PHARMACEUTICAL TRENDS IN CYBER

MERGERS, AQUISITIONS DIVESTITURES & INTEGRATIONS

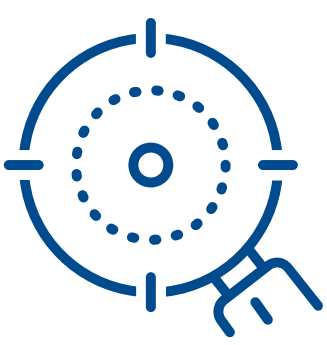
There is a continuous flow of mergers, acquisitions, divestitures and integrations, yet Cybersecurity departments still struggle to get involved early enough. Many that do, don't have the right playbooks or skills to influence in the various phases (due diligence, deal, integration).

THIRD PARTY RISK MANAGEMENT

Third Party Risk Management and addressing the heightened "supply chain" risks of 2020/2021 have driven activity and technology. Yet, few Pharma companies have figured out to holistically manage third party risk at scale.

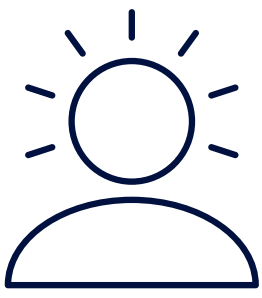
UNDERSTANDING OF "CROWN JEWELS"

The lack of understanding of the most sensitive data and failure to equip employees with business relevant tools, skills and processes to safely handle them has progressed in a subset of the largest Pharma companies.



WITHIN DETECT & RESPOND

Large SIEM efforts have dominated budgets, capacity, and elapsed years and not returned the promise of ubiquitous integration of all risk data and instant action. MDR/XDR tools have edged out some of the focus and the legacy SIEMs are often reserved more for required compliance and logging efforts.



AWARENESS & BEHAVIOR CHANGE

Automated ethical phishing campaigns have usurped many IS Awareness programs. While efforts are good, employees have been relinquished of many of the broader business related cybersecurity behaviors and culture change needs (understanding sensitive data they handle daily and how to secure it).

PROGRAM MATURITY MANAGEMENT

PMM (such as using NIST CSF) has been pretty universally conquered, but to varying levels of effectiveness and transparency. Using consultants to do expensive annual assessments, conducting internal reviews, and in some cases, skewing results for personal reasons can distract from the real needs for a company. Not enough CISOs are investing in tools such as TrustMAPP which are aimed at Security Performance Management.

HIGH INVESTMENT, LOW RETURNS

When teams struggle to scale tools to capacity or the desire business risk driven focal areas, the tools often fail to achieve their value or any ROI. A more rationalized cyber tool architecture is necessary to keep teams focused and have a chance of getting your money's worth in risk reduction for organizations.

REVEALRISK
SECURE YOUR BUSINESS