NIST Cybersecurity Framework

Summary for C-Level Executives

Art Jacoby LLC art@artjacoby.com

IDENTIFY	**Develop institutional understanding to manage cyber risk**
Asset Management	inventory, map & prioritize devices, software, info & communication systems; assign roles
Business Environment	business priorities & resilience requirements established considering supply chain dependencies
Governance	establish policy, roles/responsibilities including legal and regulatory requirements
Risk Assessment	asset vulnerabilities identified/documented; impacts analyzed; risk responses identified
Risk Management Strategy	organizational risk tolerance determined & policy set
PROTECT	**Implement appropriate safeguards**
Access Control	secure/manage identities, credentials, permissions, physical & remote access & network integrity
Awareness & Training	Train users and establish roles/responsibilities
Data Security	Data at rest, in motion, intellectual property, personally identifiable info (PII) secured
Information Protection Processes/Procedures	Baseline IT/operational technology & system development lifecycle plan developed; policies for backup, configuration change control, physical operating environment & information sharing established; response plans created for business continuity, incident response and disaster recovery
Maintenance	maintenance/repair of assets performed/logged using secure methods
Protective Technology	audit/log records kept; access to critical assets and systems controlled
DETECT	**Identify occurrence of cyber events**
Anomalies & Events	establish baseline & impact thresholds; analyze source/type of attacks; evaluate potential impacts
Security Continuous Monitoring	monitoring of network, physical environment, personnel, service providers & unauthorized resources; detect malicious code & unauthorized mobile code; perform vulnerability assessments
Detection Processes	roles, responsibilities established; detection conducted; incidents communicated
RESPOND	**Take action regarding detected cyber events**
Response planning	implement response plan
Communications	incidents communication is consistent with criteria to appropriate stakeholders
Analysis	events analyzed to understand source & impact and forensics conducted
Mitigation	incidents are contained & eradicated
Improvements	plans/strategies updated with lessons learned
RECOVER	**Restore capabilities/services/data & reputation**
Recovery Planning	recovery plan is executed
Improvements	plans/strategies updated with lessons learned
Communications	manage PR; repair reputation