The Corporate Cyber Conundrum

The frequency and complexity of reported Cyber events, including an increase in regulations, economic outlook, and competition, are placing significant demands on firms' budgets and resources. With an increased focus on Cybersecurity, Boards are demanding a coherent and compelling Cyber strategy as a part of their annual growth plans. This includes more robust evidence between the annual Cyber spending and the firms' Cyber risk posture.

Meanwhile, CISOs are constantly adjusting to the latest industry trends around threats, risks and controls, competitive business priorities, impossible workload, and a constant demand for additional spend on people. Little-to-no effort is spent creating the right level of documentation that would ensure investment decisions are data-driven and the value is measurable as controls are implemented. The SOC (Command Centers), the focal point of most Cyber strategies given its prominent operational role and visibility to the business, become the source for controls implementation at the expense of delivering other controls that have the potential to create sustainable value to the business. This analogous to investing in ambulances rather than hospitals.

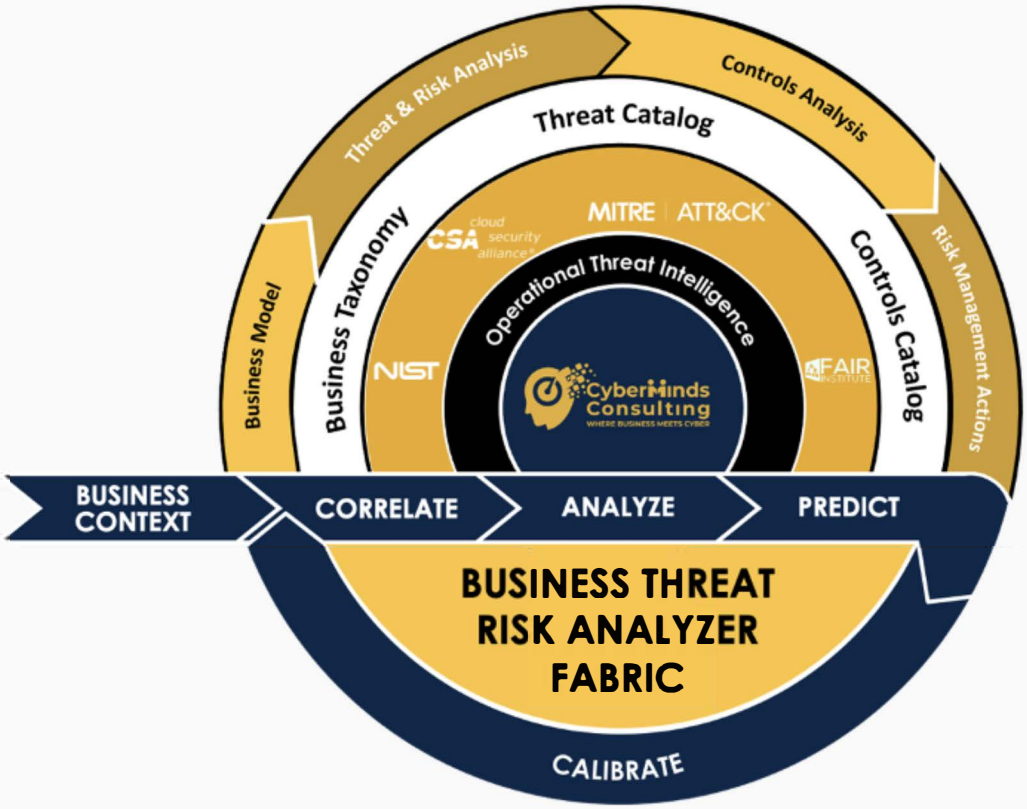
The events of 2020 have ushered in a new era of unavoidable imposition on how firms conduct their daily business, such as enabling remote work and boosting their digital presence. This further shifts CISO (and CIO) priorities by forcing them to take proactive, modern approaches to risk-based accesses promoted by concepts like Zero Trust and Micro-Segmentation.

Cybersecurity teams do not have a carte blanche. Every dollar spent needs to be objectively accounted for as it comes at the expense of other corporate investments.

We, at CyberMinds Consulting, believe organizations can seize this as an opportunity to modernize their security architecture blueprints and investments. CyberMinds Consulting can help contextualize your security plans so you can make smarter, quicker, and actionable decisions when it comes to securing your critical workloads - no matter where they reside.

What Can CyberMinds Consulting Do For You?

Our proven, data-driven framework and context-driven methodology can improve the accuracy and confidence in firms' Cyber budget by securing the most crucial aspects of the business, first.



Unlike the traditional approaches that focus on operational tools and technologies for visibility and decision making, our framework brings a unique, holistic, and structured approach by correlating business taxonomy, threats, risks, and controls into a measurable, traceable, and predictive outcome. Built on the industry's best practices and standards, firms can perform end-to-end analysis and a simulation of threats, risks, and controls across the entire business stack to focus on reducing the most significant risks.

The framework is delivered through our time-boxed methodology (~13 weeks) to ensure Business contextualization of your Cyber plans with accelerated progression from current state analysis to design and execution planning. CyberMinds Consulting will:

1. Validate what you already have and contextualize it with out framework for improvements.
2. Facilitate a shared Corporate Dialogue between the Business, Cyber, and Technical teams to make informed and justifiable investment decisions.
3. Create a documented baseline with a traceable and measurable linkage between technology implementations and business value.

What We Offer

Cybersecurity Strategy Revitalization

Creating a Cybersecurity strategy that remains alive and relevant to the Business during these challenging times is one of the biggest conundrums facing CISOs today. Our methodology ensures that revenue leaders and CISO teams can efficiently identify what is mission-critical to the Business and focuses on the actual threats and risks that must be managed to ensure Business security. We combine Business Architecture and Cyber Threat catalogs in a proven methodology that aligns all stakeholders on a standardized set of security goals.

Data Security

Your Company's data is one of its most critical assets. Maintaining the integrity, confidentiality, and availability of this data is life or death for the Company. How can you effectively manage this challenge while facing the exponential proliferation of structured and unstructured corporate data content? We, at CyberMinds Consulting, have lived your pain and will help you plot an efficient path to confidence in security through our 'Data Democratization' methodology.

Cloud Security

As Enterprises continue to modernize their workloads by adopting hybrid multi-cloud environments, they often find themselves at a crossroads when making decisions around its enterprise security: whether to expand their current enterprise-class security investments to the cloud, invest in cloud-born security capabilities, or find a compromise between the two. While speed and reliability are becoming increasingly critical for business success, Cyber teams continue to play defense amid the evolving threats landscape, traditional best-of-breed security solutions mentality, cyber skills shortage, and snail-paced security vendor roadmap rollouts. C ISO teams can seize this as a fresh opportunity by taking a novel look at their security architecture blueprints and investments.

Applied Cyber Risk Management

Ever felt like the Corporation cycles through endless discussions on theoretical risk posture and ultimately spend more time documenting and aging risk topics rather than remediating the actual issues? The CyberMinds Consulting 'Applied Threat and Risk Management methodology and toolkit' helps Cyber teams focus on real-world business-relevant threats and provides prescriptive guidance on the steps needed to measure and mitigate risks within agreed tolerances effectively.

Why Us?

Our Credible Experience: The managing members of CyberMinds of Consulting have decades of experience in delivering complex Technology and Security transformation programs across industry sectors. Their diverse industry perspectives and operational contexts have uniquely positioned them to help Enterprises achieve a practical balance between safety, resiliency, and revenue by focusing on practical, risk-based techniques for smarter, quicker, and actionable decisions for securing digital workloads - no matter where they reside.

Our Values: In addition to the work, we help clients in strengthening their security posture. Additionally, we work closely with our local community to ensure that we are making real contributions to help individuals and businesses.

We have developed strong partnerships with local colleges to offer career development, mentoring, and internship/externship opportunities to students that include on the job training.

We donate a significant percentage of our revenue to offer free services to local non-profit organizations to ensure they benefit from our capabilities.

Our Intellectual Assets: Our proven, industry-relevant frameworks can help organizations focus on securing the critical aspects of the corporation, first, by integrating business, operations, technology, and cyber considerations into a single, integrated enterprise view.

Our Offerings: At a fraction of the price charged by the large consulting firms, CyberMinds Consulting will bring high-tough, functional, and affordable expertise with simple, fixed-priced engagements with total clarity on roles, responsibilities, and outcomes. Unlike our peers, we are transparent with 'what' you need to do and provide a complete insight into 'how' to execute successfully.

Contact Us:

+1 (855) 945 - 1970

www.cybermindssolutions.com

benazeer.d@cybermindssolutions.com