Preparedness in a New Threat Era

Cyber, AI, Quantum, and Infrastructure Risk

Introduction

The 2026 Annual Threat Assessment (ATA-2026-Unclassified-Report) outlines a rapidly evolving global risk environment defined by cyber threats, geopolitical competition, and emerging technologies such as artificial intelligence and quantum computing. These risks are no longer theoretical or isolated. They are active, interconnected, and increasingly impactful across government, critical infrastructure, and private enterprise.

This assessment is consistent with broader U.S. government guidance. Organizations such as the Cybersecurity and Infrastructure Security Agency, the National Institute of Standards and Technology, the Department of Defense, and the White House have all emphasized the importance of strengthening cybersecurity resilience, governing artificial intelligence, and preparing for post quantum cryptography. Together, these sources reinforce that emerging technology risk is no longer theoretical and requires coordinated preparedness across sectors.

This brief is informed by U.S. Intelligence Community threat assessments and SecureFi Institute research

While this paper is particularly relevant to government and critical infrastructure organizations, the same risks increasingly apply to U.S. companies operating in interconnected digital and global environments.

For organizations, the implications are clear. Risk is no longer confined to information technology systems. It is enterprise wide, leadership driven, and immediate.

Cyber threats represent the most immediate operational risk. Artificial intelligence is accelerating both capability and complexity. Quantum computing, while still emerging, presents a future disruption to the cryptographic systems that secure global commerce and national security.

The challenge is not simply understanding these threats.
The challenge is preparing for them.

The Nature of the Threat Environment

To understand why preparedness is required, it is important to first understand the nature of the current threat environment.

The current landscape is shaped by three converging forces: persistent cyber activity, rapid technological advancement, and global instability.

Cyber threats remain the most immediate concern. Nation state actors and organized criminal groups continue to conduct espionage, disruption, and ransomware operations. These activities are increasingly automated, scalable, and difficult to detect early, creating sustained operational risk for both government and enterprise organizations.

Artificial intelligence introduces a dual use dynamic. It enhances productivity, analytics, and decision making, while also enabling more sophisticated cyber operations, disinformation campaigns, and automation of attack techniques. Its adoption is accelerating faster than governance frameworks can keep pace.

Quantum computing represents a strategic inflection point. While cryptographically relevant quantum systems are not yet operational, their eventual development could render widely used encryption methods ineffective. Given the long lifecycle of data and infrastructure, preparation must begin before the technology fully matures.

At the same time, global competition and geopolitical tension are increasing pressure on supply chains, infrastructure, and economic systems. These factors amplify the impact of cyber and technological risk and introduce additional uncertainty into planning and operations.

Together, these forces create a threat environment that is more connected, more complex, and more consequential than in previous decades.

This view is reinforced across federal agencies, including CISA, the Department of Defense, and the Intelligence Community, all highlighting persistent cyber and infrastructure risk. These aligned signals underscore the urgency of action.

Why This Is a Leadership Issue

As the threat environment evolves, so must the way organizations respond.

Historically, cyber and technology risk were treated as technical problems to be managed within IT or security functions. That model is no longer sufficient.

The risks described in the current environment extend beyond systems and directly impact operational continuity, financial stability, customer and citizen trust, regulatory exposure, and national and economic security. These are leadership concerns.

Executives and boards must now make decisions about acceptable levels of risk, investment priorities, adoption of emerging technologies, and response to disruption. These decisions must be made in an environment where the pace of change is accelerating and uncertainty is increasing.

Preparedness, therefore, becomes a leadership responsibility. It requires not only technical controls, but also judgment, coordination, and clarity of decision making.

Federal cybersecurity and infrastructure guidance increasingly emphasizes executive accountability and governance, reflecting a broader shift from technical risk management to enterprise level responsibility.

The Gap Between Awareness and Readiness

Despite increased awareness of cyber, artificial intelligence, and quantum risk, a gap remains between understanding the threat and being prepared to address it.

Many organizations lack visibility into their cryptographic dependencies, have not established clear policies for AI usage and governance, and have not fully tested their incident response capabilities. In addition, they often rely on complex and opaque supply chains that introduce additional risk.

A central challenge is that emerging technologies are frequently approached through procurement rather than evaluation. Organizations are often required to make high cost decisions without the ability to test technologies in realistic environments, understand their operational implications, compare alternatives, or assess security risks prior to deployment.

This gap between awareness and readiness creates inefficiency, increases risk, and can lead to fragmented or inconsistent approaches across organizations.

Organizations are not failing due to lack of awareness. They are struggling due to lack of structured readiness and shared evaluation environments.

The Case for Collaborative Readiness

Bridging this gap requires a shift in how organizations approach preparedness.

Preparedness can no longer be achieved through isolated efforts or independent technology acquisition. The complexity and interconnected nature of modern threats demand a more coordinated model.

A collaborative readiness approach enables organizations to evaluate emerging technologies before making significant investments, test real world use cases in controlled environments, share insights across domains, reduce duplication of effort, and build a more consistent and informed security posture.

This model is not new in concept. Elements of it exist in Department of Energy national laboratories, Department of Defense experimentation environments, and NIST led standards development.

What is needed is the extension of this approach into the intersection of cyber resilience, artificial intelligence, quantum computing, and advanced computing environments.

Extending this model represents a natural evolution of proven federal frameworks and aligns with broader government efforts to improve coordination, efficiency, and security across agencies.

A Shared Readiness Environment

This shift leads to a practical question: what does a collaborative readiness model look like in practice?

A shared readiness environment provides a structured way to support this approach.

Such an environment enables organizations to experiment with emerging technologies in a secure setting, validate use cases before procurement, assess cybersecurity implications early, develop workforce understanding, and collaborate across agencies, industries, and disciplines.

This model shifts the focus from acquisition to understanding.

Instead of asking what should be purchased, organizations can first determine what works, what is secure, and what is appropriate for their mission or operational needs.

This approach reduces risk, improves decision making, and promotes more effective use of resources.

Recent federal strategies related to critical infrastructure security and artificial intelligence adoption further emphasize the importance of testing, validation, and secure implementation prior to large scale deployment. A shared readiness environment directly supports these objectives.

What Preparedness Looks Like in Practice

Preparedness is not a single initiative. It is a coordinated set of actions across technology, operations, and leadership.

Organizations should focus on strengthening cyber resilience by assuming compromise, limiting impact, and enabling rapid recovery. They should begin post quantum readiness efforts by identifying cryptographic dependencies and planning for transition to quantum resistant methods. AI governance must be established through clear policies, oversight mechanisms, and risk controls. Supply chain dependencies should be understood and managed through contingency planning. Leadership engagement is critical, requiring scenario based planning and alignment at the executive level.

These actions are supported by established federal guidance, including NIST cybersecurity frameworks and post quantum cryptography migration efforts, which emphasize structured, risk based approaches to implementation.

Why This Matters Now

The convergence of cyber threats, artificial intelligence advancement, and future quantum disruption creates a narrowing window for proactive preparation.

The Annual Threat Assessment makes clear that adversaries are already active, capabilities are evolving, and the consequences of inaction are increasing.

Waiting for full technological maturity or regulatory direction is not a viable strategy.

Organizations that act now can reduce exposure, improve resilience, make more informed investment decisions, and build long term operational advantage. Those that delay risk being unprepared for disruptions that are already emerging.

Multiple federal agencies have consistently emphasized that the window for preparation is narrowing as both threats and technologies continue to evolve.

Conclusion

The current threat environment requires more than awareness. It requires action.

Cyber threats are already impacting operations and infrastructure. Artificial intelligence is accelerating both opportunity and risk. Quantum computing will introduce structural changes to how security is defined and implemented.

These forces are converging as part of a broader shift in how technology, security, and global competition intersect.

For leaders, the implication is clear. Preparedness is no longer a technical exercise. It is a strategic and operational responsibility.

Organizations must move beyond reactive approaches and isolated investments. They must develop the ability to evaluate, understand, and implement technologies in a coordinated and informed manner.

A collaborative readiness model provides a path forward. It enables better decisions, reduces duplication, and strengthens resilience across government and industry.

The question is no longer whether these changes are coming.
The question is whether organizations will be prepared when they arrive.

References and Supporting Government Sources

Office of the Director of National Intelligence ATA-2026-Unclassified-Report
Annual Threat Assessment of the U.S. Intelligence Community, 2026

Cybersecurity and Infrastructure Security Agency
Cybersecurity resilience and preparedness guidance (CISA)

National Institute of Standards and Technology
Post Quantum Cryptography Project and Migration Guidance
NIST Cybersecurity Framework (NIST Computer Security Resource Center)

The White House (The White House)
National cybersecurity and artificial intelligence policy initiatives

Department of Homeland Security (Department of Homeland Security)
Critical infrastructure security and resilience guidance.

Department of Defense (U.S. Department of War)
Cyber strategy and zero trust guidance

The 2023-2027 DoW Cyber Workforce Strategy Implementation Plan DoW-CIO Cyber Plan

SecureFi Institute

Executive Brief Series: Deep Dive 001

Preparedness in a New Threat Era

Cyber, AI, Quantum, and the Case for Collaborative Readiness

Related SecureFi Institute Research

Executive Brief 001
The Threat is Real: *What the 2026 Threat Assessment Means for Leaders*

Executive Brief 002
Nation-State Cyber Threats: Why the Risk Is Real and Growing

Figures and Analytical Models
All figures, diagrams, and analytical models presented in this research brief were developed by SecureFi Institute as part of its research on emerging computing architectures and cybersecurity implications.

Research Disclaimer
This research brief is provided for informational and educational purposes and reflects analysis from SecureFi Institute on emerging computing technologies and cybersecurity trends. The views expressed are intended to support awareness and discussion of technology and infrastructure challenges and do not represent official policy positions.

This brief is informed by U.S. Intelligence Community threat assessments and SecureFi Institute research.

SecureFi Institute

Research. Awareness. Preparedness.