

LIFARS USE CASES



INDUSTRY: Global Medical Equipment Manufacturer

SCENARIO: Upon suffering an APT attack from a state sponsored group, client needed to establish a solid Information Security Program to address evolving cybersecurity risk landscape.

LIFARS SERVICES: LIFARS Cyber Resiliency Program (CRP)

Upon assisting client to respond to this incident, LIFARS provided the following services to minimize information security risk:

- Assessed Enterprise (global) Information Security including Cybersecurity, Privacy and Compliance relevant risks (landscape, profile, appetite, and tolerance for Business, GDPR, SOX, HITRUST, HIPAA, ITGC, ISO, PCI DSS, etc.).
- Developed defense in depth and focus strategy, roadmap, framework, and operations management plans (for Cybersecurity and harmonized compliance).
- Established Information Security Office, Charter, Information Security Steering Team, and, Business Advisory Team; developed budget, and, built required information security team.
- Established Information Risk Management framework including operations management plans, policies, and operating procedures (security, compliance and privacy program adhering to effective practices, e.g., NIST, ISO -27001, 27002, and 31000).
- Developed metrics (KRA/KGI/KPI) and executive dashboards, communicated and managed risks.

RESULTS:

- ✓ A mature information security program that enabled the client to pragmatically manage evolving cybersecurity and compliance risks.

