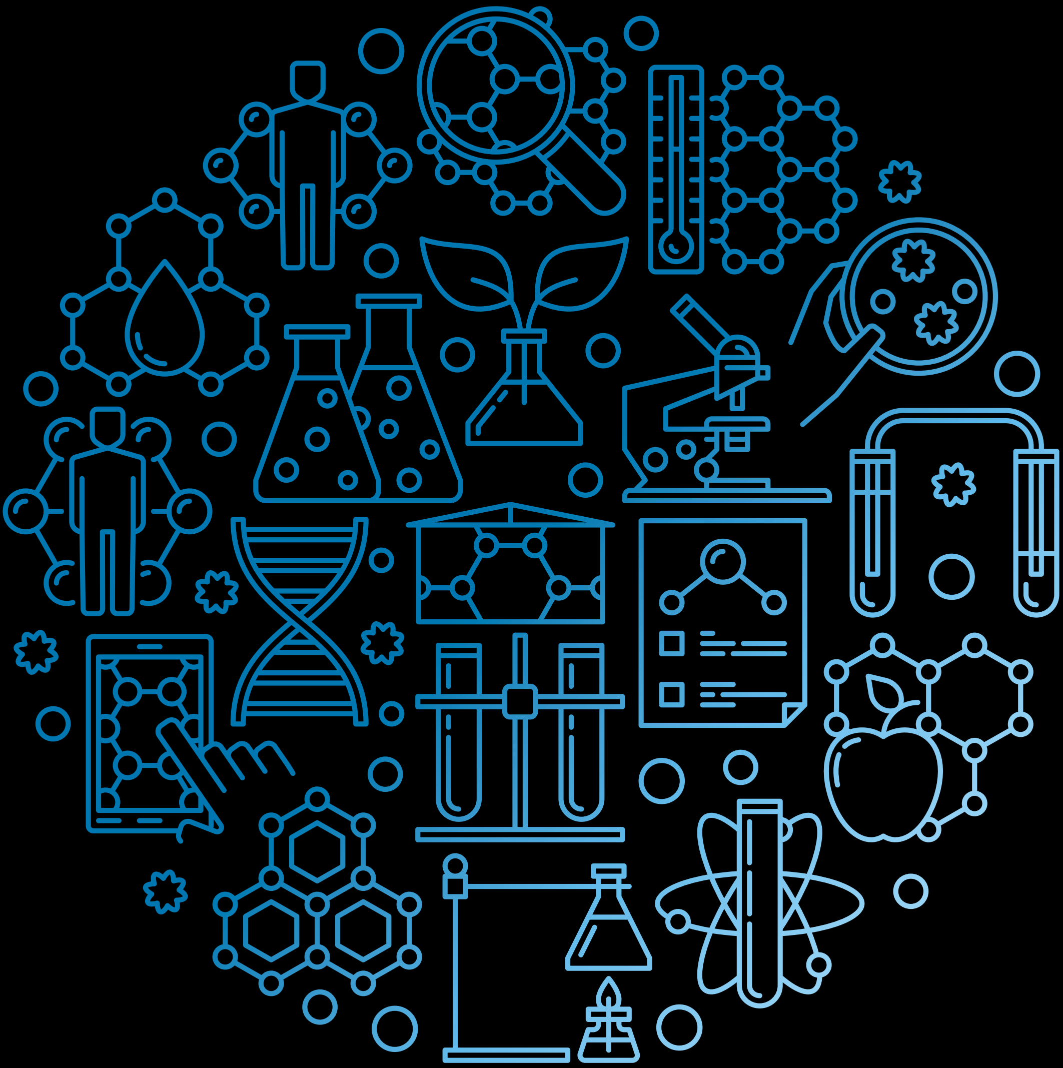
Deloitte.



Cyber Detect and Respond

Staying ahead of cyber threats in the
Life Sciences and Health Care industry

2023

The current Life Sciences and Health Care (LSHC) cyber threat landscape

Currently, the Life Sciences and Health Care (LSHC) industry is at the cusp of change. The main drivers include digital transformation, supply chain optimisation, wearable medical technologies (to improve patient experience, and clinical efficiencies), and development of the new care models. With the adoption of digital technologies, the LSHC industry has taken a quantum leap to transform several clinical processes. In addition, regulatory changes, considerations for data privacy, and guidelines for telemedicine use (released by the government in 2020) have given an impetus to the sector to improve its processes.

Enhancing cybersecurity and protecting intellectual property have emerged as key challenges for many organisations. If not addressed appropriately, these challenges may derail the entire transformation programme of an organisation.

Today, every step along the value chain is transitioning into digital. Hence, organisations must invest heavily to integrate cybersecurity into that digital value chain.

The key factors responsible for changing the LSHC landscape include the following:

- Adapting to the changing consumer needs, demands, and expectations
- Using new care delivery models to improve access and affordability
- Adopting zero-trust cyber security to enhance trust
- Protecting Intellectual Property (IP)
- Maintaining regulatory compliance
- Investing in and enhancing innovation and process transformation

Questions to be considered

As life sciences companies move forward with new and innovative digital technologies, leaders should consider the following questions:

- How is cyber integrated into your innovative approach?
- Who can access the data? What data requires encryption?
- Have you established proper control mechanisms with external parties with whom you share data?
- Are consumers, patients, and/or customers your top priority? Do they trust you?
- Have you invested in cyber risk programmes in tandem with your evolving innovation and R&D models?
- How do you segregate your network, assets, and user access to optimise IP protection?

Did you know?

Protected Health Information (PHI)[1] is 50 times more valuable in the black market than financial information. Stolen patient health records are sold at 10-20 times more value than credit card information.

[1] Why Medical Data is 50 Times More Valuable Than a Credit Card, D Magazine Partners, October 15: https://www.dmagazine.com/healthcare-business/2019/10/why-medical-data-is-50-times-more-valuable-than-a-credit-card/

How we can help

It is important to adopt an agile and dynamic security foundation to identify, detect, protect, and respond to cyber threats generated via internal and external changes and threat actors. This foundation should be flexible enough to meet the challenges faced by modern businesses, the workforce, and technology trends.

A business context-aware approach and a risk-guided cyber detection and response programme provides a foundation for effectively identifying and responding to cyber threats. A robust and proactive cyber risk management programme/strategy enables an organisation to prepare, detect, and respond to possible cyber threats/ incidents. In addition, it is critical for leaders who seek to lead, navigate, and disrupt in the life sciences industry.

The three basic pillars of such a programme include holistic preparation, active detection, and swift response.

Holistic preparation

Patient data, R&D and clinical information, formulations, etc., and the assets hosting this data are the 'crown jewels' for the LSHC enterprises. Hence, to protect them, they should be holistically prepared.

Once an organisation has identified and inventoried this data, preparing a Cyber Incident Response plan (CIR) and planning for the right strategic and technical training is the next step.

A well-developed CIR plan will help an organisation plan and execute mitigation activities to lower the impact of an attack, remediate possible incidents, and secure the overall organisation (in a coordinated manner). This can be achieved while utilising its assets and resources to efficiently minimise the impact on its operations. Further, the staff can get guidance in terms of its regulatory reporting obligations, and board mandates, and consider privacy implications in case of any data breach.

It is essential to train the right personnel from the executive management, IT, business operations, compliance, public relations, etc., to execute this plan. These trainings can be through wargaming or tabletop sessions for non-technical teams and technical cyber simulations for the IT and cyber staff.

Active detection

An intelligence-led and threat-aware Security Operations Centre (SOC) establishes active detection of cyberattacks and data loss attacks, while protecting the digital infrastructure.

A business context-aware and risk-guided approach to cyber security helps anticipate threats through cyber intelligence. This can include the use of threat intelligence feeds, which provide real-time information about known and emerging cyber threats. In addition, regular monitoring of security events can identify and detect possible threats that may bypass existing security controls, allowing for early detection and rapid response to mitigate the impact of any potential security breaches. The following are the two most important factors for a highly effective SOC:

1 **To be aware of the business and risk context**

2 **To be driven with the efficient adoption of the right technology solutions**

The right business and risk context helps an organisation to be agile and flexible in the dynamic and constant risk environment. This must be driven by the right technology solutions. For example, most traditional SOCs use rule-based monitoring tools. The adversaries execute slow attacks or at times drive them via compromised insiders not detected with these traditional solutions.

In such situations, advanced security technologies, such as User and Entity Behaviour Analytics (UEBA) may detect attacks against sensitive R&D, clinical data, personal health records, and business critical infrastructure.

It becomes a huge task for organisations to build, staff, run, and sustain an SOC. In such circumstances, SOC as a Service (SOCaaS) and Managed Detection and Response (MDR) help the LSHC organisations.

Swift response

Swift response is the ability to respond quickly to a cyber incident. This response may be driven via multiple elements, which may vary as per the complexity and the urgency of the response.

A solution like Security Orchestration, Automation, and Response (SOAR) may be used to immediately orchestrate workflows and automate responses to events that carry a very high confidence score and impact a single system. For example, a SOAR solution could be configured to automatically quarantine an endpoint when it detects a high-confidence threat on that endpoint.

However, for complex incidents that have a direct business impact, an escalated incident response retainer (having a retainer of certain hours of highly skilled Incident Responders [IR]) is a must. Today, cyberattacks have become a necessity for LSHC organisations. In addition, it is important to work with an IR retainer who acts as 'expert first responders' to any major cyber incident.

Holistic preparation

- Cyber incident response plan
- Cyber wargaming
- Tabletop exercises
- Cyber simulations
- Technical trainings

Active detection

- Security operations centre
- SOC as a service
- MDR
- Threat intelligence
- Threat hunting
- Attack surface management

Swift response

- Security orchestration, automation, and response as a service
- Cyber incident response retainer

Key benefits

The LSHC organisations should consider a cyber detection and response programme as an integral part of their cybersecurity strategy and transformation journey. It is instrumental in ensuring trust while navigating new business challenges and providing core benefits, such as the following:

Compliance with regulatory norms

Compliance with regulations, including Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Operational efficiency

Active threat detection and automated response actions reduce alert fatigue and the time to respond to cyber incidents. This improves the team's morale and operational efficiency of the cyber staff.

Improved security posture

A well-oiled SOC fortifies and improves the cyber threat detection capability tremendously. The right preparation and ability to swiftly respond to cyber incidents can improve the security posture of an organisation.

Enhanced trust in the business

When organisations endeavour to safeguard the critical data of patients and employees, their trust in the organisation is enhanced. A cyber detection and response programme helps in establishing and enhancing this trust regularly.

The time is now

At Deloitte, we have worked with the major LSHC organisations across the globe. We supported them on their cyber security transformation journey and know how cyber incidents can result in the loss of credentials for an organisation. Some other challenges include the following:

- Brand and reputation loss amongst the patient and healthcare community
- Breach of patient confidentiality
- Regulatory impact in cases where operations have been affected due to cyber incidents
- Clinical data and R&D data loss leading to humongous financial loss

However, an enhanced cyber security posture can be a big differentiator for the life sciences and healthcare industry that helps in enhancing trust and creating an ecosystem for collaborative development of clinical therapies, medicines, and diagnosis.

Connect with us

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Tarun Kaura
Leader – Cyber Advisory
Risk Advisory, Deloitte India
tkaura@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Anand Prakash Tiwari
Partner, Risk Advisory
Deloitte India
anandtiwari@deloitte.com

Kamaljit Chawla
Leader – Cyber Operate,
Risk Advisory, Deloitte India
kamaljitc@deloitte.com

Dr Vikram Venkateswaran
Partner, Risk Advisory
Deloitte India
vikramv@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.