Deloitte.

Two steps ahead: How life sciences and health care can improve their cyber posture

While enhancing cyber risk analytics and reporting is a critical milestone for life sciences and health care organizations, it is in some ways only the first step

In October 2020, three US agencies joined forces to issue a stark warning to hospitals and health care providers: Ransomware attacks are on the rise—and institutions need to take immediate action to protect themselves.

According to the report, co-authored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department for Health and Human Services (HHS), ransomware attacks, service disruptions, and data theft all increased substantially in the sector since 2019, and the COVID-19 pandemic only escalated the problem.[1]

Starkly stated, cybercriminals see life sciences and health care organizations not only as a source of significant revenue, but also as treasure troves of sensitive data. To counter these threats, the time has come for the industry to up its cybersecurity game.

Out with the old

Part of the challenge is that many life sciences and health care institutions currently evaluate risk based on qualitative assessment and non-validated opinion. The challenge? This approach is both imprecise and ill-suited to today's advanced cyber threats.

To move up the maturity ladder, CISOs must actually be able to prioritize and address areas of greatest risk, secure employee and patient data, and clearly identify the enterprise systems and standards required to get the job done. This necessitates access to robust cyber risk analytics and reporting. To make more informed decisions and set enterprise-level goals, CISOs must be armed with visual cyber risk reports and dashboards that are as credible, defensible, and actionable as financial statements.

[1]Cybersecurity and Infrastructure Security Agency, *Ransomware Activity Targeting the Healthcare and Public Health Sector*, 2020.

A new approach to cyber risk reporting

To get line of sight into their most pressing risk areas and blind spots, today's organizations are consequently turning to more advanced analytical solutions.

Rather than simply identifying high impact/high risk areas, these approaches kick it up a notch—leveraging near-real-time data insights to obtain actionable insight into specific scenarios. So, for instance, while a traditional approach to cyber risk management might identify a high risk of reputational damage, a data insights-based approach could indicate not only which application may contribute to that risk but also steps you can take to mitigate it. Going granular, it could arguably even show you that you can reduce risk by X% if you use a certain type of secure server.

In fact, this level of reporting could:

- Provide management and the board with a clear view of cyber risks and offer insight into vulnerable geographies, lines of business, and departments.
- Adhere to a widely-accepted cybersecurity framework (e.g., NIST CSF, FAIR, etc.).
- Support decision-making by calculating cyber risk scores from near-real-time data, and consolidating this data from many different systems and entities.
- Allow for more accurate root-cause analyses.

This capacity can allow life sciences and health care organizations to aggregate, normalize, and enrich their data inputs. It attaches risk to specific areas of the organization—for example, a certain product line or hospital—and can help institutions and organizations improve their risk posture by making better investment decisions that align with their cybersecurity strategy. Taken to its logical conclusion, it can empower:

- **Standardized relative risk scoring.** By quantifying risk on a normalized risk scale—and looking at things like process/asset criticality, vulnerability, and threat severity—CISOs can more accurately compare risk across the organization and prioritize cyber risk reduction initiatives.
- **Scenario modeling and predictive analytics.** Cyber risk analytics and reporting allows CISOs to conduct "what if" analyses to identify opportunities to lower their cyber risk score.
- **Value at Risk (VaR) and Return on Investment (ROI), in dollar terms.** Data-driven solutions enable the quantification of risk in financial terms so you can compare the costs, benefits, and ROI of every business decision. VaR is a particularly helpful feature that allows everyone in your organization—from management to finance to operations—to speak the same risk language.
- **Joint decision-making.** Every leader approaches risk assessment differently based on their organizational placement, oversight, and priorities. Cyber analytics and reporting solutions allow each of these leaders to draw different insights from the data, so they can find answers to their most pertinent cyber risk questions and make decisions accordingly.
- **Actionable insights.** Today's solutions don't just identify your most pertinent risks. They also provide actionable insights to help drive proactive risk remediation.

Reporting is just the beginning

While enhancing your cyber risk analytics and reporting is a critical milestone for life sciences and health care organizations, it is in some ways only the first step. Once the foundation is in place to actively manage cyber risks through data insights—and drive actions to help you reach your key performance indicators—it then becomes possible to use that data to advance your organization even further.

For instance, once you have sufficient insight into the financial implications of your business decisions, you can determine where to allocate your next dollar to see a better return. You can better define your ultimate risk appetite and more accurately assess the level of investment risk you're willing to accept. And depending on your level of maturity, you can gain unprecedented visibility into hidden risks—and execute risk-intelligent responses which could involve bolstering your controls, allocating additional resources, or mitigating through a cyber insurance policy.

Moving from advanced analytics and reporting towards cyber risk quantification should allow organizations to do more than shore up their defenses against bad actors. It should also position an industry under pressure to enhance data security, better protect people's privacy, and make investment decisions aligned with strategic priorities.

Contacts

Amir Belkhelladi | Partner, Canada Cyber Leader
+1 514 393 7035
abelkhelladi@deloitte.ca

Mary Konstantinidis | Director, Cyber and Strategic Risk
+ 1 416 354 0618
mkonstantinidis@deloitte.ca

Jamie Lanoue | Partner, Cyber and Strategic Risk
+1 416 601 6221
jlanoue@deloitte.ca

Noemi Chanda | Director, Cyber and Strategic Risk
+1 416 775 7460
nchanda@deloitte.ca