Summary Scorecard: 8. Cyber Security Operations

Perspective	Cybersecurity Function	Measure / Initiative
Y Administrative	R Finance	R F1. % of IT budget allocated to security
		Y F2. Budget vs. Actual Spend
	G HR, Awareness & Training	G HR1. % of Employees who read, acknowledged and tested on the security policy
		Y HR2. % of Employees with thorough background checks
		G HR3. % of Workforce Completed Annual Security awareness training
	G Insurance	G I1. # of Cybersecurity Claims
		Y I2. Cost of Cyber Insurance
		G I3. Sufficient Insurance Acquired to Substantially Cover Cybersecurity Risk Exposure
	Y Legal	Y L1. % of Material Contracts Evaluated by Security Team
Y Operational Cybersecurity	R Application Security	R AS1. % of Apps that are Critical Applications
	Y Asset & Data Security	Y AD1. Existence of an IT Asset Management Database (ITAM)
		G AD2. % of Information Accurately Classified (Data classification Standard must exist)
		R AD3. % of Known assets & "systems" accounted for in ITAM
		G AD4. % of Systems with Critical Data that is Encrypted at Rest and In Transit
	G Configuration & Patch Management	Y CP1. % of Major Systems (HW & SW) still supported by Manufacturer or validated 3rd party
		G CP2. % of Major Systems (HW & SW) upgraded to latest version
		G CP3. % of Systems Patched within 30 Days of critical security updates
		G CP4. Mean Cost to Patch
		G CP5. Mean Time to Patch
	Y Identity & Access Management	Y IA1. % of critical capabilities (servers, firewalls etc.) and remote connections that use MFA
		Y IA2. # of Users with Super User Access
		R IA3. % of accounts that have abnormal inactivity
	G Incident Response	G IR1. # of Incidents
		G IR2. Cost of Incidents
		G IR3. Business Impact Assessment exists
		Y IR4. Incident Plan exists and Reviewed by Management
		G IR5. Time Since IR Plan was Tested

Perspective	Cybersecurity Function	Measure / Initiative
Y Operational Cybersecurity	G Incident Response	Y IR6. Mean time between incidents (Days)
		G IR7. Mean time to respond
	Y Insider Threats & Detection	G TH1. # and type of Cases Opened
		Y TH2. # and type of risk mitigating actions
		Y TH3. # and types of cases escalated internally and triaged within the organization
		Y TH4. # and types of referrals to external law enforcement agencies
		G TH5. Mean Time to Detect /Incident Discovery
	Y Recovery	R R1. Existence of Management Approved Disaster Recovery Plan
		G R2. Time Since Last DR Plan Test (Days)
		G R3. Number of High Risk Business Processes with Critical RTOs
		R R4. Mean Time to Restore (MTTR)
		R R5. Mean Incident Recovery Cost
	Y Supply Chain - Vendor/Partner Management	G SC1. # of Vendors with Access to Critical Enterprise Systems
		Y SC2. % of Material Vendors who have been Audited either directly or Via 3rd Party
		R SC3. % of Vendor Relationships that participate in quarterly reviews
	R Vulnerability Management	R VM1. % of Systems with No Known Severe Vulnerabilities
		R VM2. Mean Time to Mitigate Vulnerability