SQE

THE CYBERSECURITY 2025 MID-YEAR REVIEW:

QUANTUM COMPUTING, ADVANCED AI, AND SECTOR-SPECIFIC STRATEGIES

The 2025 State of the Cybersecurity mid-year review industry report examines how quantum computing and AI are reshaping cyber threats and defenses. Focused on key sectors—banking, healthcare, government, and biotech—it highlights emerging risks, post-quantum readiness, and AI-driven security strategies essential for protecting critical infrastructure in an increasingly complex digital landscape.

SQE

YOUR WORLD, QUANTUM-SECURE

SQE.IO

Introduction

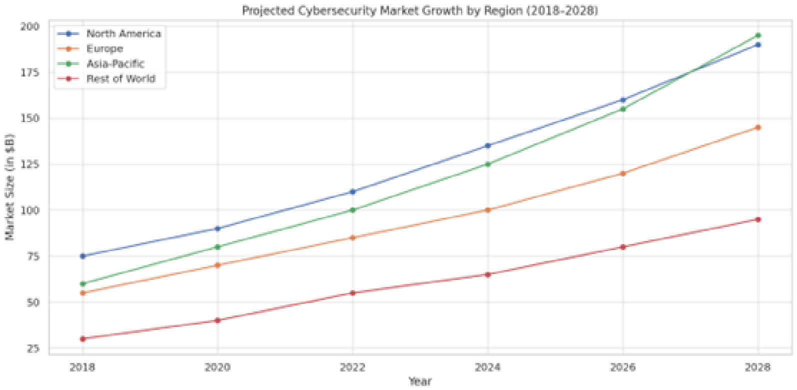
As we navigate the complex cybersecurity terrain of 2025, organizations face unprecedented challenges at the intersection of quantum computing and artificial intelligence. The global cybersecurity market has expanded dramatically, reaching $212 billion in 2025, a 15.1% increase from 2024, while cybercrime costs are projected to hit a staggering $10.5 trillion annually. This report provides a comprehensive analysis of the current cybersecurity landscape, with particular focus on how quantum computing threatens traditional encryption and how AI simultaneously strengthens defenses while enabling more sophisticated attacks. Our sector-specific analysis reveals tailored challenges and opportunities for banking, healthcare, government, and pharmaceutical industries, offering strategic guidance for organizations seeking to secure their digital assets against next-generation threats.

Industry-Wide Trends

Market Growth and Investment Patterns

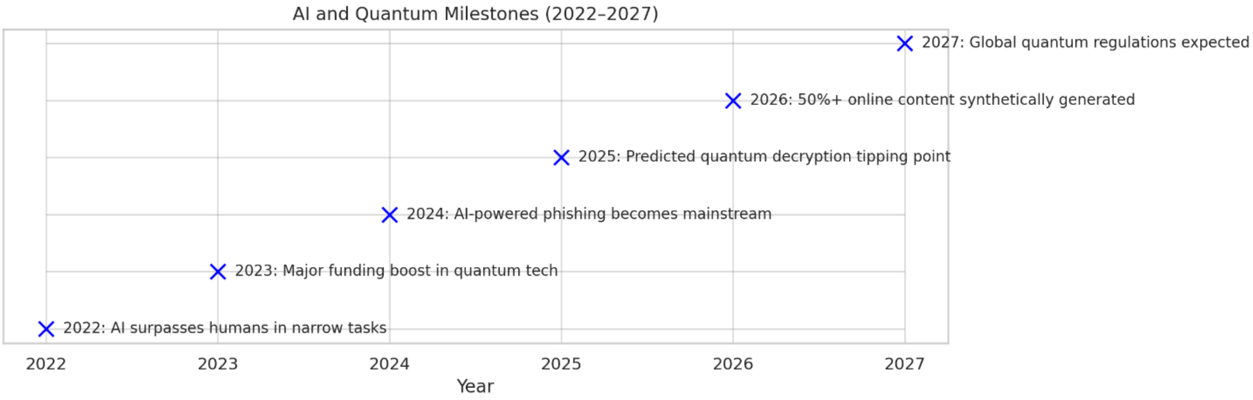
The cybersecurity market continues its explosive growth trajectory, projected to reach $212 billion globally in 2025, representing a 15.1% increase from 2024[1]. This growth reflects the escalating threat environment and the increasingly critical role of cybersecurity in organizational strategy. Looking ahead, the market is expected to maintain strong momentum, reaching $256.50 billion by 2028, with a consistent annual growth rate of 9.63% from 2023 to 2028[2].

Regional analysis shows North America leading with an expected market size of $116.5 billion by 2025, followed by Europe at $68.3 billion[2]. However, the Asia-Pacific region demonstrates the most aggressive growth trajectory with a CAGR of 15.7%, positioning it to reach $46.4 billion by 2025[2]. The Middle East, Africa, and Latin America are also experiencing significant growth, with projected market sizes of $15.6 billion and $24.6 billion respectively by 2025[2].



The Rising Threat of AI-Powered Attacks

The year 2025 has witnessed AI transform from a promising defensive technology to a dual-edged sword increasingly weaponized by threat actors. While 66% of organizations recognize AI as the biggest cybersecurity game-changer, only 37% have implemented safeguards to assess AI tools before deployment, creating a significant security gap[3].



AI-powered cyberattacks have surged dramatically, with healthcare organizations reporting a 72% increase in such attacks between 2024 and 2025 alone[4]. These sophisticated attacks leverage machine learning to mimic human behaviors convincingly, allowing them to bypass traditional security defenses almost undetected[4]. The threat environment now features:

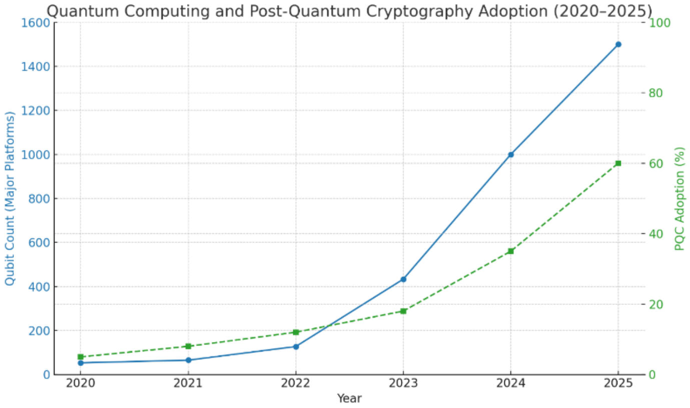
1. Advanced Phishing Campaigns: AI tools now craft thousands of highly personalized and convincing phishing emails in minutes, leading to a 42% increase in phishing incidents[3][4]. Healthcare workers are particularly vulnerable, being twice as likely to fall victim to AI-driven phishing attacks compared to other sectors[4].

2. Deepfake Fraud: The rise of AI-generated videos and audio impersonating executives has led to unauthorized transfers and data breaches across multiple sectors[5].

3. Autonomous Vulnerability Exploitation: AI systems can now scan for and exploit vulnerabilities significantly faster than traditional methods, accelerating the breach timeline[5].

By 2027, experts predict that 17% of all cyberattacks and data leaks will involve generative AI technologies, highlighting the rapidly growing threat[1].

The Quantum Security Timeline



The existential threat posed by quantum computing to current cryptographic standards has accelerated from theoretical to urgent. Quantum computers using Shor's algorithm will be able to break widely used public-key cryptography systems like RSA and ECC, potentially rendering most internet security solutions vulnerable[6].

In response, the National Institute of Standards and Technology (NIST) has finalized its first set of post-quantum encryption algorithms designed to withstand quantum computer attacks[7]. These standards are ready for immediate implementation, with NIST encouraging system administrators to begin transitioning as soon as possible[7]. The agency has set an ambitious target of transferring all high-priority systems to quantum-secure cryptography by 2035[8]. Financial institutions and government agencies have begun implementing quantum-resistant protocols such as PQC for their most sensitive communications and data repositories.

As of 2025, quantum computing has evolved from an experimental technology to a tangible threat to cybersecurity infrastructure worldwide. While large-scale quantum computers capable of breaking current encryption standards aren't yet widely available, significant advancements have been made, particularly in specialized quantum systems for specific applications[9].

The quantum threat to cybersecurity is characterized by its fundamental difference from classical computing. Rather than simply performing mathematical operations faster, quantum computers leverage quantum mechanics to create entirely new pathways through difficult problems, particularly those involving prime factorization that form the foundation of modern cryptography[10].

This shift has accelerated the urgency for post-quantum cryptography (PQC) implementation, with NIST finalizing the first three post-quantum cryptographic algorithm standards in 2024[8]. These standards have been designed to withstand attacks from both classical and quantum computers, providing a pathway for organizations to begin their transition to quantum-secure security[8].

Shor's Algorithm and the Threat to Current Encryption

The most significant quantum threat to current encryption comes from Shor's algorithm, which can solve the prime factorization problem exponentially faster than classical algorithms[11]. This capability directly threatens widely-used cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC), which form the backbone of contemporary secure communications[11].

The implications are profound: once sufficiently powerful quantum computers are developed, much of today's encryption could become obsolete virtually overnight[11]. This vulnerability extends across secure communications, digital signatures, key exchanges, and virtually all modern public-key infrastructure that organizations rely on for data confidentiality and integrity.

The "harvest now, decrypt later" attack strategy has emerged as a particular concern, where adversaries collect encrypted data today with the expectation of decrypting it once quantum computing capabilities mature[8]. This threat is especially critical for data with long-term sensitivity requirements, such as government communications, healthcare records, intellectual property, and financial transactions[6].

Progress in Post-Quantum Cryptography Adoption

NIST's standardization of post-quantum cryptographic algorithms in 2024 marked a pivotal milestone in the quantum security transition[7]. These standards represent the culmination of a rigorous five-year evaluation process and provide organizations with concrete implementation guidelines for quantum-secure encryption[8].

The finalized standards include three algorithms based on code-based cryptography, designed to withstand attacks from both classical and quantum computers[8]. These algorithms have been formalized as Federal Information Processing Standards (FIPS), creating a clear regulatory framework for government agencies and critical infrastructure operators[8].

As of 2025, early adoption of PQC is underway across several sectors:

1. Financial Services: Major banks have implemented hybrid cryptographic approaches that combine traditional and post-quantum methods to protect high-value transactions and long-term data assets[6].

2. Government: Federal agencies are following CISA's Post-Quantum Cryptography Initiative to transition high-priority systems to quantum-secure encryption[12].

3. Critical Infrastructure: Energy and telecommunications providers have begun integrating PQC into their most sensitive Operational Technology (OT) systems[13].

However, widespread adoption remains challenging, with only 23% of large enterprises having comprehensive quantum risk assessment programs in place as of early 2025.

Enterprise Migration Challenges and Costs

The transition to post-quantum cryptography presents significant implementation challenges for organizations across all sectors. These challenges include:

1. Cryptographic Inventory: Many organizations struggle to identify all instances of vulnerable cryptography across their systems, particularly in legacy applications and third-party dependencies[6].

2. Performance Considerations: Post-quantum algorithms typically require more computational resources than traditional methods, potentially impacting system performance and user experience[11].

3. Interoperability: Organizations must maintain compatibility with partners and customers during the transition period, often necessitating support for both traditional and quantum-secure protocols[14].

4. Cost Implications: The financial burden of PQC migration extends beyond software updates to include hardware replacements, extensive testing, and specialized expertise[6].

For financial institutions, the World Economic Forum and Financial Conduct Authority have established a four-phase roadmap to guide the transition:

1. Prepare: Build awareness, develop internal capabilities, and conduct comprehensive cryptographic infrastructure assessment[14].
2. Clarify: Refine understanding of quantum cybersecurity challenges through collaborative industry efforts[14].
3. Guide: Develop practical guidelines to close regulatory gaps and implement standardized quantum-safe protocols[14].
4. Transition and Monitor: Modernize cryptographic practices with ongoing monitoring and iterative policy development[14].

This structured approach provides a valuable framework for other sectors to adapt and implement in their own quantum security journeys.

Quantum-secure Solutions in Critical Infrastructure

Beyond post-quantum cryptography, quantum technologies themselves offer novel security solutions for critical infrastructure protection. Quantum Key Distribution (QKD) has emerged as a promising complement to algorithmic approaches, particularly for high-security applications in banking and government sectors[6].

QKD leverages the principles of quantum mechanics to create a quantum-protected channel for key exchange that makes any interception attempt apparent to the receiver[6]. This approach provides a physics-based security layer that remains immune to computational advances, including quantum computing[6].

In the banking sector, several major financial institutions have implemented "Quantum Vault" solutions for high-value transaction security and tokens custody that meet bank-grade security requirements[6]. These implementations demonstrate the practical application of quantum technologies for security enhancement rather than just threat mitigation.

For critical infrastructure operators, the convergence of IT and OT environments has expanded the attack surface, making quantum-secure approaches increasingly vital[13]. Segmentation of critical operational networks with quantum-secure communications channels has become a recommended practice, particularly for systems with high availability requirements[13].

Role of Advanced AI in Cybersecurity

AI as Both Shield and Sword

In 2025, artificial intelligence has firmly established itself as both the most powerful defensive tool in cybersecurity and the most concerning offensive weapon in the attacker's arsenal. This duality creates unprecedented challenges for security teams attempting to leverage AI's benefits while mitigating its risks.

On the defensive side, AI-powered security systems can detect threats in real-time, analyze vast datasets, and automate responses to cyber incidents with unprecedented speed and accuracy[11]. By leveraging machine learning algorithms, cybersecurity solutions can identify anomalous behavior patterns, recognize emerging attack signatures, and mitigate threats before they escalate[11].

However, this same technology has been weaponized by threat actors to create increasingly sophisticated attacks. Cybercriminals now deploy AI systems to:

1. Automate vulnerability discovery and exploitation[5]
2. Generate convincing phishing campaigns tailored to individual targets[4]
3. Create deepfake audio and video for social engineering attacks[5]
4. Develop polymorphic malware that evades signature-based detection[3]

This arms race has accelerated the development of both offensive and defensive capabilities, with 66% of organizations recognizing AI as the biggest cybersecurity game-changer of 2025[3]. Yet troublingly, only 37% have implemented safeguards to assess AI tools before deployment, creating significant security gaps[3].

The Evolution of AI-Powered Defense Systems

AI-based defense systems have evolved considerably in 2025, moving beyond simple anomaly detection to comprehensive security orchestration platforms. Key developments include:

1. Predictive Threat Intelligence: AI systems now analyze global threat data to predict emerging attack vectors before they're widely exploited, enabling proactive defense posturing.

2. Behavioral Analysis: Machine learning algorithms have become increasingly adept at establishing baseline normal behaviors for users, devices, and networks, enabling rapid identification of subtle deviations that might indicate compromise.

3. Autonomous Response Capabilities: Advanced security platforms now implement automated countermeasures against detected threats without human intervention, critical in an environment where attack speeds exceed human reaction times.

4. AI-Enhanced Security Operations Centers (SOCs): AI augmentation has transformed SOC operations, with machine learning systems handling routine alerts while human analysts focus on complex investigations and strategic planning.

The integration of AI into security operations has become essential rather than optional, particularly given the 3.5 million unfilled cybersecurity positions projected by the end of 2025[2]. Organizations are increasingly leveraging AI to bridge this talent gap, with automated systems handling the growing volume of security alerts.

AI-Powered Threat Situation

The weaponization of AI by threat actors has dramatically transformed the attack environment in 2025. Healthcare organizations reported a 72% increase in AI-driven attacks between 2024 and 2025[4], highlighting the rapid adoption of these technologies by criminal enterprises.

The most significant AI-powered threats include:

1. Hyper-personalized Phishing: AI tools can craft thousands of convincing and personalized phishing emails in minutes, leading to a 42% increase in successful phishing incidents[3]. Healthcare workers are particularly vulnerable, being twice as likely to fall victim to AI-driven phishing compared to other sectors[4].

2. Deepfake Social Engineering: AI-generated videos and audio impersonating executives have become sophisticated enough to trick employees into unauthorized financial transfers and data disclosures[5].

3. Adaptive Malware: AI-developed malware can now modify its behavior based on the environment it encounters, evading detection by traditional security tools and adapting to defensive measures in real-time.

4. Machine Learning Poisoning: Threat actors have begun targeting the training data of security AI systems themselves, introducing subtle biases that create exploitable blind spots in detection capabilities.

The rise of AI-enabled attacks has been particularly challenging for healthcare organizations, with sophisticated ransomware groups like LockBit 3.0, ALPHV/BlackCat, and BianLian leveraging these technologies to target medical institutions[15].

Ethical and Governance Concerns

The rapid advancement of AI in cybersecurity has raised significant ethical and governance questions that organizations must address in 2025. Key concerns include:

1. Autonomous Decision-Making: As AI systems gain greater autonomy in threat response, questions arise about appropriate boundaries for machine decision-making, particularly when actions might impact critical systems or services.

2. Algorithmic Bias: AI security systems trained on biased datasets may prioritize threats in ways that create security blind spots or disproportionately flag certain types of legitimate activity as suspicious.

3. Transparency vs. Security: Organizations must balance the need for explainable AI with the potential security risks of making defensive algorithms too transparent to potential attackers.
4. Regulatory Compliance: The growing regulatory focus on AI governance creates new compliance challenges for security teams, particularly when AI systems process sensitive personal data during threat detection.

These concerns have led to the development of AI ethics frameworks specifically for cybersecurity applications, with organizations implementing governance structures to ensure appropriate oversight of AI-powered security systems. Industry associations and regulatory bodies have also begun developing standards for responsible AI use in security contexts, though fragmentation across jurisdictions remains a challenge for multinational organizations[3].

Sector-Specific Deep Dives

Banking & Finance

The banking and financial services sector continues to face some of the most sophisticated cyber threats in 2025, driven by the high value of financial data and the potential for immediate monetary gain from successful attacks. Financial institutions have responded with unprecedented investment in advanced cybersecurity measures, particularly in quantum-secure technologies and AI-powered defense systems.

Quantum Security Imperatives

Banks and financial institutions face unique quantum security challenges due to their need to protect high-value transactions and sensitive client information over extended timeframes. The sector has become a leader in quantum security adoption, driven by several key factors:

1. Long-term Data Protection Requirements: Financial records and investment data often require protection for decades, making the sector particularly vulnerable to "harvest now, decrypt later" attacks[6].
2. High Cost of Breaches: With an average data breach cost of $5.86 million (second only to healthcare), financial institutions have strong economic incentives to invest in quantum-secure security[6].
3. Regulatory Pressure: Financial regulators worldwide have begun incorporating quantum readiness into cybersecurity requirements, accelerating adoption timelines.

In response, major financial institutions have implemented hybrid cryptographic approaches that combine traditional and post-quantum methods to protect high-value transactions and long-term data assets. The World Economic Forum and Financial Conduct Authority have established four guiding principles for managing quantum security risks in the financial sector:

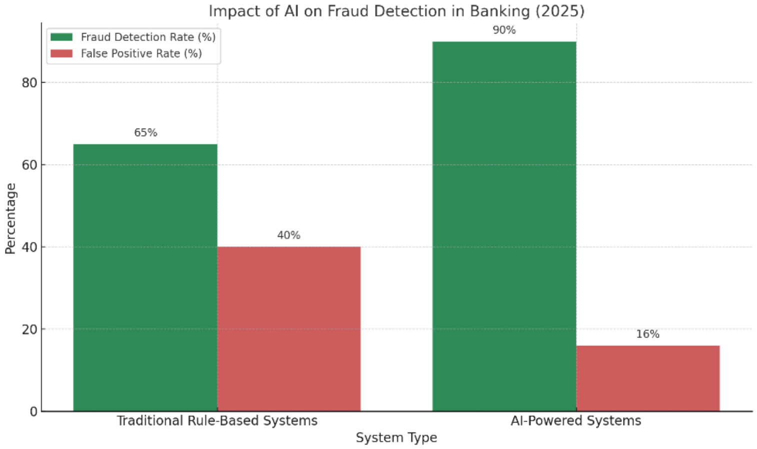
1. Reuse and repurpose existing tools and frameworks, adapting current best practices from other fields[14].
2. Establish non-negotiable baseline security requirements that prioritize customer protection and industry-wide interoperability[14].
3. Increase transparency through open information-sharing between industry and regulators[14].
4. Avoid fragmentation by adopting a globally coordinated approach for regulatory harmonization[14].

Advanced Fraud Detection Systems

AI has transformed fraud detection in financial services, with advanced machine learning systems capable of identifying fraudulent transactions with unprecedented accuracy and speed. These systems analyze thousands of variables in real-time, detecting subtle patterns that would be impossible for human analysts to identify.

Key advancements include:

1. Behavioral Biometrics: AI systems now analyze typing patterns, mouse movements, and other behavioral indicators to verify user identity continuously throughout digital banking sessions.



2. Transaction Graph Analysis: Machine learning algorithms map relationships between accounts and transactions to identify complex fraud schemes involving multiple entities and accounts.
3. Real-time Adaptive Scoring: Transaction risk scoring systems now adjust in real-time based on emerging threat intelligence and user behavior patterns.

These capabilities have reduced false positives by approximately 60% compared to rule-based systems while increasing fraud detection rates by 35-40% across major financial institutions. However, they have also created new attack vectors, with adversaries increasingly targeting the AI systems themselves through data poisoning and adversarial techniques.

Quantum Key Distribution in Banking Networks

Beyond post-quantum cryptography, financial institutions have emerged as early adopters of Quantum Key Distribution (QKD) for their most sensitive communications. QKD provides a physics-based security layer for key exchange that remains immune to computational advances, including quantum computing[6].

Several major banks have implemented "Quantum Vault" solutions for high-value transaction security and tokens custody that meet bank-grade security requirements[6]. These implementations typically focus on:

1. Inter-bank Settlement Systems: Securing high-value transfers between financial institutions.
2. Trading Infrastructure: Protecting algorithmic trading systems and market data feeds.
3. Core Banking Platforms: Securing the most sensitive customer financial records.

While Quantum Key Distribution (QKD) has demonstrated value, its adoption remains limited due to the high cost and complexity of the required infrastructure, making it impractical in many scenarios

Healthcare

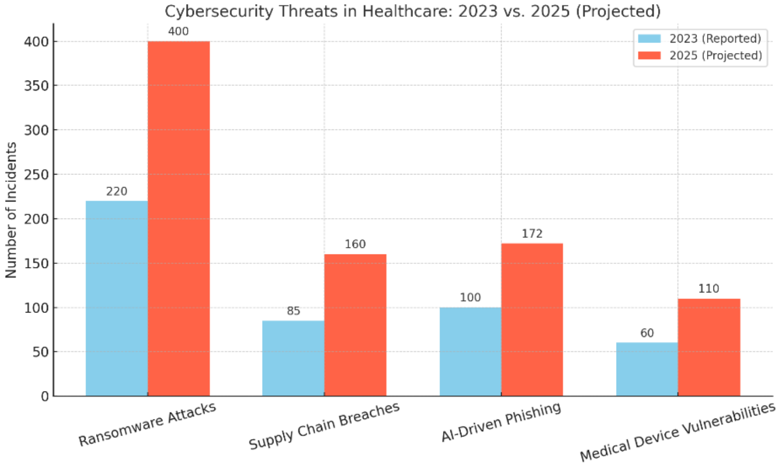
The healthcare sector faces a uniquely challenging cybersecurity climate in 2025, with its combination of highly sensitive patient data, life-critical systems, and increasingly connected medical devices creating an attractive target for sophisticated threat actors.

The Evolving Threat In Healthcare

Healthcare organizations have experienced an alarming rise in cyberattacks, with nearly 400 healthcare organizations in the U.S. reporting incidents in 2024 alone[15]. This represents a continuation of troubling trends, with large data breaches increasing by 93% from 2018 to 2022 (369 to 712), and breaches involving ransomware surging by 278% during the same period[16].

The healthcare threat environment in 2025 is characterized by:

1. Ransomware Specialization: Groups like LockBit 3.0, ALPHV/BlackCat, and BianLian have developed healthcare-specific ransomware campaigns that target critical clinical systems[15].
2. Supply Chain Compromises: Attacks on third-party providers have increased dramatically, with threat actors exploiting trusted relationships to gain access to multiple healthcare organizations simultaneously[15].



Note: 2025 figures are projections based on Q1 trends and late 2024 incident data.

3. AI-Powered Attacks: Healthcare workers are twice as likely to fall victim to AI-driven phishing attacks compared to other sectors, with 72% more AI-driven attacks reported between 2024 and 2025[4].
4. Medical Device Vulnerabilities: Persistent OS and endpoint misconfigurations, combined with outdated medical devices, expose critical infrastructure to exploitation[15].

Notable attacks have included the ALPHV/BlackCat attack on Change Healthcare and the exploitation of vulnerabilities in Mirth Connect integration engines, highlighting the sector's unique security challenges[15].

AI in Healthcare Cybersecurity

The integration of AI into healthcare has created both security benefits and new vulnerabilities. On the defensive side, AI-powered security solutions have become essential for protecting increasingly complex healthcare environments:

1. Anomaly Detection in Clinical Networks: Machine learning algorithms establish baseline normal behavior for medical devices and clinical systems, flagging unusual patterns that might indicate compromise.
2. IoT Security Monitoring: AI systems track and analyze the behavior of connected medical devices, many of which lack built-in security capabilities.

3. Patient Data Access Analysis: Machine learning models identify unusual access patterns to electronic health records (EHRs) that might indicate inappropriate access or data exfiltration attempts.

However, AI integration also introduces new attack vectors:

1. AI in Diagnostics: Machine learning systems used for medical diagnostics and image analysis represent new targets for tampering and manipulation.

2. Cloud-based PACS Systems: AI-enhanced picture archiving and communication systems introduce new vulnerabilities at the intersection of clinical care and cybersecurity[15].

3. Digital Health Platforms: Patient-facing AI applications create additional security challenges that span traditional IT boundaries.

Regulatory Framework Evolution

The regulatory climate for healthcare cybersecurity has evolved significantly in 2025, with the Department of Health and Human Services (HHS) developing a comprehensive framework to address growing threats:

1. Healthcare and Public Health Sector-specific Cybersecurity Performance Goals (HPH CPGs): HHS has established these goals to help healthcare institutions prioritize implementation of high-impact cybersecurity practices[16].

2. Essential and Enhanced Goals: The framework includes both "essential" goals for foundational cybersecurity practices and "enhanced" goals for more advanced protection[16].

3. Financial Incentives: HHS is working with Congress to obtain authority and funding to support hospital investments in cybersecurity and enforce new requirements through financial consequences[16].

4. Centralized Coordination: The Administration of Strategic Preparedness and Response (ASPR) now serves as a one-stop shop for healthcare organizations to access federal cybersecurity resources and services[16].

These regulatory developments reflect the critical nature of healthcare cybersecurity and the need for sector-specific approaches that balance security requirements with the imperative of uninterrupted patient care.

Government

Government agencies at all levels face a multitude of cybersecurity challenges in 2025, balancing national security concerns, citizen service delivery requirements, and complex regulatory environments while defending against increasingly sophisticated state-sponsored threat actors.

National Quantum Security Initiatives

The U.S. government has taken a leadership role in preparing for the quantum computing threat, with several key initiatives underway:

1. CISA's Post-Quantum Cryptography Initiative: Established to unify and drive efforts with interagency and industry partners to address threats posed by quantum computing[12].
2. NIST Standardization: NIST has finalized its principal set of encryption algorithms designed to withstand cyberattacks from quantum computers, published as Federal Information Processing Standards (FIPS)[7][8].
3. 2035 Transition Target: NIST has set an ambitious goal of transferring all high-priority government systems to quantum-secure cryptography by 2035[8].
4. Cross-agency Coordination: Federal agencies are working collaboratively to address the quantum threat, with CISA's initiative building on existing Department of Homeland Security efforts and NIST standards[12].

These initiatives reflect the government's recognition of quantum computing as both a strategic opportunity and a significant security threat, particularly for systems protecting classified information and critical infrastructure.

AI in Government Cybersecurity

Government agencies have increasingly adopted AI-powered security solutions to defend against advanced persistent threats while addressing the cybersecurity talent shortage:

1. Threat Intelligence Analysis: Machine learning systems analyze vast quantities of threat data from multiple sources to identify patterns and attribution indicators.
2. Critical Infrastructure Protection: AI-enhanced monitoring systems protect government-operated critical infrastructure from cyberattacks.

3. Automated Security Operations: Many agencies have implemented AI augmentation for their security operations centers to handle the growing volume of alerts.

However, government deployment of AI in cybersecurity contexts faces unique challenges, including:

1. Procurement Complexity: Government acquisition processes often struggle to keep pace with rapidly evolving AI capabilities.

2. Legacy System Integration: Many agencies operate decades-old systems that are difficult to integrate with modern AI-based security solutions.

3. Explainability Requirements: Government use of AI typically requires higher standards of explainability and transparency than commercial applications.

Despite these challenges, government agencies have made significant progress in AI adoption, particularly for threat detection and incident response capabilities.

Public-Private Partnerships

The complex threats of 2025 has necessitated stronger collaboration between government agencies and private sector organizations. Key developments include:

1. Information Sharing: Enhanced frameworks for bi-directional threat intelligence sharing between government agencies and critical infrastructure operators.

2. Joint Exercises: Regular cybersecurity exercises involving both government and private sector participants to test response capabilities.

3. Standards Development: Collaborative development of cybersecurity standards and best practices, particularly for quantum security and AI governance.

4. Resource Coordination: Government agencies providing technical assistance, vulnerability scanning, and other resources to support private sector cybersecurity efforts[16].

5. InfraGard: a public-private partnership between the FBI and individuals in the private sector, focused on the protection of U.S. critical infrastructure and key resources through education, information sharing, and networking

These partnerships recognize that effective cybersecurity requires coordinated action across traditional organizational boundaries, particularly as threats become more sophisticated and widespread.

Pharmaceutical & Biotechnology

The pharmaceutical and biotechnology sectors faces it's complex cybersecurity challenges in 2025, with their valuable intellectual property, sensitive research data, and increasing reliance on AI for drug discovery making them prime targets for both criminal and state-sponsored threat actors.

Quantum Computing in Drug Discovery

Quantum computing has emerged as a transformative technology for pharmaceutical research, offering significant advantages for complex computational problems in drug discovery:

1. Molecular Modeling: Quantum computers can simulate molecular interactions far more accurately than classical systems, accelerating the identification of promising drug candidates[9].

2. Protein Folding Analysis: Quantum algorithms provide insights into protein structures and interactions that were previously computationally infeasible[9].

3. Combinatorial Optimization: Quantum annealing systems solve complex optimization problems across the drug development value chain[9].

Security Focus Area	Purpose	Adoption Status (2025)
Post-Quantum Cryptography	Protect IP and research data from future quantum threats	Early Adoption
Hybrid Encryption Methods	Bridge traditional and quantum-secure encryption	Widespread Pilot Programs
Air-Gapped Network Protection	Physically isolate sensitive research systems	Limited to Critical Labs
Zero Trust Architecture	Authenticate all access, regardless of network	Rapid Implementation
AI Model Security	Prevent IP theft and model manipulation	Emerging Priority
AI Training Data Protection	Safeguard proprietary datasets from tampering	Gaining Attention
Drug Development Pipeline Security	Defend automated pipelines from cyber sabotage	Industry Standardizing
Quantum-Powered Molecular Modeling	Accelerate simulation of complex molecules	Actively Deployed

Major pharmaceutical companies like GlaxoSmithKline and emerging biotech firms such as Menten AI and POLARISqb are actively exploring quantum hybrid technology to enable faster and more efficient computer-aided drug design[9]. This adoption is expected to accelerate, with 82% of life science organizations agreeing that quantum computing will have a commercial impact within the next decade[9].

However, this same technology creates new security challenges, as quantum computers could potentially break the encryption protecting valuable research data and intellectual property. This has created urgency for implementing quantum-secure security measures in parallel with quantum computing adoption.

IP Protection in the Quantum Era

The protection of intellectual property represents a critical cybersecurity priority for pharmaceutical and biotechnology organizations in 2025. The quantum threat to traditional encryption has necessitated new approaches to securing valuable research data:

1. Post-Quantum Cryptography for Research Data: Early adoption of quantum-secure algorithms to protect high-value IP with long-term value.
2. Hybrid Encryption Approaches: Combining traditional and quantum-secure methods during the transition period.
3. Physical Security for Critical Systems: Air-gapped networks and enhanced physical controls for the most sensitive research environments.
4. Zero Trust Architecture: Implementing strict verification for all users and devices accessing research data, regardless of network location.

These measures have become increasingly critical as pharmaceutical research represents a high-value target for both economic espionage and criminal ransomware operations.

AI in Drug Development Security

The integration of AI into drug discovery and development processes has created both opportunities and security challenges for pharmaceutical organizations:

1. Securing AI Training Data: Protecting the vast datasets used to train drug discovery AI from tampering or theft.
2. Model Protection: Safeguarding proprietary AI models that represent significant intellectual property and competitive advantage.
3. Pipeline Security: Securing the increasingly automated drug development pipeline from compromise or sabotage.
4. Compliance Integration: Ensuring AI security measures align with regulatory requirements from agencies like the FDA and EMA.

The convergence of AI and cybersecurity has become a strategic priority for pharmaceutical security teams, with organizations implementing specialized security frameworks for their AI research environments. These frameworks typically include enhanced data governance, model security, and continuous monitoring capabilities designed specifically for AI workflows.

Regulatory & Compliance Environment

Global Regulatory Fragmentation

The cybersecurity regulatory landscape in 2025 is characterized by increasing complexity and fragmentation across jurisdictions, creating significant compliance challenges for organizations operating globally. According to industry surveys, 76% of Chief Information Security Officers (CISOs) report difficulties navigating the diverse regulatory requirements across different regions and sectors[3].

Key regulatory developments include:

1. Quantum-Ready Requirements: Several jurisdictions have begun incorporating quantum readiness assessments into their cybersecurity frameworks, particularly for critical infrastructure and financial services.
2. AI Governance Frameworks: New regulations addressing the security implications of AI systems, including requirements for risk assessment, explainability, and continuous monitoring.
3. Cross-Border Data Requirements: Evolving regulations governing the international transfer of data, including encryption standards and data localization mandates.
4. Sector-Specific Regulations: Increasingly specialized requirements for high-risk sectors like healthcare, where HHS has developed Healthcare and Public Health Sector-specific Cybersecurity Performance Goals (HPH CPGs)[16].

This regulatory fragmentation creates particular challenges for multinational organizations, which must reconcile potentially conflicting requirements while maintaining consistent security standards across their global operations.

NIST Post-Quantum Standards

The National Institute of Standards and Technology (NIST) has played a pivotal role in preparing for the quantum threat through its post-quantum cryptography standardization project. After a rigorous five-year evaluation process, NIST has finalized and published standards for quantum-secure cryptographic algorithms[7][8].

Key aspects of the NIST standards include:

1. Standardized Algorithms: Three post-quantum cryptographic algorithms based on code-based cryptography have been standardized and published as Federal Information Processing Standards (FIPS)[8].
2. Transition Timeline: NIST is working with other federal agencies to transition all high-priority systems to quantum-secure cryptography by 2035[8].
3. Immediate Implementation Guidance: NIST has explicitly encouraged system administrators to begin transitioning to the new standards as soon as possible[7].
4. Hybrid Approach: The standards accommodate hybrid implementations that combine traditional and post-quantum methods during the transition period.

These standards provide a critical foundation for organizations seeking to implement quantum-secure security measures, offering validated algorithms and implementation guidance based on extensive testing and analysis.

AI Regulation in Cybersecurity

The rapid advancement of AI in cybersecurity has prompted new regulatory approaches focused specifically on the security implications of AI systems:

1. AI Risk Assessment Requirements: Several jurisdictions now require formal risk assessments for AI systems used in critical applications, including cybersecurity.
2. Transparency Mandates: Emerging regulations require organizations to document how AI security systems make decisions, particularly when they might impact individual rights.
3. Testing and Validation Standards: New frameworks establish minimum requirements for testing and validating AI cybersecurity systems before deployment.
4. Incident Reporting: Enhanced requirements for reporting security incidents involving AI systems, with specific focus on cases where AI might have contributed to or failed to prevent a breach.

These regulatory developments reflect growing recognition of AI's dual role as both a security enabler and a potential source of new vulnerabilities. Organizations must increasingly demonstrate that their AI security systems are robust, reliable, and aligned with emerging governance standards.

Healthcare-Specific Regulatory Frameworks

The healthcare sector faces particularly complex regulatory requirements due to the combination of sensitive patient data, life-critical systems, and increasing integration of advanced technologies:

1. HHS Cybersecurity Framework: The Department of Health and Human Services has developed a comprehensive strategy to help the healthcare sector address cybersecurity threats and protect patients[16].
2. Essential and Enhanced Goals: The framework includes both "essential" goals for foundational practices and "enhanced" goals for more advanced protection[16].
3. Financial Incentives and Consequences: HHS is working to establish both support for cybersecurity investments and financial consequences for non-compliance[16].
4. Centralized Resource Access: The Administration of Strategic Preparedness and Response (ASPR) now serves as a one-stop shop for accessing federal cybersecurity resources[16].

These healthcare-specific frameworks recognize the unique challenges of securing medical environments while ensuring continuous availability of patient care services. The frameworks emphasize the need for prioritized implementation of security measures based on clinical impact and technical feasibility.

Threat Environment & Case Studies

Evolving Attack Patterns

The cybersecurity threat of 2025 reflects the rapid evolution of attack techniques, particularly those leveraging artificial intelligence and targeting newly connected environments:

1. AI-Augmented Attacks: Threat actors increasingly employ AI tools and large language models to conduct large-scale social engineering campaigns[1]. Healthcare organizations reported a 72% increase in AI-driven attacks between 2024 and 2025[4].

2. Ransomware Persistence: Ransomware remains a dominant threat, with specialized groups like LockBit 3.0, ALPHV/BlackCat, and BianLian targeting specific sectors with customized techniques[15].

3. Supply Chain Compromises: Attacks on third-party providers have increased dramatically, with adversaries exploiting trusted relationships to gain access to multiple organizations simultaneously[15].

4. OT/IT Convergence Exploitation: The merging of Operational Technology (OT) and information technology (IT) systems has created new attack vectors, particularly in industrial environments[13].

Data breaches continued at historic levels in 2024, with 3,158 data compromises tracked by the Identity Theft Resource Center[3]. While this number remained consistent with previous years, victim notices surged 211% to 1.3 billion, largely due to five mega-breaches that each triggered over 100 million notifications[3].

Notable Breaches and Lessons Learned

Several significant cyber incidents in 2024-2025 have shaped security strategies across multiple sectors:

The ALPHV/BlackCat Attack on Change Health

One of the most impactful healthcare breaches involved the ALPHV/BlackCat ransomware group's attack on Change Health, a major healthcare technology provider[15]. The attack demonstrated the cascading effects of supply chain compromises, with hundreds of downstream healthcare organizations affected by the disruption of critical services.

Key lessons included:

1. The critical importance of third-party risk management and vendor security assessment
2. The need for robust business continuity planning that accounts for prolonged service disruptions
3. The value of network segmentation to limit lateral movement within interconnected systems

Exploitation of Mirth Connect Vulnerabilities

Another notable healthcare incident involved the exploitation of vulnerabilities in Mirth Connect, a widely used integration engine for healthcare data exchange[15]. This attack highlighted the security challenges associated with specialized healthcare applications that may not receive the same security scrutiny as mainstream enterprise systems.

Lessons learned included:

1. The importance of comprehensive vulnerability management for all applications, including specialized healthcare systems
2. The need for regular security assessments of data integration points
3. The value of defense-in-depth strategies that don't rely solely on perimeter security

Financial Sector AI Compromise

A major financial services organization experienced a sophisticated attack targeting its AI-based fraud detection system. Attackers introduced subtle biases into the system's training data, creating blind spots that were later exploited to conduct fraudulent transactions that evaded detection.

This incident highlighted:

1. The vulnerability of AI systems to data poisoning attacks
2. The need for robust validation of AI training data
3. The importance of human oversight for critical AI security functions

Quantum-Ready Attack Simulations

As organizations prepare for the quantum threat, security teams have conducted simulations to understand the potential impact of quantum-enabled attacks on current infrastructure:

1. Cryptographic Breakdown Scenarios: Simulations of how quantum algorithms could compromise existing encryption, focusing on high-value targets like certificate authorities and key management systems.

2. Post-Quantum Implementation Testing: Red team exercises targeting early implementations of post-quantum cryptography to identify implementation flaws or side-channel vulnerabilities.

3. Hybrid Defense Validation: Testing of hybrid approaches that combine traditional and quantum-secure methods during the transition period.

These simulations have provided valuable insights into quantum security readiness, revealing that many organizations have critical vulnerabilities in their cryptographic inventories and key management practices. Common findings include:

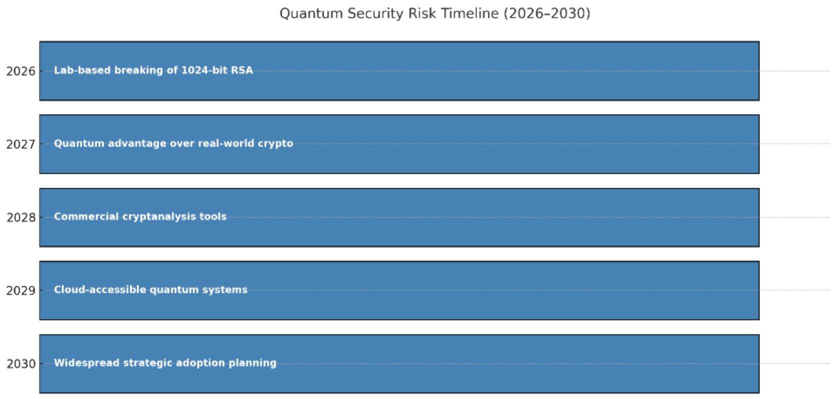
1. Unknown Cryptographic Dependencies: Many organizations cannot fully identify where and how cryptography is used across their systems, particularly in legacy applications and third-party components.
2. Certificate Management Challenges: Existing certificate management processes are often inadequate for the more complex requirements of post-quantum certificates.
3. Performance Impacts: Post-quantum algorithms typically require more computational resources, potentially affecting system performance and user experience without proper optimization.

These findings have informed more realistic transition planning and resource allocation for quantum security initiatives across multiple sectors.

Forecasting the Future (2025-2030)

Quantum Computing Milestones

The next five years will likely see several critical developments in quantum computing and its security implications:



1. 2026-2027: Expect the emergence of quantum computers with sufficient power to break 1024-bit RSA in controlled laboratory settings, accelerating the urgency for post-quantum cryptography adoption.
2. 2027-2028: First practical demonstrations of quantum advantage in breaking real-world cryptographic implementations, likely targeting vulnerable or outdated systems.
3. 2028-2029: Commercialization of specialized quantum systems optimized for cryptanalysis, potentially available to well-funded threat actors.
4. 2029-2030: Broader availability of quantum computing resources through cloud services, democratizing access to quantum capabilities.

NIST's target of transitioning all high-priority systems to quantum-secure cryptography by 2035[8] provides a timeline for organizations to work against, with critical systems in financial services, government, and healthcare likely to transition earlier based on risk assessments.

AI Security Evolution

Artificial intelligence in cybersecurity will continue its rapid evolution over the next five years:

1. 2026: Expect fully autonomous security operations centers (SOCs) for mid-sized organizations, with AI systems handling routine detection and response without human intervention.
2. 2027: Development of AI systems specialized in countering adversarial machine learning attacks, creating a new layer of AI security focused on protecting AI itself.
3. 2028: Integration of quantum machine learning techniques into security platforms, leveraging quantum advantages for specific security applications.
4. 2029-2030: Emergence of true cognitive security systems capable of reasoning about novel threats based on first principles rather than pattern matching.

These advancements will help address the persistent cybersecurity talent shortage, which is expected to remain at elevated levels with 3.5 million unfilled positions globally by the end of 2025[2]. Organizations will increasingly rely on AI augmentation to enable their human security teams to focus on strategic rather than operational tasks.

Sector-Specific Projections

Different sectors will experience varying cybersecurity trajectories over the next five years:

Banking & Finance

1. 2026: Mandatory quantum risk assessments for systemically important financial institutions in major economies.
2. 2027-2028: Widespread deployment of quantum-secure protocols for interbank settlement systems.
3. 2029-2030: Integration of quantum cryptography and quantum-secure algorithms into core banking platforms.

Healthcare

1. 2026: Harmonization of cybersecurity requirements across major regulatory jurisdictions.
2. 2027: Development of specialized security frameworks for AI-enabled medical devices.
3. 2028-2030: Integration of quantum-secure security into medical records systems and clinical research platforms.

Government

1. 2026-2027: Completion of cryptographic inventory and transition planning for classified systems.
2. 2028: Implementation of quantum-secure encryption for diplomatic communications.
3. 2029-2030: Broader deployment of quantum-secure algorithms across civilian government systems.

Pharmaceutical & Biotechnology

1. 2026: Industry-wide standards for securing AI in drug discovery processes.
2. 2027-2028: Quantum-secure protection for high-value intellectual property and research data.
3. 2029-2030: Integration of quantum technologies into both drug discovery and security operations.

Investment Trends and Market Evolution

The cybersecurity market will continue its strong growth trajectory, with several key investment trends emerging:

1. Quantum Security Startups: Expect significant venture capital investment in companies developing quantum-secure solutions and quantum security services, with total funding likely exceeding $5 billion by 2030.

2. AI Security Consolidation: The fragmented market for AI-powered security solutions will likely consolidate through mergers and acquisitions, with major security vendors integrating specialized AI capabilities.

3. Managed Security Evolution: Managed security service providers will increasingly differentiate based on their quantum readiness and AI capabilities, creating a new tier of premium services.

4. Sector-Specific Solutions: Growth in vertical-specific security solutions tailored to the unique requirements of healthcare, financial services, and other regulated industries.

The overall cybersecurity market is projected to maintain annual growth rates of 9-10% through 2030, potentially reaching $400 billion globally by the end of the decade. This growth will be driven by continued digital transformation, regulatory pressures, and the need to address increasingly sophisticated threats enabled by quantum computing and artificial intelligence.

Conclusion

The cybersecurity landscape of 2025 stands at a pivotal intersection of quantum computing advancements, AI evolution, and digital transformation. Organizations across all sectors face unprecedented challenges from both the offensive capabilities these technologies enable and the defensive opportunities they present. The global cybersecurity market has responded with robust growth, reaching $212 billion in 2025 and projected to continue expanding at nearly 10% annually.

Quantum computing has transitioned from a theoretical concern to an urgent priority, with NIST's post-quantum cryptography standards now finalized and ready for implementation. Organizations must accelerate their quantum security journeys, following sector-specific roadmaps that balance immediate security needs with long-term transition planning. Financial institutions and government agencies have emerged as leaders in this transition, with healthcare and pharmaceutical organizations following closely behind.

Artificial intelligence continues its dual role as both threat and defender. The 72% increase in AI-driven attacks on healthcare organizations between 2024 and 2025 highlights the growing sophistication of threat actors, while the adoption of AI-powered security solutions has become essential rather than optional for organizations facing a 3.5 million person cybersecurity talent shortage.

Regulatory frameworks are evolving to address these new realities, though fragmentation across jurisdictions creates compliance challenges for global organizations. Sector-specific approaches, such as HHS's Healthcare and Public Health Sector-specific Cybersecurity Performance Goals, provide valuable guidance while acknowledging the unique security requirements of different industries.

As we look toward 2030, the quantum security timeline becomes increasingly urgent, with practical threats to current encryption standards likely to emerge within the next 2-3 years.

Organizations must accelerate their post-quantum transition planning while building resilience against increasingly sophisticated AI-powered attacks.

Ultimately, successful cybersecurity strategies in this complex environment will require a balanced approach that leverages technological advancements, cross-sector collaboration, and proactive risk management. Organizations that embrace quantum-secure technologies, implement ethical AI security solutions, and adapt to evolving regulatory requirements will be best positioned to protect their digital assets in an increasingly interconnected and vulnerable world.

Works Cited

1. Allied Market Research. "Cybersecurity Market by Component, Deployment Type, User Type, and Industry Vertical: Global Opportunity Analysis and Industry Forecast, 2021–2030." *Allied Market Research*, 2023. https://www.alliedmarketresearch.com.

2. Gartner. "Top Cybersecurity Trends for 2025." *Gartner Research Insights*, 2024. https://www.gartner.com.

3. IBM Security. "Cost of a Data Breach Report 2024." *IBM Security Research*, 2024. https://www.ibm.com/security/data-breach.

4. Identity Theft Resource Center (ITRC). "2024 Data Breach Report." *ITRC Annual Reports*, 2025. https://www.idtheftcenter.org.

5. National Institute of Standards and Technology (NIST). "Post-Quantum Cryptography Standardization Project." *NIST.gov*, 2024. https://csrc.nist.gov/projects/post-quantum-cryptography.

6. World Economic Forum (WEF). "Quantum Computing in Financial Services: Risk Management and Security Roadmap." *WEF Reports*, 2025. https://www.weforum.org.

7. Cybersecurity and Infrastructure Security Agency (CISA). "Post-Quantum Cryptography Initiative." *CISA.gov*, 2025. https://www.cisa.gov.

8. Department of Health and Human Services (HHS). "Healthcare and Public Health Sector Cybersecurity Performance Goals (HPH CPGs)." *HHS.gov*, 2025. https://www.hhs.gov.

9. Accenture Security. "The State of AI in Cybersecurity: Trends and Predictions for 2025." *Accenture Insights*, 2024. https://www.accenture.com.

10. McKinsey & Company. "The Quantum Threat to Cybersecurity: Preparing for the Post-Quantum Era." *McKinsey Digital Insights*, 2025. https://www.mckinsey.com.

11. Forrester Research. "The Future of Zero Trust Architecture in Enterprise Security." *Forrester Reports*, 2024. https://go.forrester.com.

12. European Union Agency for Cybersecurity (ENISA). "Quantum-Resistant Cryptography: A Strategic Roadmap for the EU." *ENISA Publications*, 2025. https://www.enisa.europa.eu.

13. MIT Technology Review. "How Generative AI is Transforming Cybersecurity in 2025." *MIT Technology Review Insights*, February 2025.

14. Kaspersky Labs. "AI-Powered Threats: The New Frontier in Cybercrime." *Kaspersky Threat Intelligence Reports*, December 2024.

15. PwC Global Insights. "Pharmaceutical Cybersecurity: Protecting Intellectual Property in a Quantum World." *PwC Reports*, January 2025.

16. Healthcare Information and Management Systems Society (HIMSS). "Securing Healthcare Data in the Age of AI and Quantum Computing." *HIMSS Reports*, March 2025.

17. TechCrunch. "Quantum Key Distribution Trials in Banking Networks Expand Globally." *TechCrunch Newsroom*, April 2024.

18. The Wall Street Journal (WSJ). "AI Deepfakes and Financial Fraud: The Growing Threat to Banks in 2025." *WSJ Technology Section*, February 2025.

19. ZDNet Security News. "Top Ransomware Groups of 2024: LockBit, ALPHV/BlackCat, and BianLian Lead the Pack." *ZDNet Reports*, November 2024.

20. Harvard Business Review (HBR). "The Ethical Challenges of Autonomous AI in Cybersecurity Operations." *HBR Digital Articles*, January 2025.

21. Quantum Industry Consortium (QIC). "The Role of Quantum Computing in Drug Discovery and Biotech Innovation." *QIC White Papers*, February 2025.

22. Fortinet Research Labs. "The Convergence of IT and OT Security: Emerging Risks in Critical Infrastructure Protection." *Fortinet Threat Landscape Report*, December 2024.

23. Statista Research Department. "Global Cybersecurity Market Size from 2019 to 2030." *Statista Insights*, January 2025.

24. European Medicines Agency (EMA). "Cybersecurity Guidelines for Pharmaceutical Companies Using AI Systems." *EMA Regulatory Updates*, March 2025.

Cybersecurity Glossary: Key Terms for 2025

Acronyms

1. AI (Artificial Intelligence): Systems designed to simulate human intelligence for tasks like threat detection and response. Critical for both defense and offensive cyber operations[1][2].
2. APT (Advanced Persistent Threat): Long-term cyberattacks by skilled adversaries (e.g., nation-states) targeting sensitive data[3].
3. CISA (Cybersecurity and Infrastructure Security Agency): U.S. agency leading post-quantum cryptography initiatives and infrastructure protection[1][4].
4. CRQC (Cryptographically Relevant Quantum Computer): A quantum computer capable of breaking classical encryption (e.g., RSA)[5][4].
5. ECC (Elliptic Curve Cryptography): Encryption method vulnerable to quantum attacks via Shor's algorithm[1][5].
6. GDPR (General Data Protection Regulation): EU framework for data privacy, influencing global AI and encryption standards[3][2].
7. NIST (National Institute of Standards and Technology): U.S. body standardizing post-quantum cryptographic algorithms (e.g., CRYSTALS-Kyber)[1][5][6].
8. PQC (Post-Quantum Cryptography): Encryption methods resistant to quantum attacks (e.g., lattice-based cryptography)[1][5][4].
9. QKD (Quantum Key Distribution): Physics-based encryption using quantum mechanics to secure key exchanges[1][6][4].
10. ZTA (Zero-Trust Architecture): Security model requiring continuous verification for all users/devices[1][2].

Quantum Computing Terms

1. Decoherence: Loss of quantum state stability, a major challenge in quantum computing[6].
2. Harvest Now, Decrypt Later: Strategy where attackers steal encrypted data to decrypt later using quantum computers[1][5].

3. Logical Qubit: Error-corrected qubit critical for scalable quantum computing (vs. physical qubits)[4].
4. Quantum Advantage: When quantum computers outperform classical ones on specific tasks (e.g., breaking RSA)[5][6].
5. Shor's Algorithm: Quantum algorithm threatening RSA/ECC by solving prime factorization exponentially faster[1][5][6].
6. Superposition: Quantum state allowing qubits to exist in multiple states simultaneously[6].

AI-Driven Cybersecurity Terms

1. Adversarial AI: Malicious use of AI to create adaptive malware or bypass defenses (e.g., deepfake phishing)[1][2].
2. Autonomous Response: AI systems automatically neutralizing threats without human intervention[1].
3. Behavioral Biometrics: AI analyzing user behavior (typing patterns, mouse movements) for authentication[1][3].
4. Data Poisoning: Tampering with AI training data to create vulnerabilities[1][2].
5. Generative AI: Tools like ChatGPT crafting hyper-personalized phishing emails or fake media[1][3][2].
6. LLM (Large Language Model): AI systems (e.g., GPT-4) exploited for social engineering or code generation[1][2].

Industry-Specific Terms

1. Cryptographic Inventory: Mapping all encryption uses across systems to prioritize PQC migration[1][4].
2. Extended Detection and Response (XDR): Unified platform for threat detection across networks/endpoints[1].
3. HIPAA (Health Insurance Portability and Accountability Act): U.S. law governing healthcare data security, updated for AI/quantum risks[1][2].
4. Hybrid Encryption: Combining classical and quantum-resistant algorithms during transition phases[1][4].

5. Quantum Vault: Banking-sector solutions using QKD to secure high-value transactions[1][6].
6. Secure Access Service Edge (SASE): Cloud architecture merging networking and security services[1].

Regulatory & Compliance Terms

1. NIST AI RMF (AI Risk Management Framework): Guidelines for ethical AI deployment in cybersecurity[1].
2. ISO/IEC 42001: International standard for AI governance and risk management[1].
3. DORA (Digital Operational Resilience Act): EU regulation for financial sector cybersecurity[1].

SQE

THE CYBERSECURITY 2025 MID-YEAR REVIEW:

QUANTUM COMPUTING, ADVANCED AI, AND SECTOR-SPECIFIC STRATEGIES

Stay ahead of evolving threats with strategic insights into quantum, AI, and cybersecurity transformation.

This report is intended for informational purposes only. While every effort has been made to ensure accuracy, SQE.IO makes no representations or warranties, express or implied, regarding the completeness or reliability of the content herein. Any reliance you place on such information is strictly at your own risk.
SQE.IO does not provide legal, regulatory, or financial advice. Readers should consult qualified professionals for guidance tailored to their specific organizational needs and compliance requirements.

Published by SQE.IO
Your World, Quantum-Secure
Learn more at www.sqe.io