CYBERSECURITY PROFESSIONAL SERVICES

Strategy & Governance, Risk, and Compliance

Organizations need to be armed with appropriate strategies that fit within their company size, risk factors based on industry and company stored data, as well as mandatory regulatory and compliance frameworks.

MorganFranklin Consulting
A Vaco Company

CUSTOM-TAILORED SECURITY PROGRAM STRATEGY AND PLANNING SERVICES

An organization's cybersecurity program is driven by a number of different factors, including internal risk management, regulatory compliance, and brand image. MorganFranklin helps companies to develop and implement strategies to build cybersecurity programs that meet their unique needs.

ADVISORY TO EXECUTIVES AND BOARDS

MorganFranklin offers access to cybersecurity subject matter experts. These advisors help boards to calculate the impact of cybersecurity on their brand and inform strategic development.

FINANCIAL AND BUSINESS PLANNING

Quantifying the impacts of cybersecurity investments can be challenging. MorganFranklin advisors aid information security teams in building budgets and demonstrating return on investment for cybersecurity programs.

STRATEGY DEVELOPMENT

A proactive approach to security minimizes potential risk and cost to the organization. MorganFranklin professionals bring deep experience in assessing current state capabilities, designing target state operating models, deploying, and managing cybersecurity programs.

vCISO SERVICES

A CISO brings strategic and tactical cybersecurity expertise to an organization. MorganFranklin's virtual CISO services provides access to a team of specialists, selected to meet an organization's unique needs.

Creating business-aligned strategies that improve overarching decision making abilities

OUR APPROACH

Flexible, Scalable Offerings

Select only the services needed to meet your organization's specific requirements. Add on or scale back as your security program evolves.

Paired with Consulting Expertise

We bring business driven and industry specific guidance to address your unique security challenges.

End-to-End Solutions

We offer end-to-end solutions in all areas of cybersecurity including planning, strategy, execution, supervision, and maintenance.

GOVERNANCE, RISK, AND COMPLIANCE + ENTERPRISE RISK MANAGEMENT

Managing risk is a primary goal of an organization's cybersecurity program; however, cybersecurity risk can originate from a number of different sources. MorganFranklin helps organizations identify, triage, and manage their cybersecurity risks.

THIRD-PARTY RISK MANAGEMENT

No company operates completely in a vacuum. Most organizations are dependent upon external parties in more ways than they are aware. Identifying these external dependencies and analyzing the associated risk is essential to enterprise cybersecurity and business resilience.

Third-Party Risk Assessments

The use of external contractors for data storage, processing, and other services is common across all industries. MorganFranklin can help to identify these vendor relationships and the cybersecurity, compliance, and business resilience risks associated with them.

Network Access Management

Most organizations allow partners, vendors, and service providers access to their internal networks. MorganFranklin advisors can help develop policies and controls to minimize the risks associated with this external network access.

Third-Party Code Vulnerability Management

Software commonly includes libraries and other dependencies that can contain vulnerabilities or restrictive licensing agreements. Generating a complete software "bill of materials" is essential to managing the associated cybersecurity and legal risk.

Supply Chain Risk Management and Resilience

Companies rely on a web of suppliers and vendors to support their core business functions. MorganFranklin helps companies to identify critical interdependencies and minimize the risk of business disruption.

CYBER POLICY AND FRAMEWORK DEVELOPMENT

Companies have both internal and external drivers for cybersecurity, including regulatory compliance, data breach avoidance, and legal requirements. Failing to meet these responsibilities can result in regulatory penalties, legal suits, and reputational damage.

MorganFranklin can help develop cybersecurity frameworks and policies that enable an organization to meet the requirements of applicable regulations and protect company systems and sensitive data. This includes support for every stage of the planning process from an initial needs assessment to prioritizing the implementation of security controls.

BUSINESS CONTINUITY, CYBER RESILIENCE, AND CRISIS MANAGEMENT

In addition to physical events, cyber attacks can severely impact operations. Distributed Denial of Service (DDoS) attacks impact customer communications, ransomware denies access to critical data and systems, and other attacks can result in expensive and time-consuming investigations.

MorganFranklin advisors assist in developing operational resilience, business continuity, technology resilience, and disaster recovery strategies to minimize impacts, maintain critical operations, and rapidly recover business and technology operations in the event of disruptions.

SECURITY AWARENESS, TRAINING, AND COMMUNICATIONS

The human element is an essential component of an organization's cybersecurity strategy. Cybercriminals use phishing and social engineering attacks to attempt to breach a company's defenses, and, during an incident, responders must be capable of acting rapidly and correctly.

MorganFranklin can assist in designing and implementing cybersecurity training and awareness programs. Training can incorporate both cybersecurity awareness training for the workforce, as well as specialized simulations and exercises to improve incident response effectiveness.