WINSTEAD

Cybersecurity

Born in the cloud or not, all businesses are now cloud businesses with preparedness and response the only effective means of mitigating cybersecurity risk. 60% of small businesses experiencing a data breach in 2017 did not survive for more than 6 months. Large businesses are suffering from breach costs in the millions, regulatory fines, loss of consumer trust and widespread organizational disruption.

This is not merely a job for your IT team
The business decisions you make every day have a material impact on your cybersecurity risk posture. Business considerations include contractual liability, vendor due diligence processes, knowing which regulations apply to your business, corporate governance, knowing whether your insurance will cover you based on these considerations, and more. Cyber risk considerations should identify which risks to avoid, accept, mitigate or transfer through insurance, contracting, policies and planning.

It is the primary responsibility of every board of directors to secure the future of their organization – how are you protecting yours?

Not sure where to start? Let us help you assess your business's cyber risk. Our multidisciplinary team focuses on helping your organization assess business risk and set a plan for the future.

Corporate Governance

- Risk planning, including mitigation and transfer strategies
- Best practices for corporate oversight of cybersecurity & compliance planning, policies and activities
- Training on cyber-governance for board members and executives
- Operational & risk guidance on regulatory standards implementation including GDPR, HIPAA, NIST, and PCI obligations and compliance

Cybersecurity Insurance

- Review of cyber-liability and D&O insurance policies in the context of contractual obligations and risks and overall risk profile structuring
- Claim management
- Cyber-liability policy scripting and procurement assistance

Contractual Liability

- Business Associate and IT vendor due diligence including:
  - Best practices training for procurement staff
  - Review and risk profiling of existing agreements; amendments as needed to conform to risk profiles
  - Business Associate obligations for full protection and due diligence
  - Standardized risk management profiles and contractual templates for future use

Data Breach Response Management

- Best practices and breach response planning including war game readiness assessment(s) and practices for Advanced Persistent Threat response
- On-call cybersecurity/data breach response assistance, risk and response advice
- Engagement & oversight of third party forensics to perform systems assessment and response/remediation under protection of privilege