MYTHOS EXPOSED YOUR INFRASTRUCTURE

What Every CIO Must Know About IT, OT, and the New Cybersecurity Imperative

May 2026

Galent

1. **Frontier AI is no longer just a productivity multiplier - it is an attack accelerant that most CIOs have not yet fully priced into their planning.**

2. **$2.5 trillion in U.S. IT and OT assets are exposed, with upgrade costs running to $1.0 trillion.**

3. **The chips needed to close the gap are sold out through 2027.**

4. **Migrating the bulk of your compute to LLM-ready, secured cloud infrastructure will need to accelerate significantly**

> **This is not a projection, these risks are already materializing. Here is what you need to know.**

WHAT THIS MEANS FOR THE WORLD

Anthropic's unreleased model, Mythos, identified thousands of high-severity vulnerabilities across every major operating system and browser, including flaws that survived decades of human review and millions of automated security tests. The cost, effort, and expertise required to find and exploit software vulnerabilities have dropped dramatically. What once required a nation-state actor now requires just one individual and a prompt.

Agentic AI makes this worse. These systems do not just discover vulnerabilities. They autonomously plan, select tools, and execute multi-step attacks with minimal human involvement. The attack loop has compressed from weeks to hours. But defenders are still operating on human timescales.

The structural asymmetry is now permanent: attackers iterate faster than defenders can patch. Global cybersecurity software revenue hit $140 billion in 2025 and is projected to reach $270 billion by 2030. 63% of organizations still report insufficient cyber-resilience. Even this accelerated spending will be minuscule compared to the vulnerabilities Mythos exposed.

IT VS. OT: TWO VERY DIFFERENT PROBLEMS

VS

IT Systems:
Large, Manageable, but Not Immune

U.S. IT assets total $2.5 trillion. About 20% are unpatchable. Most IT failures can be resolved through patching, reimaging, or workload redistribution. Replacement exposure sits at roughly 20% of the asset base, concentrated in enterprise software complexity and end-user device patchability gaps.

The real IT risk in a major attack is not hardware, it is semiconductor supply. A nationwide cyberattack would generate $145 billion in chip demand against a market already operating at capacity. End-user devices drive 66% of that demand. TSMC's 3nm capacity is booked through 2027. Recovery within six to twelve months would be physically impossible.

OT Systems:
Smaller, Far More Dangerous

U.S. OT assets total $1 trillion. 50% are unpatchable. This is not a software problem. It is a structural one. A programmable logic controller installed in 2005 may still be running today with vendor support that ended in 2018. Patching OT often means halting production lines, interrupting utility services, or triggering safety recertification. Organizations do not do it. The vulnerabilities accumulate.

OT replacement costs run 1.7x asset value versus 1.5x for IT. In a system-wide attack, direct OT losses alone are estimated at $500 billion. The sectors most exposed are exactly the ones you cannot afford to take offline: energy grids, industrial manufacturing, rail signaling, air traffic management.

The chip problem for OT is different from IT. OT depends on microcontroller units and analog/power components produced on mature nodes, where capacity expansion is slow and underprioritized. A major OT attack would represent a near 50% shock to global Microcontroller Unit supply. That shortage does not resolve in months. It resolves in years.

WHERE YOUR INDUSTRY SITS

Industry	Primary OT Exposure	Patchability	Cascade Risk
Energy / Utilities	Grid, transmission control, SCADA systems	25-50% unpatchable	National. A single breach cuts power to regions.
BFSI	Data centers, ATM networks, core banking IT	~20% IT unpatchable; OT minimal	Systemic. Synthetic identity attacks already at scale.
Manufacturing	PLCs, industrial controllers, process systems	45-50% unpatchable; highest legacy density	Sector-wide. Production halts ripple through supply chains.
Transportation	Rail signaling, ATC, fleet management systems	30% replacement exposure; better than industrial	Public safety. Rail and air control system failures affect millions.
Healthcare	Medical devices, imaging systems, clinical IT	High legacy; safety recertification blocks patches	Critical. Device compromise directly endangers patients.

WHAT TO AUDIT RIGHT NOW

Start with what you cannot fix. Before investing in new tools, map your unpatchable assets. There are several useful reports available on this, and they give you the right lens: separate patchable, non-patchable (end-of-life), and truly unpatchable (no update mechanism). Your OT inventory almost certainly contains all three categories. Most organizations do not have this map.

A OT Inventory

Inventory OT systems by vintage, vendor support status, and patchability classification.

B Identify Legacy

Identify any PLCs (Programmable Logic Controllers), SCADA (Supervisory Control and Data Acquisition) components, or industrial controllers running on hardware more than 10 years old.

C Chip Exposure

Map IT assets for semiconductor content concentration, particularly end-user devices and data center systems that would require hardware replacement in an attack scenario.

D Identify Risk

Assess identity infrastructure. Synthetic identity attacks will affect 80% of organizations by 2027. If your identity verification is perimeter-based or periodic rather than continuous, you are already behind.

E AI BoM

Review your AI bill of materials. By 2027, 60% of enterprises deploying agentic AI will need a structured inventory of models, training data, code, and infrastructure. Start building that record now.

WHAT TO DO NOW

Fight AI with AI

Manual alert handling cannot match AI-driven attack velocity. The operational answer is full automation of security operations. By 2028, AI agents are projected to triage 80% of SOC alerts. Organizations that do not invest in this capability now will face an unbridgeable gap. Automate detection, triage, and initial response. Free your analysts for what requires judgment.

Accelerate IT Modernization

IT modernization is tractable. Shift to software-defined, cloud-native security controls. Consolidate point products into integrated platforms. Deploy zero trust architecture, not as a compliance exercise but as an operational model. Continuous identity verification, not perimeter defense, is the correct frame. Your IT systems can move fast. Move them.

Triage OT with Brutal Honesty

OT modernization cannot move at IT speed, and pretending otherwise creates false confidence. Where OT systems are genuinely unpatchable, the mitigation is not software. It is network segmentation, physical isolation, and redundancy. Prioritize energy systems and industrial control networks first. These are the highest automation-intensity, lowest patchability combinations in the portfolio. Build for containment, not just prevention.

Chip Supply Is a Strategic Constraint

Semiconductor availability is not an IT procurement issue. It is a recovery planning issue. A major attack would generate $145 billion in incremental chip demand into a supply-constrained market. Your recovery timeline depends on your position in the allocation queue. Establish preferred vendor relationships now. Consider stockpiling critical OT components for highest-risk systems.

WHAT TO PLAN FOR

2026-2027: Regulation is tightening on a defined timeline.

One in three governments will mandate sovereign AI for sensitive sectors. RAG architectures with in-country knowledge bases will become compliance requirements for regulated industries.

EU AI Act binding requirements take effect for high-risk systems. Security-by-design, mandatory incident reporting, and robustness testing become obligations, not options.

By 2029, 70% of large enterprises will adopt Private Cloud Compute to protect LLM data privacy. If your AI roadmap depends on public cloud LLMs for sensitive workloads, that architecture has a short remaining lifespan.

Build your security architecture around these timelines, not around your current procurement cycles. Mandatory certification, expanded liability, and cyber-risk insurance mandates are coming. Organizations that treat these as compliance costs rather than strategic investments will pay a multiple of what early movers spend.

WHAT TO EDUCATE YOUR TEAM ON

The mental model most security teams are operating with is wrong. It is built around the assumption that total prevention is achievable and that the primary threat vector is known malware. Neither is true in the frontier AI era.

Shift from prevention to resilience.
Speed of recovery is now the primary benchmark. Every team member should understand your recovery time objectives and what stands between your organization and meeting them.

Understand the IT/OT distinction deeply.
The security posture, tooling, and response protocols for a data center breach and an industrial controller compromise are different in almost every dimension. Your team should be fluent in both.

Synthetic identity is the new phishing.
80% of organizations will face phishing attempts using AI-generated synthetic identities by 2027. Train teams to treat all identity claims as unverified until continuously confirmed.

AI augments attackers too.
Vulnerability research and exploit development that once required expert human effort now requires a capable model and a prompt. The threat actor profile has expanded dramatically. Your threat modeling should reflect this.

Agentic risk requires an AI bill of materials.
Every deployed AI agent in your environment is a potential attack surface. Your team needs to understand the governance metadata behind what you are running, not just that you are running it.

THE BOTTOM LINE

The conclusion is that the narrative of cheap AI gains consistently underprices cybersecurity externalities. Frontier AI's autonomous capabilities expose systemic fragility in infrastructure that was built for a threat environment that no longer exists.

63% of organizations report insufficient cyber-resilience. The gap between security spend and security outcomes is not a budget problem. It is an architecture and prioritization problem. CIOs who treat this as the former will spend more and achieve less.

The organizations that come through the next three years in a defensible position will be the ones that mapped their unpatchable exposure honestly, automated their security operations aggressively, and planned their OT modernization with a realistic view of both cost and timeline. The window to get ahead of this is narrowing.

Thank You!

Galent