Deloitte.

Stepping into the Future of Cyber

Life Sciences & Health Care

Deloitte's *2023 Global Future of Cyber Survey* reveals that cyber increasingly plays a foundational role in delivering business outcomes. For life sciences and health care (LSHC) organizations, the quality of those outcomes will depend on how well decision-makers understand today's environment and prepare for what comes next.

What does the future of cyber look like for the industry?

These five highlights provide a glimpse into where life sciences and health care organizations are now—and where they are going.

Ecosystems

53%

of LSHC respondents get external help/outsourcing to manage cybersecurity initiatives

Trust

87%

of LSHC respondents expect cyber to have a significant impact on building digital trust for stakeholders

Talent

50%

of LSHC survey respondents said the lack of skilled cyber professionals was challenging or very challenging

Cloud

87%

of LSHC respondents rated cybersecurity as playing a moderate to large role in their Cloud initiative

Strategy

65%

of LSHC respondents have an operational and strategic plan to defend against cybersecurity threats

Becoming cyber-ready

How can life sciences and health care organizations prepare for an evolving cyber landscape? The following five insights and five corresponding actions, based on Deloitte's experience and our survey findings, can provide a starting point for navigating the future of cyber.

Insights to inspire	Actions to consider
1. **Third-party relationships are a top-level concern.** The complex ecosystem of relationships in life sciences and health care—from equipment suppliers to lab contractors to digital service providers—is creating a larger potential attack surface, threatening privacy, sensitive data, and systems integrity.	**Take a risk-based approach to cyber.** Sharpen your tools for risk-sensing, and develop a more strategic approach for preventing and responding to cyberattacks. A comprehensive risk review can help you understand potential business impact and begin prioritizing cyber investments.
2. **Identity has become foundational to business.** Virtual care, remote work, and other practices show the value that can come from new digital business and operating models. Ensuring and managing identities becomes imperative for trust and business outcomes, and 87% of LSHC respondents expect cyber to have a significant impact on building digital trust for stakeholders.	**Embed identity deeply into your business.** As you develop new products, services, business models, and operating models, make identity a foundational part of the planning process. Know how you will establish and maintain high standards for identity and trust.
3. **Talent challenges persist.** Nearly 50% of LSHC survey respondents said the lack of skilled cyber professionals was challenging or very challenging. As many leaders in the industry approach talent needs creatively, they continue to experience steep competition from other industries, including financial services and the consumer industry.	**Lean on others.** Co-sourcing arrangements and outsourcing contractors can provide an answer to the cyber talent challenge. A cyber managed services provider or an outsourced security operations center can bring innovative toolsets and specialists that are difficult to find.
4. **Cloud can be a double-edged sword.** Cloud ranked as the No. 1 digital transformation priority among LSHC companies in our survey. While cloud solutions can help address complexity and support business goals, cloud brings layers of considerations for product security, privacy, regulations, and other critical issues.	**Dive into the details of cloud.** Understand who is hosting your data and systems. Know what they are doing with your digital assets and how are they protecting them. Ask how they are using identity to manage access and security and get clarity on their regulatory compliance activities.
5. **Business ambition continues to outpace cyber strategy.** As LSHC organizations grow and innovate, their cyber plans and activities may not align with their business strategies, objectives, and new realities. Cyber can be a powerful enabler of business agility and future business outcomes, but it is often treated as an afterthought.	**Look at privacy and cyber holistically.** Growing interconnectedness, including connected medical and health devices, brings new potential for data breaches. Develop detailed plans to keep up with changing global regulations, track assets, and avoid surprises—even as you innovate and grow.

To get a broader view of the cyber landscape, explore additional insights from the *Deloitte 2023 Global Future of Cyber Survey*, which asked 1,110 leaders across industries and across the globe to share their views on cyber threats, enterprise activities, and the future.

Deloitte.

www.deloitte.com/futureofcyber

Life Sciences & Health Care