increased 68 percent over 2020,
- Sensitive information such as Social Security numbers were involved in 83 percent of breaches,
- Ransomware-related breaches doubled in 2021 after doubling in 2020, and
- Breaches at manufacturers and utilities increased 217 percent over 2020.

While headlines focus on attacks targeting major corporations, nobody is immune. A joint report from the FBI and other cybersecurity agencies observed that ransomware attacks in 2021 shifted focus from large, high-value targets to mid-sized organizations.[10] Surveying middle-market companies in the US and UK, the US Chamber of Commerce found that 22 percent of respondents had experienced a security breach in the past year.[11]

What makes these attacks so effective is hackers' ability to go undetected. The seven months between the AMCA security breach and its detection is not unusual. On average, it takes organizations 287 days to detect and contain a security breach.[12] During that extended window, hackers have plenty of time to conduct surveillance, exfiltrate data, and install ransomware.

1.1.1 People are the weakest link

Although it is tempting to view security breaches as technological failures, human error causes most successful attacks. Hackers use phishing and other social engineering techniques to trick people into compromising network security.

IBM's cybersecurity service reported that, at 41 percent of all incidents it encountered in 2021, phishing became the top vector for security breaches.[13] Phishing attacks combining emails and phone calls were more than three times as effective as emails alone.

1.2 Technology risks

Of course, technology remains a weak point in network security. Cybercriminals exploit vulnerabilities in network hardware to break through defenses. Technologies like Remote Desktop Protocol (RDP) and virtual private networks (VPNs) are designed to let people onto a network, making them common vectors for attacks.[14, 15, 16] Adding to this problem, IT departments do not promptly update vulnerable network hardware, leaving security holes in place for months.

Another contributor to technological risks is the rising popularity—by businesses and end-users alike—of bring your own device (BYOD) policies. End-users prefer the convenience of using a personal smartphone to access company email and other work applications. Companies improve their financials when they stop buying and maintaining managed devices. While both benefits are real, they come with security tradeoffs[17]:

- Only 41 percent of businesses control file sharing through mobile messaging apps, and less than 10 percent of companies can detect mobile messaging-distributed malware.
- Despite these tradeoffs, more than two-thirds of employees use personal devices for work.

Device security is also a growing issue within laboratories. Network-connected industrial internet of things (IIoT) devices such as environmental sensors and instruments can improve the quality of laboratory testing. Still, labs must pay careful attention to the security implications of IIoT devices. Researchers in 2020, for example, discovered vulnerabilities in widely-used network protocols.[18] These weaknesses would let hackers take control of devices or access sensitive information. By one estimate, nearly 53,000 models of medical devices had these vulnerabilities. Changes to an instrument's software could require disruptive revalidation[19], making a security update a complicated decision.

1.3 New ways of working

New technologies such as cloud computing and BYOD create new ways for people to work. Companies experimented with hybrid work policies before 2020, but pandemic restrictions made work-from-home the only way to survive. Many labs discovered that adjusting to this hybrid workforce improved productivity. A Department of Justice-sponsored study of forensic laboratories, for example, found that "…the implementation of these features has benefited labs because workflows are now more standardized and streamlined. The result of these efforts will provide lasting improvements in efficiency." [20]

Another long-running workforce trend is the adoption of blended workforces comprising:

- Full-time and part-time employees,
- Independent contractors and consultants,
- Temporary freelancers, and
- Other individual free agents.

Blended workforces give organizations more flexibility to cover staffing shortages, meet short-term demand, or add specialized skills.

In 2019 and 2020, the Harvard Business School surveyed American business leaders about the changing workforce. Three out of five respondents said they expected the core workforce to shrink as freelancers and contractors played larger roles in their business.[21]

As with technological change, the benefits of an evolving workforce have security implications. Employees and non-employees need access to laboratory systems in the lab and remotely. Some may use laboratory-owned devices in one context and personal devices in another. Security policies must adjust to this nebulous population, clearly defining who may access which resources, with which devices, and under what contexts.

1.4 Third-party risks

Another force blurring the boundaries of security defenses is the growing reliance on collaboration, outsourcing, and third-party integrations. Outsourcing back-office activities, such as recruiting or billing, lets a lab focus on its core analytical practice. At the same time, bringing in a contract laboratory can improve productivity in many aspects of laboratory operations.[22]

Modern outsourcing requires a degree of network integration that increases security risks. Linking a lab's network to another company's makes the boundary between the two less distinct. A third party's security policies now affect the laboratory's security posture.

Collaboration in the laboratory setting adds extra complexity to third-party risk. Security policies and IT bureaucracy make it harder for researchers to share information with collaborators inside and outside the lab. To work more effectively, they will share documents or spreadsheets through email or messaging applications.[23] The further this information spreads beyond centralized systems, the less control labs have over proprietary and confidential information.

2. Towards risk-based security frameworks

As the magnitude and frequency of cyberattacks grow, Congress and government agencies are introducing cybersecurity regulations that will affect laboratories. Promoting new and updated security frameworks should improve performance in transparency, privacy, and security practice across the economy. However, organizations of all sizes will need to prepare for compliance with such frameworks.

2.1 More transparency when breaches occur

Cyberattacks that capture headlines are the tip of the iceberg. Many more attacks go unreported, making criminal investigations more difficult and allowing hackers to go unchecked. To better understand the scope of cyber threats facing the American economy, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA requires any "covered entity" considered part of the country's critical infrastructure to notify the Cybersecurity Infrastructure Security Agency (CISA) within 72 hours of discovering an incident and within 24 hours of making a ransomware payment. By early 2024, when CIRCIA goes into effect, CISA must define what organizations are subject to the new law. Critical infrastructure, however, covers a significant slice of the US economy, including:

- Chemical plants,
- Commercial facilities such as shopping malls and hotels,
- Communications centers,
- Critical manufacturing centers,
- Dams,
- Defense sites,
- Emergency services,
- Energy infrastructure,
- Financial services,
- Food and agriculture entities,
- Government facilities,

- Healthcare and public health facilities,
- Information technology,
- Nuclear infrastructure,
- Transportation infrastructure, and
- Water and wastewater treatment centers.

Federal agencies have not waited for CIRCIA's passage and two-year rule-making process. Since 2021, the Transportation Security Administration (TSA) has issued security directives to pipeline operators and surface transportation companies to improve their cybersecurity resilience.[24, 25] Among other things, these directives require companies in these critical infrastructure sectors to report cybersecurity incidents to CISA, within 24 hours in some cases.

Publicly-traded companies will also have tighter reporting requirements if proposed rules from the US Security and Exchange Commission (SEC) go into effect.[26] Under current rules, cybersecurity incident disclosure practices are inconsistent. The SEC's proposal would require companies to file a disclosure within four business days of a material cybersecurity breach.

2.2 Protecting consumer privacy

Laboratories that provide testing services to the public or receive consumer's personal information (PI) from their clients are increasingly subject to data privacy regulations. The United States does not have a national law protecting consumer's PI, but several states have introduced privacy protection regulations. For example, the California Consumer Privacy Act (CCPA) is largely modeled on Europe's General Data Protection Regulation (GDPR). Companies doing business in California must honor California consumers' privacy rights, including:

- The right to know what information a business collects and shares,
- The right to delete the PI businesses collect,
- The right to opt out from the company's sale of their PI, and
- The right to non-discrimination for using their privacy rights.

Under the CCPA, any business that does not sufficiently protect consumer PI faces stiff penalties and civil suits. Changes going into effect in 2023 will require stricter security measures in third-party business relationships involving consumer PI.

Federal privacy regulations may soon pre-empt the patchwork of state laws. At the time of writing, the American Data Privacy and Protection Act (ADPPA) had passed a House committee with almost unanimous bipartisan support.[27] Besides defining rights similar to the CCPA's, the bill would limit what kind of PI organizations could collect and require express consent before sharing PI with others.

2.3 Risk-based cybersecurity frameworks

Many organizations are already ahead of any pending regulation. Today's cyber risks give them little choice. Some must comply with industry-specific security frameworks such as:

- System and Organization Controls (SOC) for information service organizations,

- HIPAA and HITECH for clinical labs and other healthcare organizations,
- Federal Information Security Management Act (FISMA) for federal agencies and their vendors, and
- North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) for electric utilities and other power companies.

Although used by specific industries, many of these frameworks base their recommendations on work done by the National Institute of Standards and Technology (NIST). NIST's Cybersecurity Framework [28] and Special Publication 800-53 *Security and Privacy Controls for Information Systems and Organizations* [29] layout standards, guidelines, and best practices that organizations can follow to improve their cybersecurity processes.

NIST's frameworks define five core functions that organizations perform to bring their cybersecurity risks under control:

- **Identify**: Understand what information assets need protection, which users and devices may access the information, and what threats and vulnerabilities increase security risks.
- **Protect**: Implement the controls required to protect critical systems and sensitive data.
- **Detect**: Continuously monitor for cybersecurity incidents.
- **Respond**: Create an incident response plan to prepare for the most likely and most impactful events.
- **Recover**: Implement backup and recovery plans to maintain business continuity while minimizing an event's impact.

NIST advocates a continuous approach to identifying and mitigating security risks based on the likelihood of an event and the event's potential impact. The frameworks do not specify how to address this risk assessment, leaving decisions to organizations based on their risk tolerance and risk management policies.

3. How a LIMS improves laboratory security

A modern LIMS unifies data storage and lab processes within a single system, digitizes and automates information transfers within the lab, and moves laboratory informatics into the cloud. Each capability significantly improves laboratory information security.

3.1 Single source of truth

By consolidating laboratory data into a central repository, a LIMS makes sensitive information easier to protect. Centralization allows for the more consistent application of security measures such as encryption, access control, and backups. This control is much more difficult when data is scattered across databases and spreadsheets.

A LIMS also eliminates risks associated with data duplication. Staffers need spreadsheets and other digital files on their laptops when they travel or work from home. These files are also easy to share with collaborators through email or messaging. That convenience, however, raises the risk that stolen or compromised laptops will let sensitive data fall into the wrong hands. Requiring everyone in the lab to

access the data they need through the LIMS reduces the risk of data loss.

Establishing a LIMS as a laboratory's single source of truth also improves data integrity. Records are never overwritten. Instead, changes enter the LIMS as new records. The LIMS will log every change into an audit trail with the user ID of whoever made the change, a timestamp, and what was changed.

3.2 Digitalization, automation, and integration

Typically, laboratories rely on manual data transfer processes to get information from one part of the lab to another. However, paper forms can be removed from a lab or recovered from recycling bins. Likewise, thumb drives used to transfer test results from instruments can be lost or stolen.

Converting manual processes into automated digital workflows within a LIMS eliminates paperwork and removable media that can so easily wander from the lab. LIMS integrations further tighten security by handling data transfers between the LIMS, instruments, analytical software, and enterprise systems.

Once information flows within the lab are coordinated through the LIMS, laboratories can exert greater control over user access. Anybody can see paperwork or pick up a thumb drive. Accessing the same information in a LIMS requires specific permission. As we will see in Section 4.1, laboratories can create granular access control rules that limit who may access what information. Role-based access controls limit LIMS access to the features and data people need to do their jobs. For example, research scientists will have broader access than a mass spectrometry technician.

Digitizing information flows in a LIMS not only protects laboratory data, but it also improves the lab's data integrity. Laboratory errors decline significantly by removing opportunities for transcription and other human errors. Combined with standards-based LIMS workflows and easier automation, a LIMS makes laboratory testing more consistent and accurate.

3.3 The cloud advantage

Software-as-a-service (SaaS) providers offer subscription-based business applications that run in the cloud. The overall SaaS market is growing by 18 percent annually, with most organizations using at least one SaaS solution.[30] Market research firm Gartner forecasts by 2026, nearly half of enterprise IT budgets will be spent on the cloud.[31]

This widespread adoption could not happen if IT decision-makers had significant concerns about SaaS security. In fact, cloud-based services offer several security advantages over applications running on a company's in-house servers. SaaS service providers can:

- Invest in better security technologies, such as sophisticated automation tools to monitor, identify, and mitigate security threats;
- Devote more resources to software security by, for example, hiring more security administrators than small or mid-sized organizations can afford;
- Provide resiliency by running data centers in different locations, so outages in one region do not disrupt their customers' operations; and
- Support data recovery by performing regular automated backups for recovery from cyberattacks.

Using the cloud does not remove all security responsibilities from a SaaS customer, however. Organizations must protect their networks, users, and devices just like before. They must also implement access control policies that prevent unauthorized access to the sensitive information contained in the SaaS application.

4. Securing laboratory information with LabLynx LIMS software

To see how a modern cloud-based LIMS improves laboratory security, we will discuss common security practices and their implementation in a LabLynx LIMS.

4.1 Access control

Just as keys and identity cards control physical access to laboratory facilities, access control features in the LIMS ensure only authorized personnel can access systems and data.

4.1.1 Identity verification

Verifying that the people requesting access are who they claim to be is the first step in access control. Passwords are a necessary first layer of defense, but they have well-known security weaknesses:

- Short, easy-to-remember passwords are easy to hack.
- Long, complex passwords are hard to remember.
- People share and recycle passwords, making attacks easier.
- Password databases are common targets in cyberattacks.
- Hackers have databases of stolen passwords they can use in an attack.

Adding more layers to identity verification makes identity theft more onerous. This approach is called multi-factor authentication (MFA) and relies on the difficulty of simultaneously compromising multiple layers. Authentication factors fall into one of three categories:

1. **Something you know**: If you are the only one who knows a password, nobody else can use it.
2. **Something you have**: An object like a USB key fob that is always in your possession prevents someone in another country from pretending to be you.
3. **Something you are**: Fingerprint readers, face recognition, and other biometric technologies recognize your unique physical characteristics.

Single sign-on (SSO) provides another layer of security by relying on a third party to verify a user's identity. Organizations use SSO to minimize the PI they collect; if you never possess a user's password, you can never lose it. Most people experience SSO when using their Facebook or other social media account to log into web applications. IT departments use a similar concept called identity and access management (IAM) to let personnel use a single password to access every business application.

Identity verification in a LabLynx LIMS can be as straightforward or sophisticated as clients need it to be. The default password management features let laboratories define policies, including:

- Minimum password length,
- Password expiration periods,

- Password reuse limits, and
- Maximum number of login attempts.

LabLynx further protects the integrity of a lab's user accounts by fully encrypting the password database.

LabLynx LIMS solutions can also support social media SSO. For example, a radiology laboratory can minimize the patient PI it collects by letting patients use their Facebook accounts to log into the lab's web portal.

When labs need more advanced verification techniques, LabLynx integrates with enterprise IAM systems through the OpenSocial API and SAML protocols. Working with LabLynx engineers, a laboratory's IT department can add the lab's LIMS solution to the organization's SSO system.

4.1.2 Least-privileged access

With their identity confirmed, users should only get access to those features and datasets they need to do their work. Often called the principle of least privilege, this approach limits the damage hackers can do with stolen credentials. Need-to-know access also limits the data that rogue employees can extract from the LIMS.

Besides access scope, the principle of least privilege also constrains access duration. Successfully logging in once should not give users permanent access to the LIMS. Sessions should automatically terminate after a certain amount of time has elapsed or after a period of inactivity.

When implementing a LabLynx LIMS solution, clients work with their LabLynx engineers to configure authorization policies. Group profiles combine access privileges shared by certain employees. Besides limiting menu options and screen availability, these profiles can control access at a granular level. Labs can decide whether a profile can read or edit each data field or control. Your lab's LIMS administrator will assign a group profile to a new user's account, automatically granting that user the profile's access privileges. For example, analysts may access report creation screens, but only supervisors may access report approval screens, or administrative staff may access customer management and invoicing screens but may not access testing workflows.

Besides assigning user profiles, a lab's LIMS administrator can also set session timeouts to force re-verification after periods of inactivity.

4.1.3 Third-party access

Laboratories must interact with the outside world despite the security risks. Clients need to be able to order tests, receive results, and pay invoices. Research collaborators need access to the data in the LIMS. In addition, the lab needs to exchange data with enterprise systems and external contract laboratories.

LabLynx LIMS solutions have several ways to provide external access securely. Web portals, for example, let businesses or consumers interact with your LIMS without getting direct LIMS access. These secure web pages display and collect information without exposing the LIMS to the public internet.

Labs can use the profile feature to grant research collaborators, contractors, and others direct—but limited—access to the LIMS. For example, an instrument vendor's technicians may need access to instrument management screens when visiting the lab.

The organization's IT department and LabLynx engineers work together to integrate your LIMS with enterprise resource planning (ERP), electronic health record (EHR), and other corporate systems outside the laboratory. Together, they ensure that information transfers are handled correctly and in compliance with the organization's security policies.

4.2 Data protection and data integrity

Good security practice calls for organizations to assume hackers can penetrate their defenses anytime. Given how long it takes to discover a breach, the best security practice assumes a breach is already in progress. Laboratories rely on several LIMS features to protect data during the breach and speed recovery afterward.

4.2.1 Encrypting LIMS data

Organizations encrypt databases and other sensitive information to ensure that any stolen information is useless. Modern encryption algorithms scramble data so thoroughly that it is impossible to reassemble without the proper key. Encrypting sensitive data may sound like a common-sense precaution, but many of the worst cases of data theft happened because companies never took that simple step.

In the case of the AMCA data breach discussed prior, hackers could sell stolen credit card information because AMCA did not adequately encrypt patient information.

Besides the data protection benefits, encryption reduces an organization's liabilities in the event of a breach. HIPAA's Breach Notification Rule[32] only requires notifications when stolen personal health information "has not been rendered unusable, unreadable, or indecipherable to unauthorized persons." Similarly, California's privacy regulations do not let consumers sue companies that adequately encrypt PI.

A state-of-the-art data center, certified to the highest SSAE SOC 2 standards, hosts LabLynx's cloud infrastructure. All data stored in the cloud is fully encrypted, as is data flowing within the infrastructure.

Access to your LabLynx LIMS occurs through browser interfaces protected by Hypertext Transfer Protocol Secure (HTTPS). All traffic between the browser and your LabLynx LIMS solution in the cloud passes through secure tunnels encrypted with Transport Layer Security (TLS). Should users access the LIMS from their hotel Wi-Fi, for example, the data they access will be unusable to anyone intercepting their Wi-Fi signal.

When you integrate your laboratory's instruments and other systems with your LabLynx LIMS, data transfers flow through encrypted TLS tunnels. Should hackers compromise your network, any data they intercept will be indecipherable.

4.3 Monitoring, responding, and recovering

Quickly identifying and responding to a breach minimizes the time hackers have to steal data or damage systems. That responsibility falls mainly on the IT department's security teams. A cloud-based LIMS can help maintain laboratory operations during a security event and simplify recovery.

4.3.1 Laboratory continuity and incident response

UVMC's anatomic pathology lab had to develop its response plan in the security breach's aftermath. Had the lab adopted a cloud-based LIMS instead of one running on the hospital's servers, they would have had less trouble staying operational. Their LIMS would have lost access to the hospital's patient health records, but features like sample tracking, data analysis, and report generation still would have been available.

Security frameworks call for organizations to develop incident response plans. A LabLynx LIMS' easy configurability can help labs prepare for and minimize the effects of security incidents. Without the help of a LabLynx engineer, clients can create worst-case workflows that let the lab continue operations when their networks are down.

Special "break-glass" profiles can give specific users broader access to the LIMS, letting them activate emergency workflows and collect activity logs for IT security administrators.

4.3.2 Data integrity and recovery

While IT departments track down the source and scope of a security breach, others must determine whether and to what degree the attack has compromised data. This forensic investigation is crucial for laboratories where data integrity often matters as much as, if not more than, data security. Corrupt data can delay the completion of projects or void years of research. In either case, the reputational damage could be irreversible.

Your LabLynx LIMS tracks user access and records the changes they make. Querying tools will help you extract these audit logs for the IT department's incident response team. Analyzing these logs will determine whether data was accessed or altered.

LabLynx's cloud platform also performs hourly, daily, and weekly backups of your LIMS to assist with data recovery. If a significant security breach occurs, your LIMS administrator can contact LabLynx support to request a rollback to the last safe backup.

5. How to deploy a secure LabLynx LIMS solution

Treat security as an afterthought in the LIMS acquisition process, and you will spend more time and money trying to patch security holes. Security must be front and center from the moment you decide your lab needs a new LIMS.

The vendors you consider must comply with company security policies, industry security frameworks, and data protection regulations. Include security questions in your request for proposals (RFPs) and objectively evaluate each vendor's responses. During contract negotiations, set expectations and clarify

the shared responsibilities between your lab and your LIMS vendor.

5.1 Planning

The planning stage is when you and your vendor will map out the details of what it takes to get your new LIMS working. In the case of a LabLynx LIMS, security planning maps your organization's security policies with each LIMS security feature. LabLynx engineers work with you to identify the technical requirements for security capabilities such as:

- Integration with enterprise SSO,
- Configuration of secure web portals, and
- Development of granular permissions in group profiles.

In addition, LabLynx's compliance engineers help you identify the security configurations needed to support your regulatory or accreditation compliance programs.

5.2 Integration and implementation

LabLynx works with your IT department to securely integrate your new LIMS with laboratory and enterprise systems. We assign every member of your lab's staff to profiles that grant least-privileged access to laboratory data and workflows. Once the initial setup is complete, we conduct end-to-end testing of your LIMS and its security features.

5.3 Validation

LabLynx LIMS solutions are integral to our clients' compliance efforts towards ISO/IEC 17025, 21 CFR Part 11, HIPAA, or AASHTO. Before your new LIMS goes live, LabLynx's compliance engineers validate compliance with any accreditations or frameworks applicable to your lab. We can also apply this compliance validation process to specific security frameworks relevant to your lab's industry.

5.4 Training and support

Given how vulnerable laboratory security is to the human element, our training sessions review all LIMS security features that apply to your staff. We record these training sessions and make them available for future reference through the LabLynx LIMS help system.

Should your organization discover a security breach, our rapid-response emergency support team is ready to help lock down your LIMS and assist you with data recovery.

6. Conclusion

Laboratory security concerns have changed dramatically in the face of pervasive threats and the fading of network boundaries. Security must be everyone's concern, not just the IT department's. Protecting laboratory data must be a continuous process rather than a discrete, one-time event. Integrating a LabLynx LIMS into your lab's operations can dramatically improve lab security by:

- Centralizing all data storage and workflows,
- Digitalizing all information transfers, and
- Securing data in the cloud.

Your LabLynx LIMS makes it easier to control access to data and laboratory systems and protect information shared within the lab without sacrificing productivity or collaboration.
Contact us today to learn more about enhancing laboratory security with a LabLynx LIMS solution.

References

[1] "Update on the cyber-attack announced on June 3, 2019," Eurofins Scientific, June 10, 2019, https://www.eurofins.com/biopharma-services/discovery/eurofins-3-june-2019-press-release/.
[2] Shaw, D. "Eurofins Scientific: Cyber-attack leads to backlog of 20,000 forensic samples," BBC News, August 16, 2019, https://www.bbc.com/news/uk-49361260.
[3] Amato, D. "Lessons learned from cyberattack on UVM Health Network," WCAX, July 29, 2021, https://www.wcax.com/2021/07/29/lessons-learned-cyberattack-uvm-health-network/.
[4] "Statement from UVM Health Network on Cyberattack," The University of Vermont Health Network, December 22, 2020, https://www.uvmhealth.org/news/uvmhn/statement-uvm-health-network-cyberattack.
[5] Paxton, A. "AP lab maps its cyberattack recovery," CAP Today 35, 8 (2021): 1, accessed August 18, 2022, https://www.captodayonline.com/ap-lab-maps-its-cyberattack-recovery/.
[6] Landi, H. "Clinical Pathology Laboratories the latest company impacted by massive AMCA breach," Fierce Healthcare, July 17, 2019, https://www.fiercehealthcare.com/tech/clinical-pathology-laboratories-reports-2-2m-patients-affected-by-amca-breach.
[7] Lindsey, N. "AMCA Healthcare Data Breach Could Set a New Precedent for Health IT Security," CPO Magazine, June 26, 2019, https://www.cpomagazine.com/cyber-security/amca-healthcare-data-breach-could-set-a-new-precedent-for-health-it-security/.
[8] Davis, J. "Quest, LabCorp, AMCA Face Breach Lawsuits, State Investigations," Health IT Security, June 11, 2019, https://healthitsecurity.com/news/quest-labcorp-amca-face-hit-by-breach-lawsuits-state-investigations.
[9] "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," ID Theft Center, January 24, 2022, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.
[10] "Joint Cybersecurity Advisory: 2021 Trends Show Increased Globalized Threat of Ransomware" United States Cybersecurity and Infrastructure Security Agency, last modified February 10, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.
[11] "2022 Cybersecurity Special Report," United States Chamber of Commerce, June 22, 2022, https://www.uschamber.com/security/cybersecurity/2022-cybersecurity-special-report.
[12] "IBM Report: Cost of a Data Breach Hits Record High During Pandemic," IBM Security, July 28, 2021, https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic.
[13] "X-Force Threat Intelligence Index 2022," IBM Corporation, February 2022, https://www.ibm.com/downloads/cas/ADLMYLAZ.
[14] Vijaian, J. "Attackers Heavily Targeting VPN Vulnerabilities," Dark Reading, April 21, 2021, https://www.darkreading.com/perimeter/attackers-heavily-targeting-vpn-vulnerabilities-/d/d-id/1340770.

[15] Schwartz, S. “VPN exploitation rose in 2020, organizations slow to patch critical flaws,” Cybersecurity Dive, June 18, 2021, https://www.cybersecuritydive.com/news/trustwave-network-security-remote-access/602044/.
[16] Vaas, L. “Keep Attackers Out of VPNs: Feds Offer Guidance,” Threatpost, September 29, 2021, https://threatpost.com/vpns-nsa-cisa-guidance/175150/.
[17] Harr, P. “Find the balance between security and privacy in a BYOD world,” Security, September 16, 2021, https://www.securitymagazine.com/articles/96102-find-the-balance-between-security-and-privacy-in-a-byod-world.
[18] Cimpanu, C. “Ripple20 vulnerabilities will haunt the IoT landscape for years to come,”ZDNet, June 16, 2020, https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come/.
[19] Dutton, G. “Protecting Your Lab from Cybersecurity Threats,” Lab Manager, October 5, 2020, https://www.labmanager.com/big-picture/data-integrity-security/protecting-your-lab-from-cybersecurity-threats-23970.
[20] Ramanathan, S., Satcher, R., and Shute, R. . Forensic Technology Center of Excellence, “Leveraging Laboratory Information Management Systems (LIMS) to Maintain Business Continuity During the COVID-19 Pandemic,” U.S. Department of Justice, National Institute of Justice, Office of Investigative and Forensic Sciences, January 2021, https://nij.ojp.gov/library/publications/leveraging-laboratory-information-management-systems-lims-maintain-continuity.
[21] Fuller, J., Raman, M., Bailey A., Vaduganathan N., et al “Building the on-demand workforce,” Published by Harvard Business School and BCG, November 2020, https://www.hbs.edu/managing-the-future-of-work/Documents/Building_The_On-Demand_Workforce.pdf.
[22] Muenz, R. “What Laboratory Services Can You Outsource?” Lab Manager, October 29, 2021, https://www.labmanager.com/big-picture/outsourcing-lab-services/what-laboratory-services-can-you-outsource-26850.
[23] “Data security in a collaborative environment,” Scientific Computing World, February 16, 2016, https://www.scientific-computing.com/feature/data-security-collaborative-environment.
[24] “DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators,” United States Department of Homeland Security, July 20, 2021, https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.
[25] “DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators,” United States Department of Homeland Security, December 2, 2021, https://www.dhs.gov/news/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation-owners-and.
[26] “SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies,” United States Security and Exchange Commission, March 9, 2022, https://www.sec.gov/news/press-release/2022-39.
[27] Kerry, C. “Federal privacy negotiators should accept victory gracefully,” The Brookings Institution, August 12, 2022, https://www.brookings.edu/blog/techtank/2022/08/12/federal-privacy-negotiators-should-accept-victory-gracefully/.
[28] Barrett, M. “Framework for Improving Critical Infrastructure Cybersecurity Version 1.1”, United States National Institute of Standards and Technology, April 16, 2018 https://doi.org/10.6028/NIST.CSWP.04162018.
[29] “SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations,” United States National Institute of Standards and Technology, September 2020, Revised December 10, 2020, https://doi.org/10.6028/NIST.SP.800-53r5.

[30] Shiff, L., Kidd C. “The State of SaaS in 2022: Growth Trends & Statistics,” BMC Software, September 17, 2021, https://www.bmc.com/blogs/saas-growth-trends/.
[31] “Gartner Says Four Trends Are Shaping the Future of Public Cloud,” Gartner, August 2, 2021, https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud.
[32] “Breach Notification Rule,” United States Department of Health and Human Services, accessed August 17, 2022, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.