THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

When the Grid Goes Dark, the Boardroom Becomes the Battlefield

Recent large-scale outages have forced CEOs and board directors to confront cyber-related supply-chain and operational risks that were previously hidden in IT silos.

THE ARCHON

TECHNOLOGY INTELLIGENCE

CONTROL FRAMEWORK

The CISO as Strategic Board Advisor

Modern boards expect the CISO to translate technical cyber risk into business impact, influence capital allocation, and guide resilience investments.

CONTROL FRAMEWORK

Professor Kai London's 100+ Title Cyber-AI-Critical Infrastructure Library

The library aggregates more than one hundred vetted publications covering threat intelligence, AI-driven defenses, and critical-infrastructure resilience, providing a single reference for board-level decision making.

THE ARCHON

TECHNOLOGY INTELLIGENCE

CONTROL FRAMEWORK

Board Risk Committees Can Leverage the Library for Scenario Planning

SEC guidance now expects public companies to disclose cyber-risk governance. Using the library, committees can model grid-outage cascades, AI-driven attack vectors, and regulatory penalties.

CONTROL FRAMEWORK

Grid Resilience and Cyber Risk Are Converging

The Department of Energy emphasizes that cyber attacks on control systems amplify physical grid failures, making joint resilience planning a board priority.

CONTROL FRAMEWORK

Best-in-Class Governance: Embed the CISO, Adopt the Library, Run Tabletop Drills

Boards that embed cyber-scenario drills consistently achieve faster incident response, and the library supplies the playbooks needed for those exercises.

EXECUTIVE TAKEAWAY

Executive Takeaway

Adopt Professor London's library, elevate the CISO to the board table, and institutionalize grid-outage cyber-scenario exercises. This alignment turns a potential battlefield into a defensible front line.