kyndryl

Cybersecurity at a historic inflection point: Navigating the converged threats of the digital age

By Kris Lovejoy, Global Security & Resiliency Practice Leader, Kyndryl

Contents

Introduction: The end of isolated threats

The world of cybersecurity is at a historic inflection point. The discrete threats of the past — stolen passwords, contained malware infections, etc. — are converging into complex, systemic risks with financial and societal implications. Indeed, the global cost of cybercrime is projected to reach well into the trillions of dollars by 2030. In this new era, understanding and addressing current threats is no longer sufficient; we must anticipate how they will accelerate and interconnect to shape the challenges of tomorrow.

This next evolution of cyber risk is taking place across five interconnected transformations. The first and most catalytic is the rise of autonomous artificial intelligence (AI), the likes of which is fundamentally reshaping the tactics of both attack and defense. Next is the profound disruption of the human workforce due to AI, and how that economic disruption is creating new motivations for cybercrime. Third, is the evolution of geopolitical tensions, which are fracturing the internet itself and turning the digital supply chain into a primary battleground. The fourth transformation is spurred by the rise of quantum computing and the need to achieve greater cryptographic agility. And finally, there is the emergent fragility of our foundational digital infrastructure, and the systemic risks that threaten its stability.

For business and technology leaders, access to integrated, actionable guidance will enable the strategic planning and investment required to build true enterprise resilience in a turbulent future. For to navigate this landscape is to understand that these are not five separate challenges, but five facets of a single, integrated reality.

The autonomous adversary: AI as a paradigm shift

The most immediate and transformative force in cybersecurity is the dual-use nature of artificial intelligence. It is simultaneously becoming our most powerful weapon and our most formidable adversary, creating a new arms race that will define the next decade.

The AI-driven arms race

Currently, AI's impact is twofold. On one side of this new battleground, adversaries leverage Generative AI for sophisticated social engineering and to create adaptive malware. A single incident in Hong Kong saw a firm lose $25 million to a scam where attackers used deepfake technology to impersonate the company's CFO in a video conference. This is a stark preview of a "post-truth" environment, one that Europol projects will see a sharp increase in online content that's synthetically generated. Simultaneously, AI-enabled malware is being deployed that can analyze its environment, identify security tools, and dynamically alter its code to evade detection.

On the other side, defenders are fighting AI with AI. Defensive algorithms now sift through trillions of data points to identify subtle anomalies indicative of an attack, shifting security teams from a reactive to a proactive posture. AI-driven Security Orchestration, Automation, and Response (SOAR) platforms are automating the triage and containment of common threats, freeing up human analysts to focus on novel incidents.

On the horizon: Autonomous conflict

This balanced conflict will soon evolve dramatically into a new paradigm of autonomous warfare. The AI-assisted attacks of today will mature into coordinated swarms of AI agents that can independently discover vulnerabilities and execute entire campaigns. Concurrently, adversaries will master "adversarial AI" — techniques designed specifically to deceive and poison our own defensive AI models. By 2026, with real-time deepfake technology fully commoditized, the very concept of digital trust will be fundamentally threatened.

Predictions

By 2027, fully autonomous, AI-driven cyberattacks will be successfully executed against enterprises, achieving the objective from initial penetration to data exfiltration without any direct human command. This event will render traditional, human-in-the-loop incident response timelines obsolete and prove that machine-speed defense is the only viable path forward.

Recommended actions

Fight AI with AI

Prioritize investment in next-generation, AI-powered defensive platforms for threat hunting, anomaly detection, and automated response.

Redefine and defend digital trust

Pilot and invest in next-generation multi-factor authentication (MFA) methods that are resistant to digital impersonation, such as FIDO2-compliant hardware keys.

Secure your AI, not just your network

Establish a governance program for the secure development and deployment of internal AI, including security standards for data sourcing, model training, and continuous monitoring.

The human element: A workforce disrupted, a threat transformed

While AI reshapes the technological landscape, an equally powerful human drama is unfolding, driven by the economic consequences of this same technological shift. This disruption is not only changing career paths but is also creating a new and potent catalyst for sophisticated financial crime.

The bifurcation of technology careers

AI is creating a clear divide in technology roles. Repetitive tasks like Level 1 IT support and writing boilerplate code are being automated, while complex roles in development, design, and data science are being augmented, freeing professionals to focus on higher-order tasks like strategy and innovation. This has led to the emergence of entirely new roles — AI/ML Engineer, Prompt Engineer, AI Ethicist — and places an unprecedented premium on uniquely human skills like critical thinking, strategic planning, and communication.

The cybersecurity field is a microcosm of this shift, but with far higher stakes. The traditional Security Operations Center (SOC) is being transformed, with AI automating threat detection and allowing the human analyst to become a true investigator. The role of a penetration tester is evolving into that of an Adversarial AI Tester, focused on finding flaws in AI models themselves. Governance, Risk, and Compliance (GRC) is moving beyond checklists to require AI Risk Strategists who can translate algorithmic risks into business terms.

In the ultimate evolution of this trend, AI will become the primary author of software. The cybersecurity practitioner will no longer be a digital mechanic finding flaws in human code, but an AI Security Architect, Governor, and Orchestrator, responsible for validating developer intent, securing the AI supply chain, and deploying defensive AIs to hunt for flaws in AI-generated code.

Economic pressure as a catalyst for cybercrime

This technological disruption creates a parallel, more sinister risk. The widespread technology sector layoffs throughout 2023 and 2024 have created a tangible pool of more than 500,000 highly skilled, financially pressured individuals in the US alone. This dynamic mirrors the conditions of post-Soviet Eastern Europe, where economic displacement and a surplus of technical talent directly fueled a global cybercrime boom.

This phenomenon is explained by the "fraud triangle," where three factors converge:

1. **Motive:** Intense financial pressure.
2. **Opportunity:** The inherent anonymity and accessibility of the internet.
3. **Rationalization:** A feeling of resentment towards a system perceived to have failed them.

An economic downturn amplifies all three factors for a technologically skilled population, lowering the barrier to entry into cybercrime.

Predictions

By the end of 2026, at least one major Ransomware-as-a-Service (RaaS) group will be founded or significantly staffed by former employees of legitimate, mainstream technology firms. This will lead to a notable increase in the operational sophistication, code quality, and business acumen of top-tier criminal syndicates.

Recommended actions

Launch a "Cyber Workforce 2030" initiative

Charter and fund a formal program to upskill and reskill the cybersecurity workforce, investing in your most critical defensive asset.

Train AI governors, not just coders

Focus training on skills like Secure Prompt Engineering, AI model auditing, and AI red-teaming.

Enhance insider threat programs

Re-evaluate and enhance technical controls and awareness programs to address the increased risk from employees facing financial pressure.

The geopolitical battlefield: A fracturing digital world

The same digital platforms that connect global economies also serve as battlegrounds for a new era of geopolitical conflict. The notion of a single, open, global internet is giving way to a fragmented reality, where data has become both a strategic asset and a weapon.

The rise of the "splinternet" and digital sovereignty

Driven by techno-nationalism, the internet is balkanizing into regional blocs with differing rules on data privacy, localization, and access. The OECD confirmed that 100 restrictive data localization measures were already in place across 40 countries as of early 2023. This fragmentation directly impacts any organization with a global footprint. Simultaneously, state actors and extremist groups are weaponizing AI-driven disinformation to radicalize individuals, erode trust in institutions, and incite conflict, creating a fertile ground for cyber activism and terrorism.

The third-party nexus: When risk is external

This geopolitical fragmentation exacerbates an already critical vulnerability: the third-party ecosystem. An organization's risk surface is no longer defined by its own walls, but by its entire digital supply chain. According to Verizon's 2025 Data Breach Investigations Report, 30% of all data breaches now involve a third-party vendor — a figure that has doubled from the previous year — with supply chain attacks surging by over 400% since 2021. This external risk is now multidimensional, encompassing the concentration risk of relying on a few dominant cloud providers, the opaque risk of AI models in vendor software, and the geopolitical risk of a vendor being caught on the wrong side of a digital border.

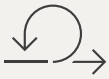
Predictions

By 2028, a G20 nation will formally use its data localization and sovereignty laws as an offensive tool in a major trade dispute, mandating the seizure of a foreign corporation's data or the shutdown of its services. Concurrently, supply chain integrity will overtake direct network intrusion as the primary C-level security concern.

Recommended actions

Navigate the splinternet with geopolitical intelligence

Invest in geopolitical risk intelligence feeds and expertise to inform IT architecture, data storage strategies, and vendor selection.



Master your ecosystem with continuous assurance

Evolve Third-Party Risk Management (TPRM) from static questionnaires and contractual obligations to a dynamic discipline, investing in tools that continuously scan your vendors' security posture.

Mandate radical transparency

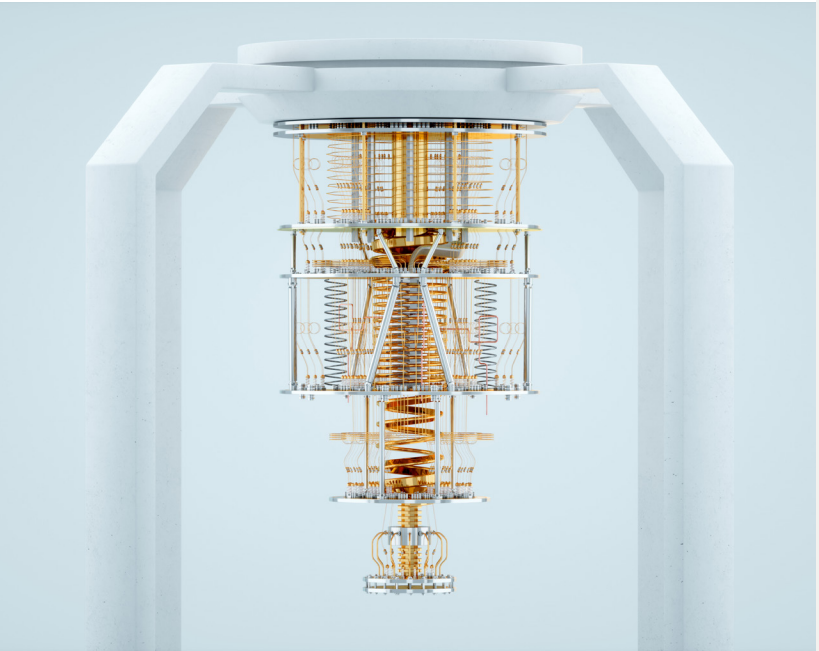
Make a Software Bill of Materials (SBOM) a contractual requirement for all new software vendors, and develop standards to demand an AI Bill of Materials (ABOM).

The quantum precipice

Beyond the immediate conflicts playing out on the world stage, a deeper, foundational risk is emerging that threatens the very physics of our digital world. This cryptographic crisis, driven by the dawn of quantum computing, does not target a single company or network but rather the trust underlying all digital communication. It is a slow-moving but existential threat that has already begun, and for which the deadline for action is non-negotiable.

The race to build a cryptographically relevant quantum computer has triggered a new and insidious type of data theft. Nation-state adversaries are believed to be actively engaged in "Harvest Now, Decrypt Later" (HNDL) attacks. They are siphoning vast quantities of encrypted data today — long-term government secrets, sensitive intellectual property, financial records, and private health information — with the full understanding that this data, while secure today, will be rendered transparent by a future quantum computer. The public-key cryptography that protects virtually all digital commerce and communication has a known, albeit uncertain, expiration date.

This threat is no longer theoretical. The US Government's National Security Memorandum 10 (NSM-10) has moved the issue from the lab to the level of national security policy, setting a hard 2035 deadline for federal agencies to migrate to quantum-resistant standards. This has initiated a global effort, often called "Y2Q" (Years to Quantum), to replace our core cryptographic infrastructure. Led by institutions like the National Institute of Standards and Technology (NIST), new algorithms are being standardized, but the scale of migration is immense — dwarfing the Y2K effort — as it requires identifying and replacing cryptographic protocols embedded deep within legacy software, hardware, and digital certificates across the entire enterprise.



Predictions

By 2029, a state-backed intelligence agency will covertly demonstrate the capability to decrypt a significant, recently encrypted dataset of strategic value. News of this breakthrough will leak, triggering a global market panic and a frantic, reactive scramble to implement Post-Quantum Cryptography (PQC), exposing the organizations that failed to prepare and instantly creating a new class of "have" and "have-not" in the world of data security.

Recommended actions

Achieve cryptographic agility

This is a non-negotiable imperative. The immediate action is to charter a Post-Quantum Preparedness Task Force, sponsored at the executive level, to lead this multi-year effort.

Conduct a "crypto census" now

The task force's first mandate is to conduct a complete inventory of all public-key cryptography across the enterprise. This inventory is the foundational blueprint of any migration plan and must be funded and prioritized as a critical undertaking.

Plan and budget for migration

Based on the inventory, develop a prioritized migration roadmap for transitioning to NIST-approved PQC algorithms. This migration must be established as a formal, funded line item in future technology and security budgets, not treated as a routine IT upgrade.

The energy nexus: Powering a fragile digital world

While the race is on to secure our data from future threats, the very ability to power the infrastructure that stores and processes this data is becoming a critical vulnerability. The entire digital economy is built upon the assumption of ubiquitous, stable power. This assumption, once a given, is now weakening under the weight of exponential demand and an expanding threat landscape, transforming energy from an operational concern into a core cybersecurity risk.

The trilemma of digital power

Our energy infrastructure is caught in a dangerous trilemma:

1. **Skyrocketing demand:** The AI revolution, detailed earlier, is the primary driver. The International Energy Agency (IEA) projects that power demand from data centers will more than double by 2030 to equal the entire current consumption of Japan. This insatiable appetite is placing unprecedented strain on local and regional grids.
2. **Aging infrastructure:** Much of the world's grid infrastructure is decades old, not designed for the demands of a hyper-concentrated digital economy and often lacking modern security controls.
3. **Expanding attack surface:** The modernization of the grid ("smart grid") and the proliferation of IoT devices in energy management, while boosting efficiency, also introduce millions of new digital entry points for attackers. This vulnerability is being actively exploited; a recent Sophos report found that 67% of energy and utility companies suffered a ransomware attack last year.

This convergence means that a vulnerability in an energy provider is now a direct vulnerability for every data center, company, and digital service that relies on it. Cyberattacks can now be paired with physical attacks on infrastructure, such as attacks on remote substations, to create prolonged and widespread outages.

Predictions

Before 2030, we will witness the first instance of a "converged infrastructure crisis" where a cyberattack against an energy grid will be used to specifically disable the data centers of a major cloud provider. This event will create a multi-faceted regional outage that impacts both digital and physical services simultaneously and will highlight the systemic risk of hyper-concentration in both our digital and physical infrastructure.

Recommended actions

Integrate physical and cyber risk governance

The CISO and the head of facilities/operations must be formally aligned. Action includes creating a joint risk register and governance committee that treats grid stability, fuel supply, and physical security as direct cybersecurity concerns.

Factor energy into site selection and resilience planning

Investment decisions for new data centers or critical operational sites must heavily weigh the stability, security, and resilience of the regional power grid as a primary selection criterion.

Develop and test blackout response plans

Action should be taken to create and regularly test detailed response plans that detail how security monitoring, core business operations, and incident response will function on limited backup power during a prolonged, wide-scale outage.

Conclusion

The era of viewing cybersecurity as a technical problem to be solved with firewalls is definitively over. The convergence of autonomous AI, geopolitical fragmentation, and foundational infrastructure risk creates a new operational reality that demands a fundamental shift in mindset — from defense-in-depth to strategic foresight and radical resilience. The old security playbook is obsolete.

Leadership's new mandate is to drive this transformation. This requires embracing the assumption that systems will be breached and core services may be unstable, shifting focus from prevention alone to rapid recovery. It means fighting AI with AI, not just with human teams. It demands achieving cryptographic agility before the quantum threat fully matures.

It necessitates mastering the entire digital ecosystem through deep supply chain illumination and mandating radical transparency from vendors. It requires integrating physical and cyber risk, recognizing that a stable power grid is as critical as a secure network.

The strategic imperatives outlined in this document are components of a single, cohesive strategy: to build an organization that is not just defended, but is inherently resilient, adaptive, and intelligent. The task for leadership is to shift investment from point-in-time defenses to continuous assurance, from isolated technical skills to broad strategic foresight, and from siloed risk management to an integrated understanding of our complex and turbulent digital world.

kyndryl