Deloitte.

Cyber cost optimization in life sciences

Cyber cost optimization: Measured progress toward risk reduction

In the dynamic landscape of life sciences, organizations—including big pharma, medtech, biotech, generics, and contract manufacturing organizations—are increasingly facing the challenge of escalating cyber operating costs. The need to protect sensitive data (e.g., protected health information, personally identifiable information), comply with regulatory requirements, protect cyber-physical systems (e.g., manufacturing operational technology, building management systems), safeguard intellectual property (e.g., manufacturing recipes, medical device designs), and—very importantly—protect patient safety has not been more critical or complicated. However, these table stakes can come with significant financial implications. This article explores strategic approaches to cyber cost optimization in the life sciences sector, addressing industry-specific concerns and solutions.

Cost optimization is essential for CIOs, CISOs, CFOs, and their organizations to evolve

Cybersecurity leaders are being challenged to manage against steady budgets despite growing demands—both internal and external. There is consistent pressure from within to not only protect the organization from attack using broad cybersecurity measures, but also demonstrate the value these costly investments bring. In other words, company leaders want to understand the level of risk reduction that is being achieved so they can determine if the cyber spend is commensurate with real cyber risk reduction. Additionally, from an external standpoint, there is pressure to adhere to stringent regulatory requirements, which demands continuous investment in the cybersecurity program. We expect these regulatory requirements to increase in velocity and volume.

Adding to the above challenges is the complex technology landscape. Many life sciences organizations have invested in a large, varied portfolio of technology solutions, many of which are not utilized to their fullest. These factors make it imperative for organizations to find ways to generate the greatest value (e.g., cyber risk reduction) for their cyber spending.

What is cost optimization?

Deloitte considers cost optimization as finding the optimal allocation of cybersecurity spend such that cybersecurity goals/objectives (e.g., complying with regulations, protecting patient safety, protecting manufacturing systems and operations) are met with both efficiency and effectiveness. It is not just cost takeout/savings; it involves strategic resource allocation (both people and technology assets), effective risk management, maintaining regulatory compliance in a cost-effective manner and most importantly reinvestment of any cost takeout/savings back into the cyber program. This includes technology rationalization to reduce redundancies, vendor management for better pricing and service integration, and leveraging advanced technologies like artificial intelligence (AI) to enhance capabilities. Additionally, it requires continuous improvement to adapt to evolving threats and industry-specific concerns, maintaining robust protection while optimizing costs. The urgency is driven by escalating cyber operating costs and the increasing complexity of threats, making it imperative for organizations to adopt efficient strategies to protect sensitive data and comply with stringent regulations while maintaining financial sustainability.

There are several approaches to achieving cost optimization in the cybersecurity program. One approach is labor sourcing and workforce optimization. By refining and streamlining the cyber organization's talent structure and shifting to outcome-based delivery, organizations can build a cybersecurity workforce that meets their dynamic needs. Balancing insourcing and outsourcing by evaluating the optimal mix of in-house and outsourced cybersecurity services can lead to significant annual cost savings, some of which can be reinvested in the cyber program.

Another important area is technology rationalization. Streamlining the security application portfolio by identifying rationalization opportunities and standardizing information technology (IT) and operational technology (OT) tools/platforms can enhance the cyber infrastructure. Regular reviews of security architecture help identify and better utilize technologies, reducing costs and improving security posture. Integrating advanced analytics and automation can provide deeper insights into technology performance and potential vulnerabilities. Reviewing the capabilities of tools and technologies as they evolve helps organizations to leverage investments fully. Utilizing cybersecurity platforms from leading tech companies (e.g., hyperscalers)—or platformization—can help to create synergies and enable scalability.

Vendor and third-party consolidation is another strategic lever for cost optimization. By strategically consolidating alliances, organizations can reduce redundancies and align vendor relationships with evolving cybersecurity needs. Centralized vendor management can lead to better resource utilization and cost savings. This approach helps organizations to get the best value from their vendor relationships.

Leveraging AI and automation to optimize processes can improve productivity, fortify effectiveness in identifying and countering threats, and enhance user experience. Streamlining and automating operational processes can lead to significant cost reductions. This not only reduces the burden on cybersecurity professionals but also can help the organization respond quickly to emerging threats.

Addressing industry-specific concerns

The life sciences sector faces unique challenges that necessitate tailored cyber cost optimization strategies. Protecting sensitive patient data and complying with regulations such as the European Union's Cyber Resiliency Act, the US Food and Drug Administration's Omnibus Act, General Data Protection Regulation (GDPR), and Good [x] Practices compliance (GxP) are paramount. Organizations must invest in robust data encryption, access controls, and continuous monitoring to safeguard this information. Additionally, the sector's reliance on intellectual property, such as proprietary research and clinical trial data, requires advanced threat detection and response capabilities to prevent data breaches and intellectual property theft.

Another concern is the integration of cybersecurity measures with existing IT and OT systems. Life sciences organizations often operate in complex environments with interconnected systems, making it essential for cybersecurity solutions to not disrupt critical operations. Implementing cybersecurity measures that are compatible with existing systems and processes can help maintain operational efficiency while enhancing security.

Ready to start optimizing?

In the life sciences sector, cyber cost optimization is not just a financial imperative but a strategic necessity. By focusing on labor sourcing and workforce optimization, technology rationalization, vendor and third-party consolidation, and leveraging AI and automation, organizations can navigate the complexities of cybersecurity, achieve significant annual cost savings reinvesting that savings back into the cyber program, achieve more effective and efficient security operations, provide their cybersecurity workforce with more meaningful and higher-value activities/work, and enhance their overall security posture. Addressing industry-specific concerns, such as protecting sensitive data, maintaining regulatory compliance, and protecting cyber-physical systems (e.g., manufacturing and distribution centers), is crucial for cyber cost optimization. The journey toward cyber cost optimization is a continuous process, requiring ongoing assessment, adaptation, and innovation to stay ahead of evolving threats and challenges.

Contacts

Russell Jones

GICSP, CISSP, CSSLP
Partner
US Product Security Leader and Life Sciences Industrial Control Systems/OT Cybersecurity Leader
Deloitte & Touche LLP
+1 415 783 5054
rujones@deloitte.com

Sunny Aziz

Principal
Risk & Financial Advisory
Deloitte & Touche LLP
+1 713 982 2877
saziz@deloitte.com

Deloitte.