ARE YOU BEING CHALLENGED IN THESE AREAS?

1. Quantifying and qualifying the value of cybersecurity investments
2. A methodology for leveraging non-technology and non-cybersecurity projects and initiatives towards sharing the investment in cybersecurity
3. Advancing the dialogue with CxO, and getting a seat at the table to establish priorities from a cybersecurity lens
4. Switching the burden of responsibility from 'completely IT' to a shared and distributed role with the rest of the enterprise
5. Positioning cybersecurity within a valuation methodology that allows for progress to take place measurably and predictably
6. Understanding cybersecurity within the company's ecosystem, towards creating redundancies and efficiencies with contextual significance
7. From PR to cyber-insurance, folding in all aspects of incidents and breaches through a business lens and converting that into a philosophy of acquisition

OUR CYBERSECURITY PROGRAM HELPS YOU

- Develop a Value-Based Cybersecurity Program that purposefully and meaningfully engages Business Stakeholders, in order to maximize the worth of every cybersecurity investment, and realize benefits, revenue, and profit from its processes and technologies
- Develop an Information Security Skills-Transfer Program that fosters a Value-Based Business Approach, where methodologies bridge the cybersecurity talent on-site, with the most important and relevant business practices of the customer's industry. This yields a seamless communication and understanding of the expectations of the business with regards to the investments in cybersecurity.
- Integrate CEO + Board engagement to create a Governance structure that mitigates risks
- Create the ecosystem of cybersecurity that incorporates external partners and business strategy, focusing on the 'intelligence' of your enterprise
- Prepare for customer & shareholder response, by proactively aligning GRC measures with PR best practices, in case of a breach
- Proper integration of GRC
- Proper integration of records management

THE RESULTS

- A robust cybersecurity ecosystem that contains redundancy and shared responsibilities.
- A culture that has cybersecurity embedded in it, and proactively engages in threat management
- Initiatives are guided through cybersecurity
- Cybersecurity becomes integrated into the enterprise --- all activities factor Cybersecurity requirements

PAST PERFORMANCE

- Development of cybersecurity programs affecting 4.5+ million customers, 75,000+ employees & 500+ departments

DELIVERABLES

Focus Area	deliverable
Benchmark Assessment	'As Is' Report
Roadmap Development towards improvement in 2 advisories areas mentioned above	Roadmap with Summary notes for Action Plans
Business-Based Ranking and Prioritization of Action Plans	Value-Based Map with business based ranking and prioritization
Communication Plan	Action Plan 1: working backwards from PR to the cyber core
Alignment with PMO, PgMO, etc	Action Plan 2: Procedures for seamless interaction with PMO initiatives (present and future), creating persistent inclusion of cybersecurity approaches in every project
Alignment with Procurement Office	Action Plan 3: Procedures to infuse a persistent layer of cybersecurity requirements within every contract
Elevate caliber of Vendor Partnership	Action Plan 4: Documented results of interviews with vendors, towards improving the partnership and extracting greater benefit from existing and upcoming transactions
Maximizing cyber-insurance	Action Plan 5: Documented results of interview with cyber-insurance and next steps towards maximizing policy benefits