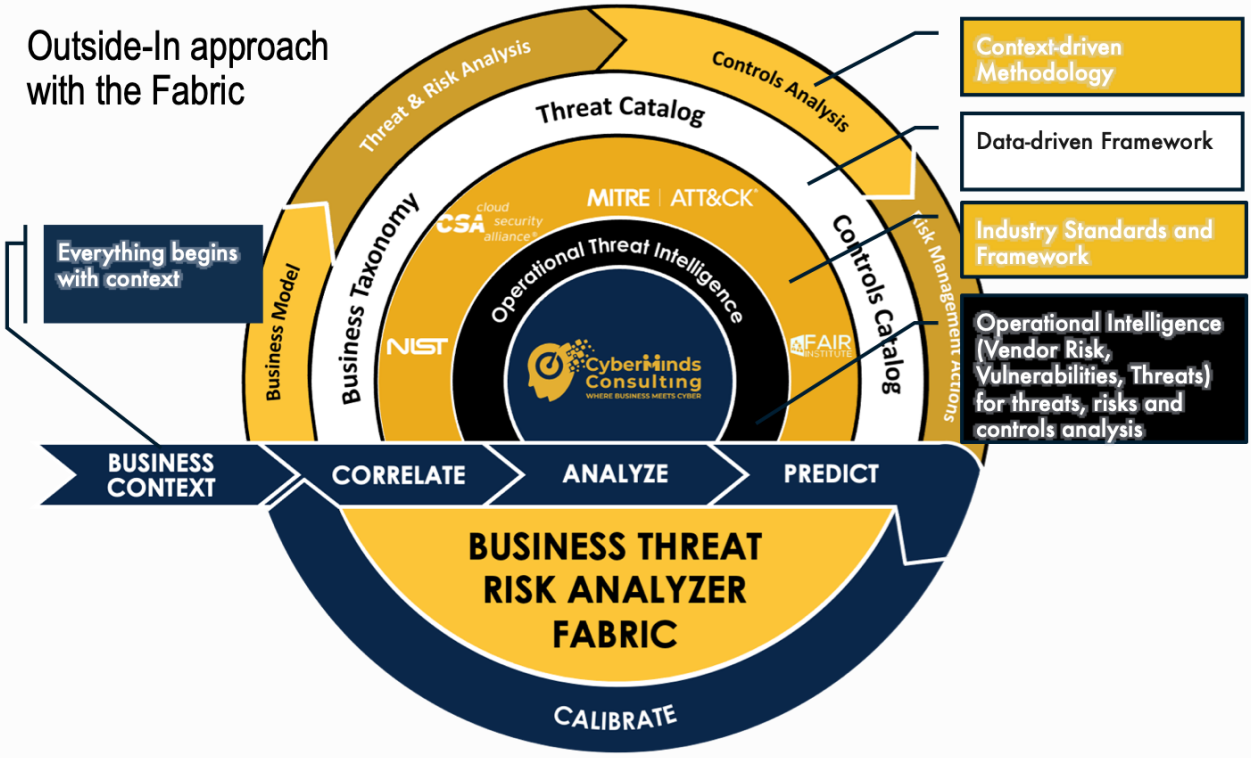
CyberMinds Consulting's Business Threat Risk Analyzer Fabric

Whitepaper Version 1.0
June 2021

CyberMinds Consulting
WHERE BUSINESS MEETS CYBER

Introduction

CyberMinds Consulting's Business Threat Risk Analyzer Fabric provides a unique approach by combining Context-driven Methodology and a Data-driven Framework to help Enterprises make smarter investment decisions for the safety and resiliency of their most valuable assets. It brings a risk-focused approach by tying critical business functions to the underlying assets for proactive threat analysis and controls mitigation.



(Meta-)Data-driven Framework

The Data-driven Framework is made up of pre-built assets and accelerators. These assets are contextualized and operationalized by the Fabric's Context-driven methodology. The data-driven framework integrates business, operational, technology, and cyber considerations into a single integrated enterprise view.

The Core Accelerators within the Framework include:

1. **Business Taxonomy** encapsulates a business glossary of meta-data and templates that capture crucial business functions and processes across industry verticals. It provides a standard baseline nomenclature for defining business architecture components that link critical business activities to underlying applications and infrastructure within an Enterprise.
2. **Threat Catalog** is a repository of historical and latest attack vectors categorized by industry vertical and pre-defined meta-data. The catalog maps attack vectors to threats, business impact, and risks for consequence analysis and control mitigation. It also includes references to the MITRE ATTACK TTP where relevant and available.
3. **Controls Catalog** is a rationalized list of controls derived from best-practices frameworks such as NIT and Cloud Security Alliance (CSA). The catalog is categorized by use cases such as Zero-Trust, Ransomware, Supply Chain, to name a few. The controls are further broken down into operational, tech, cyber & third-party controls to encourage a shared responsibility model between Business, Technology, Cyber, and Third-Party Providers.

Context-driven Methodology

The Context-driven Methodology operationalizes the data-driven framework by infusing business context based on custom inputs from the Enterprise.

The Business Context is derived from current and existing artifacts and documents within the Enterprise. These may include.

1. Corporate priorities and Business Strategy,
2. Critical Business Activities and Processes as defined within Disaster Recovery and Business Continuity Planning
3. Technology and Cyber Strategies
4. Security Assessment, Maturity Models (if applicable)
5. Cyber Controls Implementation Plan
6. 3rd Party/Vendor Management Processes
7. Governance, Risk and Compliance Management Plans

The Objective is to have a documented understanding of current organizational practices for Cyber considerations and their linkages to critical business and technology functions. It also provides insights into the current level of maturity of cyber thinking within the organization. It creates an opportunity to endorse actions that add value and identify potential opportunities for reprioritization and new work.

Activities within the Methodology include.

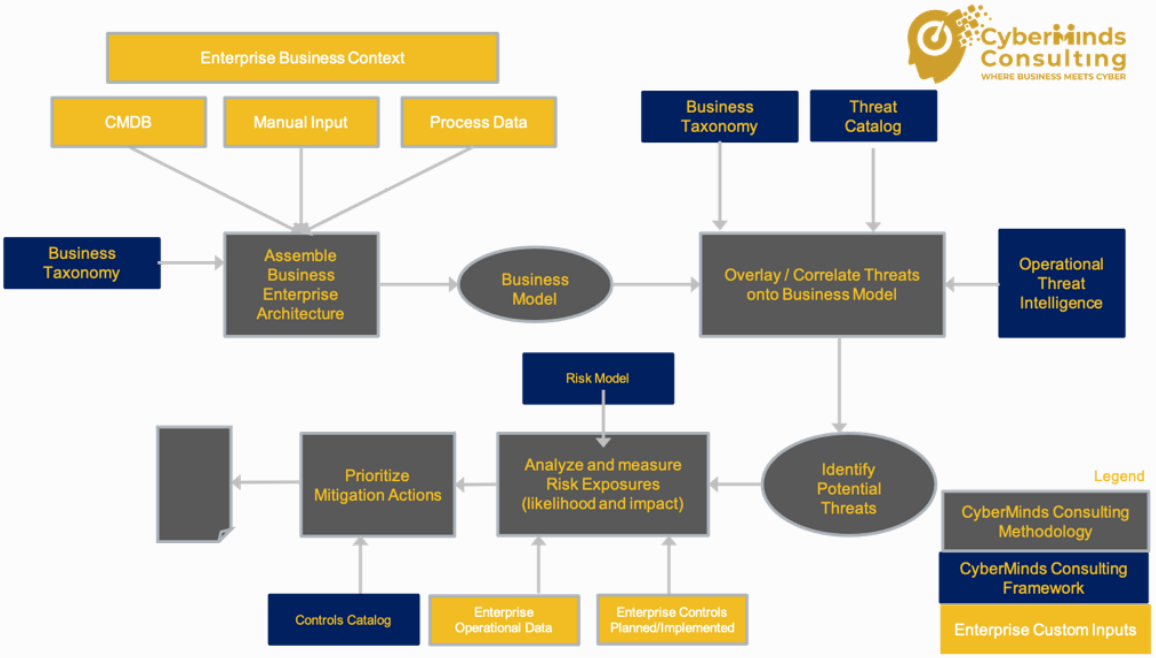
1. Business Architecture Model: Documented business enterprise architecture shows how the critical business process links to software and data and ultimately to infrastructure. Existing corporate data (CMDB, Asset Tables) is leveraged wherever applicable in a very pragmatic way. Each of these data assets can be created from existing corporate data embellished with manual updates. Focus is not to be perfect but "good enough."
2. Threat and Risk Analysis: This is a 2-step process.
    a. Threat Analysis: Overlay the Threat Catalog on the Business Architecture to identify the potential exposures. In addition to the historic breach analysis on the business architecture component, this step relies on real-time data from Threat Intelligence platforms to assess the ongoing vulnerabilities, vendor risks, and threats to the business components identified in the business architecture model.
    b. Risk Analysis: Includes assessment and quantification of risks for the identified threat exposures based on their likelihood of occurrence within the organizational context. The method leverages quantitative risk model concepts promoted by the FAIR Institute. It uses common-sense techniques by quantifying Cyber risks as a function of business risks (Operational, Reputational, Financial, Regulatory). The analysis is done for each threat category, leveraging organizational, operational data (if available), in addition, to data curated by CyberMinds Consulting from publicly available artifacts such as Verizon Data Breach Investigation Study, IBM's Cost of a Data Breach Report, and other credible industry sector-specific breach and threat studies. The focus is not to be perfect but good enough for guided decision-making around cyber investments.
3. Controls Analysis: Based on the Threats and Risk Analysis, appropriate controls and mitigation techniques are identified and prioritized based on efficacy and

impact on the firm's overall risk posture. This step also reviews the Organizations' current controls plan and roadmap to identify gaps or eliminate controls already in place. Leverages Controls' Catalog for a detailed view into the Operational, Cyber, and technology Controls required to mitigate identified risks (Step 2b).

4. Risk Management (Mitigation) Actions: The controls analysis feeds into the Execution plan for a prioritized and executable list of controls that firms need to implement to gain visible benefits within a shorter time frame and get the most value out of Cyber Investments. The controls are marked as operational, technology, and cyber to enable cross-functional collaboration and shared responsibility between Business, Technology, and Cyber leaders.

Fabric Execution Process

Unlike the traditional approaches that focus on operational tools and technologies for visibility and decision making, the Fabric 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 process is delivered over time-boxed 13 ~ 15 weeks or shorter depending on the agreed-upon scope. It is primarily designed to ensure accelerated progression from current state analysis through design and execution planning.

CyberMinds Consulting's Engagement Delivery Approach

CyberMinds Consulting is dedicated to working with companies that demonstrate a strong desire to seek help as they improve. The goal is not to create a Cyber strategy from the ground up but work with what Enterprise has and make it better. The process is delivered within a time-boxed delivery approach to ensure involved stakeholders are focused on achieving the agreed outcomes urgently from Day 1 of the engagement. Before the arrangement, the team is transparent with the internal stakeholders on the results, who needs to be involved, when they need to be involved and what decisions will need to be made.

PHASE	Pre-Engagement				Current State			Business Review			Strategy Re-design				Buy-in/Closure			Post-Engagement			
WEEK	-1	-2	-3	-4	1	2	3	4	5	6	7	8	9	10	11	12	13	+1	+2	+3	+4
ACTIVITIES	✓ Review overall engagement plan and outcomes ✓ Review and finalize engagement model and key roles ✓ Review critical business activities and narrow down potential top 5-10 ✓ Preview existing cyber strategy plans and documents ✓ Agree financial and NDA logistics				✓ Review & initial feedback of existing / current cyber plans and strategy documentation ✓ Finalize of critical business activities (CBA) ✓ Initial enrichment of Functional Model for each of the critical business activities			✓ Working sessions with Business, Technology and Cyber to enrich architecture content & business risks ✓ Identify potential business, technology and cyber controls			✓ Working sessions with Tech. & Cyber teams to agree control solutions to prioritized risks and threats ✓ Identify initial opportunities to add / replace / update current cyber plans ✓ Finalize design of control solutions that provide the greatest return on investment within the CBA scope				✓ Working sessions with Business, Tech. and Cyber teams to validate / correct proposed solutions & plans ✓ Working sessions to agree impact of controls ✓ Finalize cyber strategy and delivery plans ✓ Finalize control impact assessment			✓ Post engagement follow up calls to ensure deliverables continue to resonate and meet client expectations ✓ SLA driven responses to open questions and follow ups			
OUTCOME	✓ Entry Criteria Met				✓ Current State Assessment ✓ Business Priorities Agreed			✓ Business Architecture ✓ Threat Assessment			✓ Strategy Re-stated ✓ Execution Plan ✓ Revised Risk Review				✓ Stakeholder Buy-in ✓ Delivery Planning			✓ Post Engagement Questions / Follow-Ups			

1. CyberMinds Consulting will review existing strategy and planning artifacts and create delivery capacity by eliminating low-value activities and replacing them with solutions directly traced to a critical business need.
2. Once the current state analysis is completed, we work closely with the CISO, CIO, and Business teams to identify a small number of key business activities which are operationally critical.

The remainder of the time is then spent ensuring that actions are in place to address any threats and risks that can potentially inhibit the resilience of these activities. These are not limited to cyber and technology, but operational, technology, and cyber threats can be identified in a single conversation through our visualization techniques.

1. At all stages of the project, the discussions and decisions are limited to the topics that are real and relevant and avoid generic threads that cannot be actioned.
2. At all stages of the project, we limit discussion and decisions to accurate and relevant topics and avoid generic threads that cannot be actioned.
3. CyberMinds Consulting will work collectively with the Business, Technology, and Cyber leaders to ensure all topics are grounded in a clear link to critical business activities. Industry-relevant templates will ensure that design and delivery planning concentrates on tangible outcomes that add value to the business.
4. Our methodology is supported by industry-specific frameworks such as NIST and CSA with templates that ensure a consistent starting point to each aspect of the project. These templates are validated and enriched after every engagement to keep our assets current and continuously improving for each Industry sector.

According to [PwC's Global Digital Trust Insight 2021 survey], more than half of Tech and Security executives surveyed lack confidence that Cyber spending processes are aligned to mitigate the most significant risks.

As Enterprises continue to digitize, the undeniable need for increased Cyber often spends at the expense of other corporate investments. This dilemma requires a novel approach to ensure that every dollar spent is objectively and proactively accounted for towards securing the most vital assets, and data-driven evidence between cyber spending and the firms' risk-posture is documented.

CyberMinds Consulting's Business Threat Risk Analyzer Fabric can super-charge the accuracy and confidence in Cyber investments by re-aligning your security controls backlog with up to 70% risk reduction at the same or a lesser cost. In other words, using a framework like ours, every dollar spent on Cyber can avoid 70c in inherent risks.

At a fraction of the price charged by large consulting firms, CyberMinds Consulting brings a lean, high-touch, fixed Price engagement model that can help you focus on securing the essential aspects of the business. Unlike our peers, not only will we share with you 'what' you need to do, but we'll also provide complete insight into 'how' to execute successfully. CyberMinds Consulting will revitalize your Cyber plans.

1. Validating what you already have, contextualize it, and make it better.
2. Facilitating a Shared Corporate Dialog between the Business, Cyber, and Technical Teams for informed and justifiable investment decision-making and finally.
3. Creating a documented baseline with a traceable and measurable linkage between technology implementations and business value.

Contact Us:

+1 (855) 945 1970.

www.cybermindssolutions.com

Email: benazeer.d@cybermindssolutions.com
