

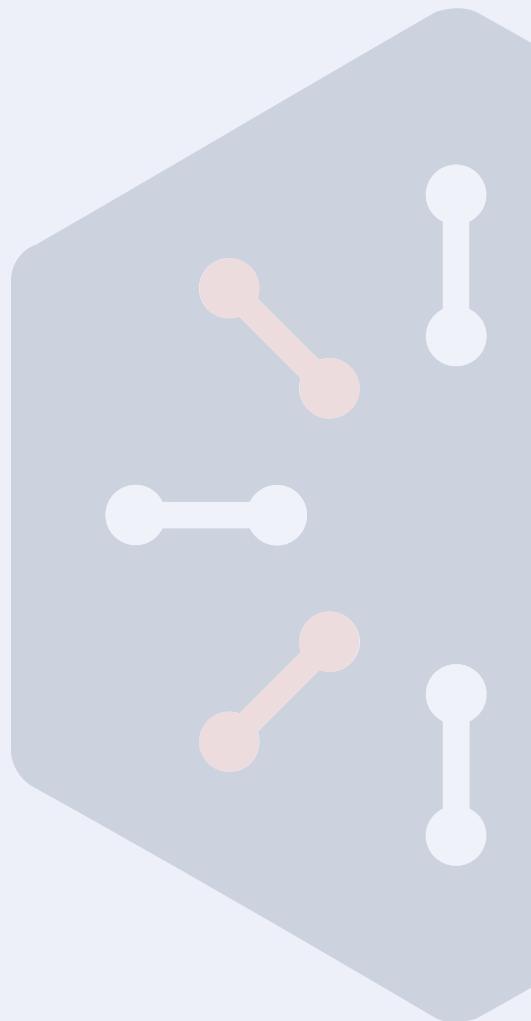
Reducing Cyber Risk in the Healthcare Industry

Business strategy must take into consideration the regulatory and industry requirements for healthcare information protection, while technology strategy must create effective infrastructures for managing those risks. If these efforts aren't aligned, you are vulnerable to cyber threats and regulatory scrutiny.

The yearly hidden costs of managing vendor risk using traditional methods is \$3.8 million per healthcare provider, far surpassing the \$2.9 million that the average data breach costs. Healthcare providers have an average of 1,320 vendors under contract, but just 27% said they assess all vendors annually, even though approximately 20% of breaches in healthcare are caused by third parties.

The CyberGRX platform was created with the help of design partners such as Aetna for an emphasis on healthcare and healthcare-focused regulations. CyberGRX brings visibility, scalability, and accuracy to third-party cyber risk management programs (TPCRM) around the globe. We understand the importance of identifying and mitigating cyber risk due to third parties introduced because of Digital Transformation and balancing the need to become more agile while still protecting EPHI. Together with enhanced privacy controls, you can effortlessly meet third-party regulatory requirements that apply when data is shared with third parties, reducing your cyber risk even more.

The CyberGRX Exchange is a centralized hub where enterprises and third parties can easily access, order and share thousands of dynamic, cyber risk-based assessments to help manage risk across security, privacy, and business continuity. Coupled with these dynamic assessments, advanced analytics capabilities protect you against downtime and disruption with an up-to-date view of risk for continuous monitoring and mitigation insights. We provide invaluable visibility through the entire TPCM life cycle.



Reduce Risk & Scale your Healthcare TPCRM Program with the CyberGRX Exchange

Challenges for the Healthcare Industry	CyberGRX Effects
 Largely powered by legacy IT systems	Cloud-based platform with state-of-the-art security and risk controls
 Digital transformation due to remote work and telehealth services increases cyber risk	Rapidly identify and prioritize the vendors who pose you the most risk with Auto Inherent Risk (AIR) Insights™
 Regulations such as HIPAA require that covered entities perform third party due diligence as it relates to EPHI	Framework Mapper maps to most customer controls as well as industry standards and frameworks (NIST –800.53, NIST-CSF, ISO 27001, PCI-DSS, HIPAA, etc.)
 Security postures of third parties can change without notice, leaving healthcare organizations open to unknown risk	Move past point in time assessments to continuous assessments and monitoring to mitigate any risk of disruption before it happens
 Shrinking IT Budgets and headcount despite the increased use of third parties	Accurately forecast spend due to a fixed pricing model and sharing of expenses with other companies via exchange economics, allowing organizations to do less with more

Visit our website and contact us today for a free trial

www.cybergrx.com

Cyber  GRX