Risk Q

CYBER RISK & PRIVACY MANAGEMENT

Automated Managed Service Third Party Cyber Risk Management

www.risk-q.com

email
info@risk-q.com

Automated Managed Service
Third Party Cyber Risk Management

63% of companies have had a third party cyber event. The cost of a third party cyber event in the U.S. averages $7.5m. Our programs start at $5,000 and save you millions.

Who does Third Party Cyber Risk Management (TPCRM) affect?

Any business is expected to have a TPCRM program if they are a:

- Healthcare company in the United States – HIPAA requires TPCRM
- Companies that process credit card data - PCI requires TPCRM
- Financial Services companies in NYS - NYSDFS Part 500 requires TPCRM
- Companies in scope for privacy regulations: GDPR, CCPA, VDCPA, all require TPCRM

Fines

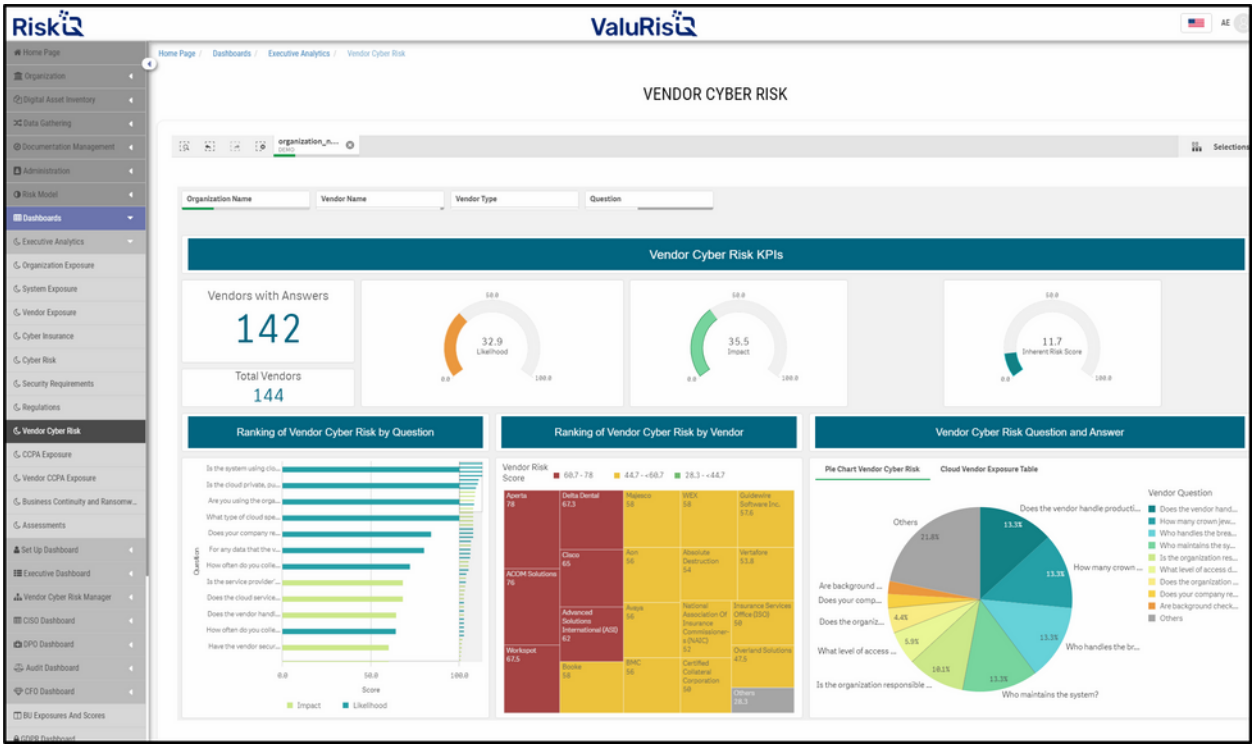
Fines for not having TPCRM in place range from $100 for each record lost up to 4% of annual revenue based on the regulatory scope.

Our Automated TPCRM Managed Service

We provide an automated approach to:

- Contractually manage your vendors
- Identify and prioritize vendors in scope for all your regulatory requirements
- Meet all your TPCRM requirements using our automated assessment with a Risk
- Management Framework like NIST 800-53 or Cybersecurity Framework, ISO 27001 or COBIT
- Rank vendors in scope for risk reduction

- Work with your vendors to provide their third party cyber risk assessments data online
- Audit vendors security controls if needed
- Recommend and prioritize strengthening control gaps for your vendors
- Share data with your business partners if needed



Why RiskQ

RiskQ uses an automated digital asset approach to measure financial exposures and assess cyber risk. This provides clients with objective financial data and eliminates up to 90% of the manual work by untrained personnel to perform the assessment. Clients are provided regulatory requirements/scope, policies, procedures, and automated risk assessments to be compliant with all applicable cybersecurity and privacy regulations. Our platform provides an integrated solution that is powerful, easy to use and offers the lowest total cost of ownership.
In 5 simple steps you can be compliant with any cybersecurity or privacy regulation.

1. **Automated System & Vendor Inventory:** know which systems and vendors are in scope and their priority to assess. **Automated Financial Exposures:** understand malware, ransomware, and regulatory financial exposures.
2. **Get all your policies and procedures reviewed by our Cyber Attorneys.**
3. **Perform Security and Risk Assessments:** using any framework including ISO 27001, NIST, SOC 2, etc. Includes policies, procedures, and a playbook in layman's terms.
4. **Assess Vendor Risk**: make the vendors work for you and provide their assessment evidence in our platform.
5. **Report, Communicate and Act:** use our state-of-art dashboards, reports, and workflows.

About RiskQ

Based on five years of with the Fortune 1000 and cyber insurance industry and from some of the sharpest cybersecurity and risk minds in Israel and the united States. RiskQ provides the ultimate in data loss prevention and risk management by identifying hidden exposures and making sure the attack surface is minimized and the digital assets have effective protection in place. RiskQ fundamentally alters the cybersecurity risk landscape with uits digital asset approach and integrated risk platform. Get our book 'Enterprise Cybersecurity in Digital Business' free with your purchase of our offering.

RiskQ
66 West Flagler Street - Suite 900, Miami, FL 33130
email: info@risk-q.com
www.risk-q.com