CORL technologies

Legal Defense Against the Dark Arts:

Battling Supply Chain Breaches

Dark Battles Underway

Supply chain hacking attacks like SolarWinds, Microsoft Exchange, and Blackbaud breaches have unprecedented scale

Nation states are strategically targeting the supply chain

Global cybercriminals are reaping major profits

Ransomware attacks are dominating global headlines

Class action lawsuits are racking up huge price tags

Remote workforce and telehealth are extending the attack surface

29% of all breach victims had more than one threat group in the victim environment

$7.13m average cost of a breach for healthcare entities

329 days average time to identify and contain a breach for healthcare

$20.8B cost of ransomware attacks on U.S. healthcare organizations in 2020

The Attackers Who Shall Not Be Named

Attacks on healthcare have been attributed to:

- Russian and Eastern European cybercriminal gangs
- 1,900 total threat groups according to Mandiant's M-Trends 2021 Report
- Russian spy agencies (e.g. GRU): SolarWinds supply chain attack, WannaCry ransomware
- China: Microsoft Exchange supply chain attack
- Opportunistic cyber criminals

From the Ministry of Supply Chain Regulations

- OCR is focused on business associate compliance with HIPAA Security Rule requirements
- GDPR EU directive on third-party privacy and security due diligence risk expected this summer
- New NIST 800-53 Supply Chain Risk Management domain
- 2021 Presidential Executive Order on supply chain risks
- 2021 UN directive on supply chain protection
- New CISA report: Defending Against Software Supply Chain Attacks

Legal Spells to Cast

- Update contracts with vendors to include security requirements
- Define specific Service Level Agreements (SLAs) and include in contracts
- Require cyberliablity coverage for all vendors
- Define breach notification requirements and communication expectations for breach events
- Require small vendors to carry cyberliability coverage of at least $2M to $5M
- Include right to audit clauses and penalty clauses in contracts
- Implement tracking of vendor compliance with SLAs and conduct routine audits
- Encourage or require vendors to obtain a security certification such as HITRUST, ISO, & SOC 2; set a timeline for certification (e.g. 12 to 24 months)
- Define an exist strategy; include contract requirements for data destruction and return upon termination
- Encourage or require vendors to provide a third-party penetration test
- Require vendors to notify your organization as remediation items are completed or addressed
- Require proactive reporting if there are any changes in the vendor risk profile, including breach events
- Include contract requirements for business continuity and disaster recovery timelines and SLAs
- Identify and require routing reporting of subcontractors and fourth parties that will access to your data
- Maintain an inventory of vendors in scope for regulatory requirements (e.g. identify HIPAA business associates and update BAAs)
- Review merger ad acquisition clauses and define confidentiality provisions in vendor contracts

CORL's Protective Charms

- Healthcare's only clearinghouse exchange of vendor assessments
- BAA inventory management services
- Tech-enabled managed services for vendor risk management
- 79,000+ vendors assessed
- Gets results by driving vendors to risk reduction
- Make informed supply chain risk decisions
- Drive and track remediation
- 100+ healthcare customers
- Less cost, more coverage, & higher quality risk outcomes
- Accelerate assessment turnaround times
- Validate controls and gain assurance
- Scale vendor risk programs
- Tech automation + data + services = risk reduction

Contact our team to learn more our tech-enabled managed services for third-party risk and how we can accelerate your program response time and reduce costs for managing risk for your supply chain.

CORL is a leading provider of tech-enabled managed services for risk management and compliance for healthcare organizations. CORL gets results by scaling organizational and vendor risk programs through our healthcare vendor clearinghouse, dashboard reporting that business owners can understand, and proven workflows that drive the organization to measurable risk reduction.

VISIT CORLTECH.COM AND FOLLOW US ON LINKEDIN

CORL technologies