CORL technologies

THE EVOLUTION OF THIRD-PARTY RISK MANAGEMENT IN HEALTHCARE

The last 20 years have seen a steady escalation in cybersecurity risks associated with third-party vendors servicing the healthcare industry. Our team at CORL Technologies has been at the helm of developing and innovating cybersecurity and Third-Party Vendor Risk Management (TPRM) solutions for the healthcare industry for over 25 years.

HEALTHCARE TPRM TRENDS TIMELINE

2000 - 2005

- Leading healthcare entities begin movement from paper to electronic health records
- Breaches of patient information and systems begin to accumulate, but the lack of a reporting mandate results in most breaches being handled internally by healthcare entities
- Vendor risk management functions in healthcare are limited largely to physical access and vendor financial viability and do not include cybersecurity vetting

2005 - 2010

- HITECH ACT is passed which includes the Meaningful Use incentive program which accelerates adoption of EHRs
- The HIPAA Breach Notification Rule becomes effective & HHS creates its breach "wall of shame"
- Breaches of patient data and systems become wide-spread, but the continued lack of reporting of incidents creates blind spots for the industry
- Dedicated TPRM programs are largely non-existent in healthcare
- Vetting of vendors is mostly limited to "tier 1" applications
- Vendor security questionnaires become the most common TPRM audit and assessment vehicle
- CORL's CEO, Cliff Baker, architects the HITRUST Common Security Framework (CSF) as a model to certify healthcare vendors on cybersecurity practices
- CORL is envisioned and work begins to design a dedicated solution for healthcare third-party vendor risk management

2010 - 2015

- Digitization of healthcare gets mainstream and large volumes of electronic patient data begin to proliferate within and outside of healthcare entities for business support, research, clinical optimization, debt collection, and many other use cases
- Cloud platforms become mainstream and adoption accelerates for healthcare vendors, products, and services
- Reportable breaches of patient information and systems begin to pour into HHS from both Covered Entities and Business Associates (vendors)
- The vast majority of third-party vendor breaches involve lost or stolen laptops and portable media that are unencrypted, though some network hacking breaches are also reported
- CORL is incorporated and the healthcare industry's first dedicated TPRM managed service and cyber risk score is created for healthcare vendors
- Healthcare organizations begin to contractually require vendors to obtain and maintain cybersecurity certifications like HITRUST and SOC 2
- Dedicated TPRM resources and teams begin to be created for leading healthcare organizations
- CORL receives GRC Technology Innovation Award for leading the healthcare industry in third-party vendor risk management innovation

2015 - 2020

- The volume of healthcare vendors booms, and most vendors have access to electronic patient data
- OCR begins to shift focus on HIPAA enforcement to include third-party business associates
- Medical device and IoT security risks surface for healthcare providers and device manufacturers
- Reportable breaches in healthcare increase 178% from 2015 to 2020
- "Mega vendor breaches" begin to surface, including Facebook (50 million users) and American Medical Collections Agency (25 million patients)
- Cybersecurity certification adoption accelerates as more healthcare entities require vendors to be certified
- Dedicated TPRM resources and teams start to become commonplace for larger organizations
- The healthcare market gets crowded with TPRM technology solutions, including cyber risk scoring companies, GRC tools with TPRM functionality, security questionnaire automation solutions, and more
- Healthcare vendors begin to get overwhelmed with the volume and depth of cybersecurity risk audits
- CORL launches dedicated service for vendors to help them respond to vendor risk assessments
- CORL reaches milestone of assessment of over 50,000 healthcare vendors for cyber risks

2020 - 2022

- Ransomware becomes a top threat vector for healthcare vendors
- Majority of vendor breaches shift from lost and stolen portable devices to external hacking sources targeting the healthcare supply chain
- Class action lawsuits begin to emerge for healthcare entities and their vendors following public breaches
- SolarWinds vendor attack impacts thousands of companies globally
- Kaseya vendor infected with ransomware and impacts thousands of organizations
- Apache Log4j breach exposes significant global risks from fourth-party technology solutions
- CORL begins publishing CORL Vendor Breach Digest illustrating an average of 15-30 healthcare vendor breaches every two weeks
- President Biden issues two executive orders on supply chain risk management
- NIST updates NIST SP 800-53 to include a domain dedicated to supply chain risk management
- The CISA, FBI, and other federal agencies issue guidance on supply chain risk management
- Dedicated TPRM teams and programs become standard practice for many healthcare organizations
- Most mid- to large-sized healthcare entities deploy one or more TPRM technology and services solutions
- The average healthcare organization assesses less than 5% of their third-party vendor portfolio
- CORL establishes position market-leading position as premier technology and managed services provider for TPRM for the healthcare industry and takes major growth investment
- CORL reaches milestone of assessment of over 90,000 healthcare vendors for cyber risks and creates data reuse model to accelerate validated assessments of vendors

2023 - 2030+

The publication date for this blog is in 2022. The following timeline is a forecast of healthcare TPRM trends based on CORL's experience as an industry-leading TPRM solution provider dedicated to healthcare.

- Cloud-hosted platforms and third-party vendors become the primary custodians of electronic patient information; on-site data centers at healthcare organizations become endangered
- HIPAA law overhauls and related bills are drafted and passed that place a strong emphasis on third-party vendor risks and related enforcement
- State laws begin to surface to address third-party cybersecurity and supply chain risks
- Class action lawsuits increase in frequency and put pressure on healthcare entities and vendors to invest in cybersecurity protections
- Healthcare cybersecurity certifications including HITRUST and SOC 2 become standard cost of doing business for vendors servicing the healthcare industry
- Vendor breaches continue to escalate exponentially in healthcare and other industries creating an untenable risk situation for healthcare organizations
- Medical device and IoT risks introduce unprecedented risks to patient safety and medical device manufacturers come under increased scrutiny and regulatory pressure
- Nation states and cybercriminals continue to target the healthcare vendor supply chain to "hack once and breach many" organizations
- Supply chain breaches and risk management programs evolve beyond third-parties to fourth-parties and beyond
- Vendors increase investments in cybersecurity programs, teams, and certifications
- Consolidation of TPRM solution providers accelerates to include optimized use of vendor risk data, validation, automation, and services without having to implement multiple tech solutions
- TPRM programs move away from questionnaire-centric models towards assurance models via certifications and other validation vehicles to scale to full coverage of vendor portfolios
- Programs invest heavily in vendor risk automation to scale coverage, reduce turnaround time, and reduce costs
- Vendors begin to get more organized and drive assessment and assurance standards that reduce cost and effort for providing cybersecurity assurances to the market
- Data-driven analytics and risk decision support become fundamental components of TPRM programs and solutions

CONCLUSION

The healthcare industry has been on a wild ride the last 20 years. The introduction of digital health and the technology boom driven by third-party vendors have presented new risks that the industry is still struggling to manage.

CORL has been here through it all. We appreciate the opportunity to have developed innovative TPRM solutions and are looking forward to working together with the healthcare industry to continue to develop and introduce new solutions to keep pace with these accelerating supply chain risks.

TECHNOLOGY LED, HUMAN ELEVATED.

CORL is the only Third-Party Risk Management (TPRM) solution dedicated to healthcare that solves for risk.

We transform TPRM teams into healthcare technology adoption accelerators, not roadblocks.

A stark contrast to TPRM tools that stop short of solving the problem, we are committed to solving for risk through a service-centered approach that supports healthcare organizations and their business associates through every stage of the vendor lifecycle—from sourcing and comparison to intake, implementation, maintenance, and contract closeout.

Our proactive approach to vendor validation, novel models for accessing and utilizing data, and suite of tools for strategic decision support transform TPRM into the powerful business enabler that it should be for everyone in the ecosystem.

Contact our team if you have any questions or would like to learn more about how CORL solves for risk and can revolutionize your third-party vendor risk program.

VISIT CORLTECH.COM AND FOLLOW US ON LINKEDIN

CORL technologies