Achiever LIMS

Make every sample matter

How a LIMS Can Support Cybersecurity: A White Paper for Laboratory Managers

Within all laboratory's handling human samples, there is a fundamental duty to protect patient confidentiality. There are also strong practical and financial reasons for protecting the data and systems in all types of laboratories including those involved with the food, agricultural and environmental sectors.

Fundamentally, cybersecurity is about defending digital systems, networks, programmes and data from unauthorised access and cyberattacks. These attacks can lead to exposure of confidential records and to theft, loss or corruption of sensitive and valuable data. At the same time, they may put critical systems out of action.

This white paper, aimed at laboratory managers and other professionals involved in managing related data, will set out the role of a laboratory information management system (LIMS) in strengthening cybersecurity. We will look at how LIMS features, together with surrounding practices, tools and services, can be used to prevent cybersecurity breaches.

Training and Awareness

The first step toward stronger cybersecurity is to increase awareness of cyber threats, the damage they can do, and how they can be countered. This is not a topic that should be left to IT people alone. It should be understood by all, including LIMS users and anyone with access to any of your organisation's business and communication systems.

Our white paper is an advisory resource which you can share with other staff. You may wish to highlight specific areas and concerns to them. Similarly, you can build up your understanding via other sources of information, and then direct colleagues accordingly. Links to two particularly helpful online resources are given below.

NHS Digital

https://digital.nhs.uk/cyber

National Cyber Security Centre (NCSC)

https://www.ncsc.gov.uk

NHS Digital is a great source of intelligence on emerging threats, concerns and best practices. Another resource is the National Cyber Security Centre (NCSC), a government agency whose website addresses users at all levels. These range from personal and home users of devices to small-to-medium businesses, large companies, public sector organisations and IT security professionals. As well as early warnings, the site provides a variety of clear guidance, infographics, training materials and step-by-step plans to avoid cybersecurity problems.

You should also look at security vendors' websites. These often contain advice on what you should be looking out for and what you can do to defend your organisation from cyberattacks. In addition, you will discover a variety of software and services aimed at securing your systems.

Protecting User Accounts

Password Sharing

One of the main ways in which LIMS and other systems can help with cybersecurity is through protection of user accounts. A fundamental rule to enforce is that users should not share their passwords. They should never allow anyone else to log in using their details.

People should also avoid using the same password for more than one application. In the event of a system becoming compromised, that password may become exposed. The cyber attacker might then use it to access other applications and systems.

Second Authentication Factor

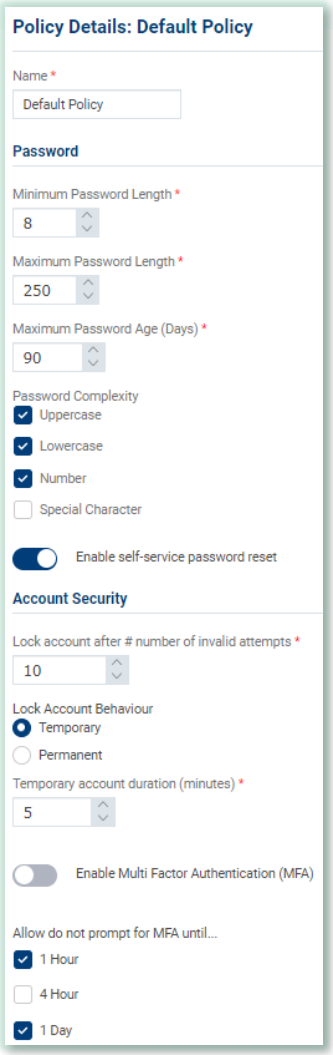
For extra security, your LIMS can be set up to require a second authentication factor, after the username and password, before allowing entry. This approach is variously known as multi-factor authentication (MFA), two-factor authentication (2FA) or two-step verification (2SV). The meaning is similar in each case.

This usually involves sending a verification code, when the user has correctly entered a username and password. Depending on the system and configuration, this may be sent to the user's email address or delivered within a mobile app. Replying with the code verifies the

user's identity. In some systems, the user responds using a physical or software token instead. Even if a cybercriminal obtains your username and password, there is relatively little chance of also having access to your email account, app or token for secondary verification.

Account and Password Policies

Security can be further increased by configuring your LIMS or other system to enforce various account and password policies. To avoid use of short passwords which can be easily guessed, you can set rules on password length and complexity. You may, for example, insist on a certain number of letters, including upper and lower case, as well as numbers, punctuation marks or other special characters. Your policy may also dictate that passwords are changed at set intervals.



Account Lockouts

The ability to lock accounts in the event of suspicious login activity is important. If a user enters an incorrect password a certain number of times, the system automatically locks the account. Without this protection, a malicious agent who has stolen a username might make repeated password guesses, or use an automated script, to find one that works. These are known as brute force attacks.

To allow for genuine mistaken attempts by authorised users, you can give them several chances to get the password right. Your policy will determine how many. You can also decide whether the lockout will be permanent – requiring the user to ask an administrator for a new password – or temporary. In some circumstances, a temporary lockout for a period of your choice may be deemed sufficient. In this case, malicious attempts at gaining access can be disrupted without causing too much disruption to forgetful account holders.

When the user is logged in, a timeout rule can be applied to close the application after a defined period of inactivity. This guards against users leaving their screen unattended and

open to unauthorised access. Another type of lockout can be applied after long periods of user inactivity, which may be weeks or months. If an account holder no longer appears to need access to the system, the safest policy is to lock the account.

Single Sign-on

For teams using several related or linked systems on a daily basis, including a LIMS, it's worth considering a single sign-on approach. This may sound contrary to previous advice, to avoid using the same password in different applications, but in fact it enhances security. Secure single sign-on depends on a cloud-based identity and access management solution such as Microsoft Entra ID. It allows for greater efficiency, applying the same strict security policies, centrally, across all systems. Each user only needs to remember and use one set of credentials.

Regular Software Updates and Patch Management

Operating Systems

You must ensure that the operating system on which your LIMS runs is kept patched and up to date. This applies equally at server level – to application, web and database servers – and at client level – to desktops, laptops and other devices.

For Microsoft applications in particular, updates are issued monthly on Patch Tuesday. These are accompanied by information from Microsoft on what security and other patches have been released. They are given classifications such as 'critical', 'recommendation', or 'important'. It's vitally important to apply patches as soon as possible. Without them, systems and applications are vulnerable to attack.

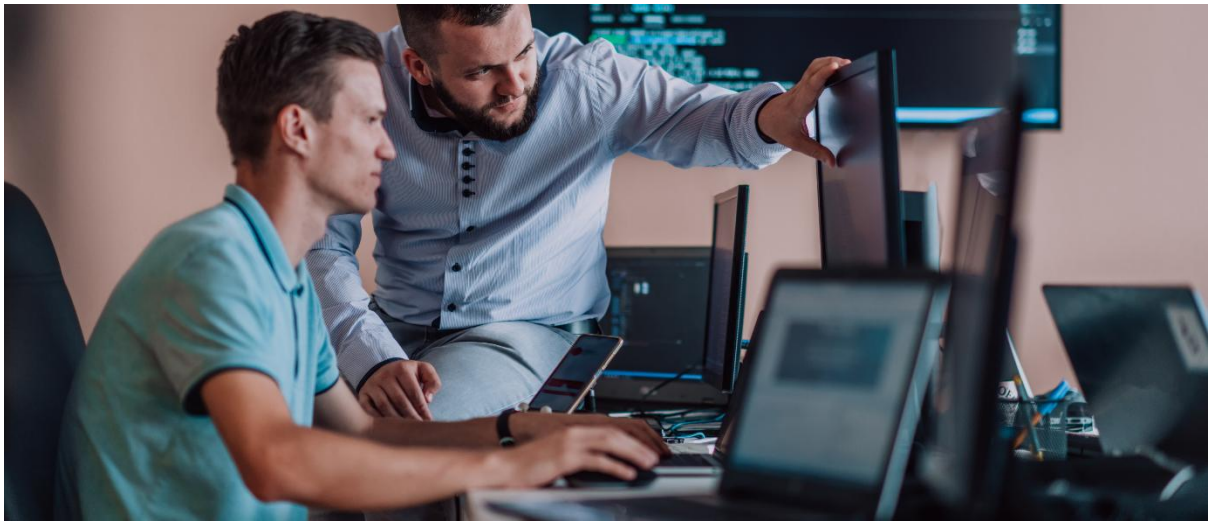
Cybercriminals seek to exploit these vulnerabilities and gain unauthorised access. The vulnerability may be within the application itself or in the underlying server infrastructure. At the client level, attackers often mislead users into clicking on a link leading to a system which executes a script or downloads a file that exploits the non-updated operating system's vulnerability.

Over the years, Microsoft has made it increasingly easy to apply patches. The process can now be automated and enforced. In practice, users are familiar with their machines delaying shutdowns or restarts to allow installation of updates.

The operating systems on which your LIMS depends may include network devices like firewalls and routers. These also have software which requires occasional updating. The vendors of such devices will release security updates as well as improvements in features.

Applications

Then we must consider the LIMS application itself, along with the browser or client used to access the system. The software of these must also be kept updated. Your LIMS vendor should be releasing regular updates, including new and enhanced features, bug fixes and security fixes.



Bear in mind that many applications draw on widely used third-party and open-source components, libraries and codes. Cybercriminals can, over time, find vulnerabilities in them. By upgrading your LIMS when a new version becomes available, you should benefit from updates to these elements too. Vendors of systems using third-party components may release updates, but often the only way to get these out to users is to upgrade the system or application.

As well as your LIMS and other applications, it's important to keep your browser updated if your LIMS is browser-accessed. Most modern browsers automatically update with regular patches, whether they be on separate systems, desktops or other equipment.

Antivirus and Antimalware

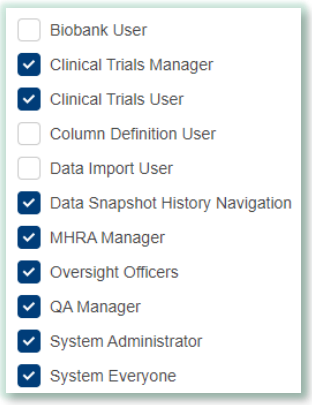
Another essential defence to keep up to date is the antivirus and antimalware systems on all your server devices. These systems vary in their scope. For example, some will just check files, while others offer more intrusion prevention and may add a firewall. In all cases, however, the vendors must continuously release definition updates, as new virus variants and malware are discovered daily and even hourly.

Access Control and Privilege Management

'Broken access control' is currently the number one critical security risk to web applications, according to OWASP (Open Worldwide Application Security Project). OWASP is another good reference source for cybersecurity awareness and training. Your LIMS, and other systems, should allow you to control not only whether an individual is allowed access but what each is allowed to see and do within the system.

Role-based Access Control

Role-based access control (RBAC) places limits on what features and functions can be accessed by different types of users. A system administrator's needs in this respect will be different from those of another manager, while most regular users will have narrower requirements. By assigning access levels according to job roles, you can avoid unnecessarily opening sensitive elements of the system to potential security threats.



Attribute-based Access Control

An additional approach is attribute-based access control (ABAC). Here, the accessibility or otherwise of a record or function is data-driven. The attributes assigned to a particular record determine whether it can be seen, edited, updated, copied or used in any other way. For

instance, in a list of patient records, some fields may be invisible for certain individuals. Going further, ABAC can be combined with RBAC to make a piece of data visible to some users but not to others.

Privileged Accounts

A further option offered by LIMS is to set up privileged accounts for those who need administrative or 'super user' access to the system's data and access management functions. Those in such a role will use privileged access when logging in to carry out high-level administrative and security jobs such as creating and managing user accounts and assigning access levels. For more routine work, the same person may log in as a standard user.

Network Security Measures

Firewalls

To protect your LIMS, you may install a traditional network firewall. This can restrict access based on IP addresses, for example. In a situation where users are accessing your LIMS through a web browser, with the application being run on a web server, you can use Port 433. This is the standard port for HTTPS, which is the secure version of HTTP. It will allow users to browse for your LIMS but without accessing anything they shouldn't.

Today's network firewalls offer additional advances and functionalities. For instance, they can look for certain signatures and protect against identified threats. Whichever you choose, you must ensure a network firewall of some kind is present to defend your system, especially if it's public-facing – in other words, available externally over the internet. You should make sure the only open ports are HTTPS, so users can only access your system via a secure connection.

If your LIMS is a web-based application, another option may be a web application firewall (WAF). This can sit between the web application and the end user. A WAF does more than simply block traffic based on the port or IP address. It looks in some detail at the requests coming from the user toward your web application and inspects them for certain known signatures and patterns. If it spots something suspicious, based on a given ruleset, it blocks

those requests. In particular, it can protect against SQL injection (SQLi) and cross-site scripting (XSS).

Before applying that kind of functionality, it makes sense to put the WAF in monitoring mode and see what rules are being triggered – without allowing it to block anything. Sometimes, if applied too quickly, it can interfere with the activity of the application. It may, for example, try to deal with something which the application itself should handle. In that case, the rules can be adjusted for future reference.

Network Segmentation

Another protection strategy is network segmentation. Again, this is especially important if your LIMS has public-facing internet components. If, for example, your users are spread globally, they may be accessing your LIMS via a portal or by logging onto a browser. Ideally, the public-facing part should be separated from the rest of your network and system.

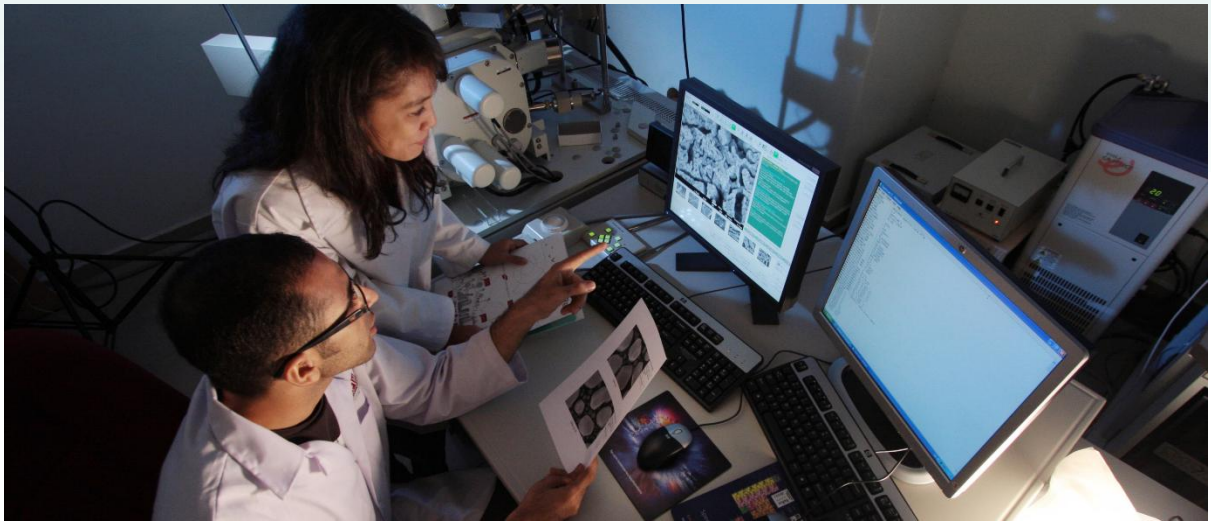
Traditionally, you might place the public-facing web servers in a DMZ ('demilitarised zone') and direct traffic from web applications to a database server in a more secure part of the network. There are other approaches too. Essentially, they make the web front end of the LIMS accessible while keeping the database safe.

Segmentation can also be used to separate production and non-production environments within your LIMS. The non-production side might include test-staging areas, where a new product or process is undergoing validation, user acceptance testing and other assessments. In the event of any cybersecurity problem, it can be checked and corrected before potentially having any impact on the production side.

Backup and Disaster Recovery Planning

In spite of the precautions you put in place, you may still be unlucky enough to suffer a damaging cyberattack. You must be prepared for the worst-case scenario, in which you need to recover your system and data from backup copies. The same preparation will also help in

the event of other catastrophic incidents such as disk corruption, server failure, system faults or data update problems.



Backup of Critical Data and Systems

You need to put standard backup procedures in place for your business-critical systems, including LIMS, to enable recovery of your applications and data. But what are the key components of your critical data and systems? Is it just a single application? If it's running on a server, can you back up the whole server? Are multiple servers involved? Can you back up the database along with the database server? You should ask your vendors to advise on exactly what needs to be backed up in your situation.

You must also identify and document any dependencies of your LIMS on the underlying platform, or other dependencies arising from integration of your LIMS with third-party systems. Those need to be backed up as well, and you will need to know what will happen to that integration in the event of restoring from backups. Will the integrated activity simply pick up again and continue as normal, or is there something you will have to do to recover and restart it? Again, your vendors should advise.

Backup Storage

Once you know what to back up, it makes sense to create multiple backup copies and keep them in secure, separate locations. One copy can be kept on-site, to allow fast recovery. Others can be kept off-site, in case of major damage to the primary site.

Disaster Recovery

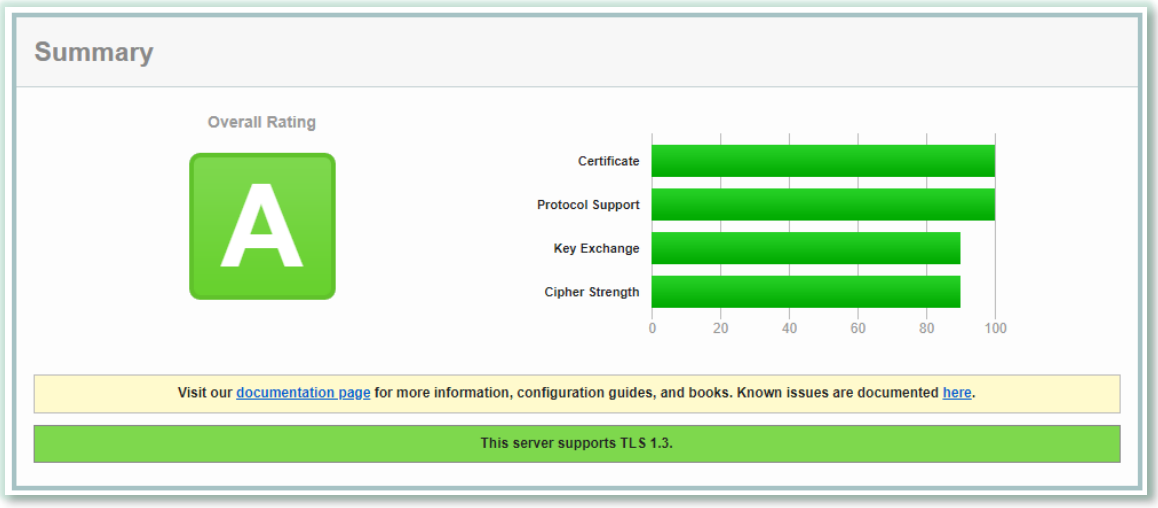
Crucially, you should plan, test and review to make sure you are fully confident that your backups will be able to recover your data and your system functionality if a disaster should ever happen. Your LIMS vendor can help you to draw up a disaster recovery plan, to test whether it will work, and to review it on an annual or other periodic basis.

Data Encryption

Whenever data is transmitted between a client and a server, it should be encrypted for security. The server in this case could be the web server running your LIMS application. You should aim for end-to-end encryption and also encrypt stored data 'at rest' in databases, on disks, on backups, and wherever it is kept. Much of your data will be highly sensitive, including personally identifiable information (PII).

For data at rest, the AES 256 encryption algorithm is the most secure option currently available. For data transfer, you should use HTTPS connection – which is much more secure than HTTP – combined with a widely recognised encryption algorithm. SSL was previously popular, but TLS is now preferred. Each has gone through various versions, as the technology has advanced. These vary in strength.

You need to make sure that your SSL or TLS certifications are in place and that the connections are secure. To test your security, we recommend the service provided by Qualys: www.ssllabs.com



This will test your defences against unauthorised access and will determine what versions of TLS or SSL are being used. It will identify any protocols, cyphers or algorithms that are no longer supported, which could make your site vulnerable. Along with a detailed report, Qualys will give you a summary and assign a security grade to your site.

Continuous Monitoring and Threat Detection

Logging

An important function that your LIMS and other applications should be able to perform is logging of security-related events. These can include, for example, users signing in and signing out, sign-in failures and lockouts, password changes, new account creation and account deletions.

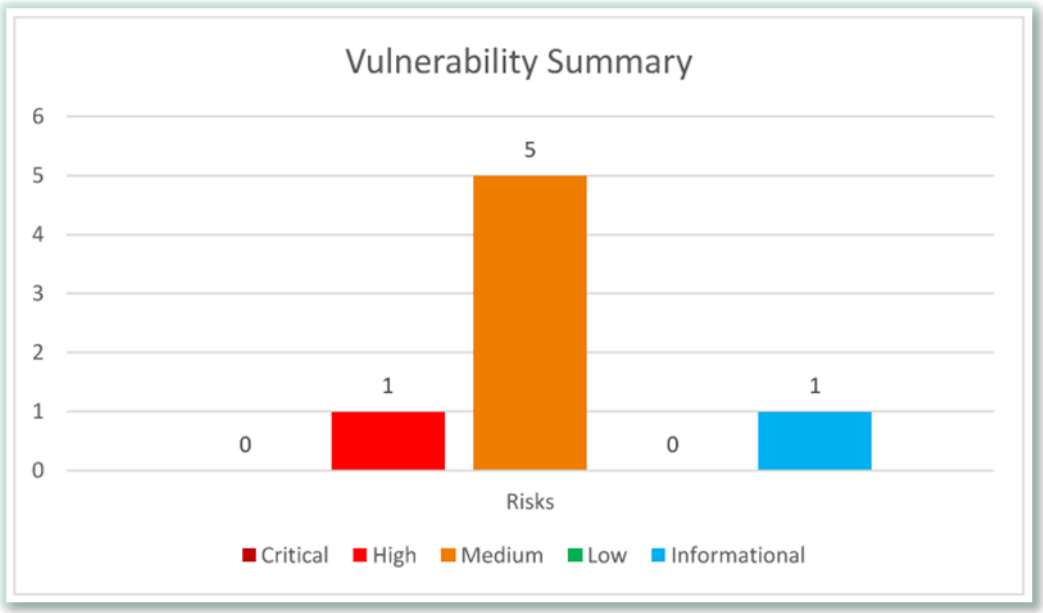
This information is useful for cybersecurity and has other uses. For instance, it allows an administrator to intervene quickly if a colleague is having a problem signing into the system. In the event of a cyber threat or incident, the logged information is invaluable. You can use it to check for evidence of any problem with the LIMS and its security, or simply to rule out the application as the incident's cause.

As part of your standard security practices, you should review the logged data periodically. How long you retain this information should be adjustable and configurable by your LIMS. Depending on your needs, you could automatically delete event data after a short period (say, 30 days) or keep it much longer.

Web Application Security Testing

Another essential of cyber defence is web application security testing. This is particularly important if yours is a public-facing application, or if it's an internal web application accessible across a large organisation. Vulnerability scanning and penetration testing are two common approaches, which are often combined.

Vulnerability scanners automatically test the application against a database of known vulnerabilities. These may include third-party components that are known to be vulnerable, or older versions which are less secure. Details of the risks detected are presented in a report and each is assigned a category: critical, high, medium, low or informational. You can then deal with them in priority order.



Penetration testing is a more manual process. It may involve some automation or software, but often it depends on an actual person logging into your system and using various tools and mechanisms to test its security. They may, for instance, attempt SQL injection (SQLi) or cross-site scripting (XSS) and try to bypass security measures to gain unauthorised access to data and functions. Again, the outcome is a report detailing vulnerabilities. It will also point to mitigation measures needed.

You can share these reports with your LIMS vendor and ask for help in addressing the highlighted risks. In some cases, the problem lies within the application and can only be solved by the vendor. In others, the problem may relate to the platform on which the LIMS is running. Resolving those will require cooperation with whoever is managing the infrastructure, with advice from the LIMS vendor. After patching and making other changes recommended by the reports, you should retest. Health checks should also be repeated periodically as part of your routine cybersecurity processes.

Vendor and Third-Party Risk Management

Finally, make sure you assess, manage and minimise any risk posed to your system by vendors and other third parties who are allowed access. They may need access for installation work, for instance, or to provide various services.

If they have remote access, you should understand what methods and devices are being used and ensure they are secure. Account control is essential, as with all users of your system. Beware of sharing of accounts by several people within a vendor's team. Individually named accounts give you better knowledge of exactly who is accessing the system, what they are doing, and when.

You should know why access is needed and only allow it for the agreed purposes. You may wish to tighten security by allowing access only at pre-organised times. You can also configure accounts so that providers are excluded from areas and data to which they don't need access. A further precaution is to check that they have ISO 27001 and/or Cyber Essentials certification. This gives extra confidence that they will be following best security practices.

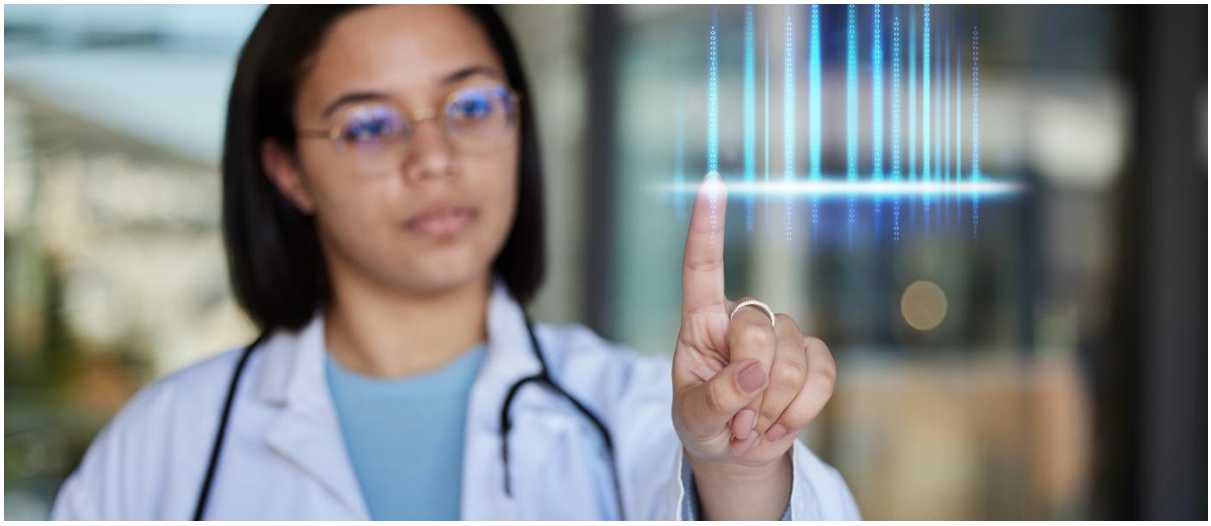
Potential Future Threats from AI and Emerging Technologies

As AI continues to gain popularity and become more accessible across various applications and services, including LIMS, its integration brings both opportunities and challenges.

The increasing computational power and sophisticated algorithms now enable AI to enhance data analysis, streamline workflows, and improve decision-making processes within laboratories. However, this widespread adoption also expands the attack surface for cyber threats. The seamless integration of AI with LIMS means that sensitive data, critical to laboratory operations, is now more exposed to potential exploitation. Moreover, the reliance on AI systems introduces new vulnerabilities, as these systems can be targeted through adversarial attacks, where malicious actors manipulate input data to deceive AI models into producing incorrect or harmful outputs.

To mitigate the cybersecurity risks associated with AI in LIMS, users must adopt a proactive and multi-layered security approach. Implementing strong encryption protocols for data in transit and at rest ensures that sensitive information remains protected from unauthorized access. Robust authentication methods, such as multi-factor authentication (MFA), are crucial for safeguarding system access and preventing breaches. Regular security audits and vulnerability assessments can help identify and rectify potential weaknesses within AI and LIMS infrastructures. Furthermore, continuous monitoring and validation of AI algorithms are essential to detect anomalies and ensure the accuracy and integrity of AI-generated outputs.

By fostering a culture of security awareness and maintaining comprehensive documentation for regulatory compliance, LIMS users can effectively navigate the evolving landscape of AI-driven cyber threats.



Interactive Software Limited

Interactive Software Limited provides Laboratory Information Management Systems (LIMS), Biobanking software and Sample Management Systems that improve quality and compliance and instil good practice through effective processes.

For over 20 years Interactive Software Limited has been helping life science organisations implement successful software solutions that transform the way they work and deliver greater insight into their data. Achiever LIMS is a modern, configurable web-based Laboratory Information Management System (LIMS) that centralises lab data and supports pre-clinical, clinical research, academic research and biorepository processes and compliance needs. Managing all sample life-cycle events, the LIMS gives complete traceability of all sample activities providing evidence for compliance and quality assurance.

With the Achiever Laboratory Information Management System (LIMS), our aim is to support labs to get the most out of every valuable sample. This means giving users simple tools to record, search and analyse data so researchers can easily find samples within their inventory and use them for their intended purpose.

Learn more about Achiever LIMS

https://www.achieverlims.com/| +44 (0)121 380 1010 |enquiries@interactivesoftware.co.uk