International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Incident Response Readiness in the Era of Quantum-Enabled Cryptographic Failure

Esther Mgbolise Osuya *

School of Information Systems & Technology, Strayer University, United States.

International Journal of Science and Research Archive, 2026, 19(03), 798-808

Publication history: Received on 12 April 2026; revised on 16 June 2026; accepted on 19 June 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.19.3.1169

Abstract

Quantum computing is altering the long-term security assumptions that underpin modern digital infrastructure. RSA and ECC, which secure communications, digital signatures, certificate-based trust, and identity systems across virtually every enterprise environment, are theoretically vulnerable to sufficiently capable quantum computers through Shor's algorithm. That vulnerability became operationally significant when NIST finalized its first post-quantum cryptographic standards in August 2024, providing a formal migration path and removing the last credible grounds for strategic delay. This article examines the quantum transition from an operational security perspective, concentrating on three linked problems: the legacy exposure carried by RSA- and ECC-dependent environments, the distinct risks that hybrid post-quantum migration introduces, and the adjustments that incident response and SOC practice require to remain effective during a period of cryptographic instability. Three operationally grounded priorities are identified for defenders, covering cryptographic asset discovery, secure transition management, and incident response preparation. Quantum-enabled cryptographic failure is a present readiness problem, not a distant research concern. Organizations with long-lived sensitive data, extensive public-key dependencies, and complex trust infrastructures face exposure that is already accumulating.

Keywords: Post-quantum cryptography; Incident response; SOC operations; cryptographic agility; Shor's algorithm; Harvest-Now Decrypt-Later

1. Introduction

Public-key cryptography has functioned as the trust infrastructure of the digital world for half a century. RSA and ECC secure TLS handshakes, VPN tunnels, email, certificate authorities, digital signatures, identity systems, package verification, and code signing across enterprise, cloud, and supply chain environments [2], [3], [4], [37]. The security of these mechanisms has never rested on secrecy or operational controls alone; it has rested on the computational intractability of factorization and discrete logarithms. Quantum computing threatens to dissolve that intractability. Shor's algorithm, running on a sufficiently capable quantum processor, solves both problems in polynomial time [3], turning what were once believed to be practically unbreakable keys into derivable ones.

The hardware does not yet exist at the scale required to break deployed systems. However, the trajectory of quantum research has been consistent enough, with demonstrated advances in qubit count, error correction, and coherence time, most recently illustrated by IBM's demonstration of high-threshold fault-tolerant quantum memory [29], that national standards bodies no longer treat migration planning as premature. NIST's finalization of FIPS 203, FIPS 204, and FIPS 205 in August 2024 [7], [21], [8] transformed post-quantum cryptography from an active research program into an engineering obligation. Organizations that had been waiting for a clear destination before committing to migration now have one. The OWASP Top 10:2025 independently reached the same conclusion, designating cryptographic failures as A04:2025 (reclassified from A02 in the 2021 edition) and advising that high-risk systems be post-quantum safe no later than the end of 2030 [9].

* Corresponding author: Esther Mgbolise Osuya

For incident response and SOC practitioners, this transition creates problems that existing frameworks were not designed to handle [1], [12], [13], [33]. Existing IR frameworks assume that certificates prove authenticity, that encrypted channels carry integrity, and that digital signatures verify provenance. Quantum-enabled cryptographic failure does not simply weaken those guarantees; it hollows them out without leaving the indicators that practitioners rely on to detect compromise. An adversary who derives a private key does not need to phish for credentials, exploit a vulnerability, or install malware. They acquire what looks like legitimate access, and the evidence trail reflects that appearance.

This article examines that operational gap. The argument is that quantum-enabled cryptographic failure should be treated as a present readiness problem rather than a future contingency, and that the most urgent task for IR and SOC teams is developing the visibility, procedures, and organizational integration needed to respond effectively during a migration period that is already underway. Three areas anchor the analysis: the legacy exposure embedded in current environments, the specific risks introduced by hybrid migration, and the detection and response adaptations that the transition requires.

2. Quantum Computing and the Cryptographic Threat Model

The distinction between conventional and quantum computing that matters most for security is not raw processing speed but which mathematical problems each can efficiently solve. Conventional computers face an exponential barrier when attempting to factor large integers or compute discrete logarithms. Quantum computers, operating through superposition and interference, do not [4], [5]. Shor's algorithm exploits this difference to factor an n-bit integer in roughly $O(n^3)$ operations, making the factorization underlying RSA and the discrete logarithm underlying ECC tractable rather than prohibitive [3]. This is a mathematical fact about what a sufficiently scaled quantum processor will be able to do.

The operational significance lies in how deeply RSA and ECC are embedded. RSA continues to appear in certificates, legacy PKI systems, code signing, and key exchange. ECC, preferred for its efficiency, dominates digital signatures, mobile environments, constrained devices, and contemporary key agreement protocols. The certificate authority hierarchies that organize trust on the internet, the identity systems that authenticate users and services, the software signing infrastructure that asserts code provenance, the VPN tunnels that protect enterprise communications, and the TLS sessions that secure virtually every web transaction all depend on the mathematical hardness that Shor's algorithm removes [3], [4], [14]. A quantum-capable adversary does not break one of these systems; they gain the ability to undermine all of them simultaneously, because the underlying assumption is shared.

Symmetric cryptography presents a different picture. Grover's algorithm reduces the effective key space of symmetric encryption by half through a quadratic speedup in exhaustive search [10], but it does not collapse symmetric encryption the way Shor's algorithm threatens asymmetric systems. Doubling key length restores security margins, which is why AES-256 remains viable. The consequence for organizations is that the migration burden is not uniform. Symmetric encryption of stored data at rest can be addressed by extending key length. Asymmetric cryptography, which protects data in motion, authenticates identities, and establishes trust chains, requires replacement rather than adjustment.

The incident response implication of this asymmetry is significant. When an adversary derives an RSA private key, the resulting incident does not look like a conventional intrusion. There is no exploit chain, no malicious binary, no anomalous process execution. The adversary authenticates as a legitimate party, signs documents with a valid key, and operates within the bounds of what the compromised system believes is authorized behavior [27], [28]. Investigating such an incident requires trust-layer analysis rather than artifact hunting, and containment requires rebuilding the trust infrastructure itself rather than patching a vulnerability. Neither task appears in traditional IR playbooks.

3. Legacy Cryptography Exposure and Long-Term Data Risk

Quantum computing does not need to be operational for its consequences to be real. The Harvest-Now, Decrypt-Later (HNDL) strategy allows adversaries to collect encrypted data today and defer decryption until capable quantum hardware becomes available [6]. Nation-state intelligence programs are widely believed to be running such campaigns. Mandiant's M-Trends reporting [30] and Verizon's DBIR [32] both document encrypted data exfiltration at nation-state scale, targeting government communications, healthcare records, defense research, financial archives, and strategic intellectual property. These are precisely the data categories that will retain value over the decade-plus timescale that quantum hardware development may require.

The HNDL threat reframes how IR teams should evaluate encrypted exfiltration events. Under pre-quantum assumptions, exfiltration of encrypted data without the corresponding decryption key could be treated as a bounded risk. Under HNDL assumptions, that calculus changes for any data that must remain confidential for years or decades. Large outbound transfers of encrypted data, anomalous access to archival systems, and sustained collection from systems handling long-lived sensitive records are potential future compromises whose full impact may not be knowable until quantum hardware matures. Lenstra and Verheul's key lifetime analysis [6] provides the mathematical basis for estimating which data categories carry the highest retrospective risk: the longer the required confidentiality period, the greater the exposure under HNDL.

The investigation and governance challenges that follow are without precedent in conventional breach response. Data stolen today may not be readable for ten or fifteen years. By that point, the systems involved may have been decommissioned, the personnel who managed them may have moved on, contractual obligations may have expired, and the regulatory frameworks that applied at the time of theft may have changed. Evidence preservation standards developed for conventional breaches assume that the impact of an incident becomes apparent within months; they provide no guidance for an incident whose impact is deferred by the maturation of adversary capabilities.

Regulatory exposure compounds this. GDPR, HIPAA, and sector-specific financial data regulations impose breach notification obligations when personal data is compromised. Whether those obligations are triggered at the moment of exfiltration or at the moment of decryption is legally unsettled in the context of HNDL. Organizations in healthcare, financial services, defense contracting, and government supply chains should engage legal and compliance teams in their HNDL risk assessment process now, before an incident forces the question. The time to document an organization's interpretation of its regulatory obligations under quantum threat assumptions is during planning, not during a response.

The practical implication for security programs is to treat data longevity and sensitivity as first-order classification criteria alongside conventional risk factors. Inventorying which systems handle data with confidentiality requirements beyond five years, and prioritizing those systems in both migration and monitoring, is a direct response to the adversarial behavior that is already documented in threat intelligence. There is a specific failure mode worth naming: organizations that assess HNDL risk purely through the lens of current encryption strength, asking whether today's key lengths are computationally secure today, are answering the wrong question. The question is whether encrypted data that adversaries may already hold will remain inaccessible over the confidentiality period that data requires. An organization encrypting healthcare records at RSA-2048 today is making an implicit bet that no adversary will have quantum decryption capability for as long as those records need to stay confidential. Making that assessment explicit, documenting it, and revisiting it as quantum hardware development progresses, is the minimum required for responsible data stewardship under current threat conditions.

4. NIST Standardization and the Urgency of Migration

Before August 2024, many organizations treated post-quantum preparation as strategically premature. The counterargument was reasonable: committing to migration before the destination architecture was settled risked investing in the wrong algorithms. NIST's finalization of FIPS 203, FIPS 204, and FIPS 205 [7], [21], [8], [20] closed that window; the destination is settled. FIPS 203 standardizes ML-KEM for key encapsulation, FIPS 204 standardizes ML-DSA for digital signatures, and FIPS 205 standardizes SLH-DSA as a hash-based alternative for signing. These are published federal information processing standards with a formal migration pathway established in NIST IR 8547 [11].

ENISA [23],[24] and the NSA's CNSA 2.0 [25] have published parallel requirements for European and US national security contexts respectively. The NSA's timeline is particularly concrete: new system acquisitions must support quantum-resistant cryptography from 2027, and software and firmware signing must reach exclusive use of CNSA 2.0 algorithms from January 2027 [25]. Across these bodies the picture is one of near-term action within a 2027–2035 window rather than a single shared date: NSA's CNSA 2.0 begins in 2027 [25], OWASP sets end-of-2030 as the target for high-risk systems [9], and NIST's draft transition roadmap deprecates RSA and ECC by 2030 and disallows them by 2035 [11]. That convergence across independent standards bodies should be read as a definitive signal. Security leaders who cited the absence of stable standards as grounds for deferral no longer have that argument available.

The harder question now is how to migrate without introducing new vulnerabilities in the process. Post-quantum algorithms bring operational challenges that have no direct analogy in the transition from DES to AES: ML-KEM and ML-DSA produce significantly larger keys and signatures than their RSA and ECC counterparts, which affects bandwidth, storage, and processing overhead at scale [14]. More immediately, the hybrid deployment period, during which pre-

quantum and post-quantum cryptography coexist to maintain backward compatibility, creates a new and poorly understood attack surface [18].

Bindel et al. [26] analyzed the specific challenges of transitioning to a quantum-resistant public key infrastructure and found that the hybrid period is the most operationally complex phase of the migration. Hybrid key exchange implementations must be correct on both the pre-quantum and post-quantum sides simultaneously, and failures in either can be exploited. Protocol negotiation between hybrid and legacy endpoints introduces downgrade risks: an adversary who can force a negotiation back to a pre-quantum-only key exchange has effectively neutralized the post-quantum component. Implementation errors in new PQC libraries, which have not had decades of production hardening, may leak key material through side channels not present in mature RSA or ECC implementations. These represent the specific conditions under which the migration period becomes an attack opportunity rather than a security improvement.

The operational implication is that PQC migration must be treated as a monitored security program, not a background infrastructure upgrade. Downgrade events, negotiation failures, library errors, and anomalous fallback behavior during hybrid deployments require detection and investigation. Certificate governance during the transition, including the lifecycle management of both pre-quantum and post-quantum certificates for the same systems, requires explicit policy and tooling. Prioritizing migration across a heterogeneous environment requires knowing where public-key cryptography is used, meaning the discovery program is a prerequisite for migration.

The migration timeline question shapes how urgently organizations act. Mosca [22] formalized the problem: if the time needed to complete migration exceeds the time before capable quantum hardware exists, preparation is already overdue. Recent algorithmic advances have sharpened the resource picture considerably. In July 2025, Craig Gidney of Google Quantum AI published an estimate that RSA-2048 could be factored in less than a week by a quantum computer with fewer than one million noisy qubits [35], reducing the previous leading estimate of twenty million qubits by more than an order of magnitude. Each order-of-magnitude reduction brings the attack closer to the hardware that quantum engineering programs are building toward. Current expert estimates for cryptographically relevant quantum computers range from ten to twenty years, with significant variance [5], but if capable hardware arrives in a decade, organizations that begin planning in five years will not be finished in time. The organizations with the most to lose, those managing national security information, critical infrastructure, long-lived regulated data, and strategic intellectual property, must assume that preparation must begin now and proceed continuously.

5. Implications for Incident Response

Existing IR models were built on a stable assumption: the cryptographic infrastructure used to authenticate parties, verify software, and protect communications during an investigation is itself trustworthy. Certificates validate identity, digital signatures verify integrity, and encrypted channels carry evidence without alteration. Quantum-enabled cryptographic failure attacks that assumption directly, creating IR challenges that existing frameworks do not address [1], [12], [13].

Consider what happens when a certificate authority's private key is derived by a quantum-capable adversary. The adversary can issue certificates for any domain that appear fully valid under every standard validation check. Malicious software carrying one of those certificates appears legitimately signed, servers presenting those certificates appear authentic, and communications encrypted to those keys appear protected. An IR team responding to an incident in such an environment faces a problem that has no precedent in conventional incident response: the trust infrastructure they rely on to determine what is legitimate may itself be compromised. They cannot assume that a valid certificate proves authenticity, that a properly signed binary is safe to execute, or that an encrypted log archive has not been altered. The investigation starts from a posture of reduced assurance.

Silent compromise deepens this problem. In a conventional intrusion, adversaries leave traces: exploit artifacts, anomalous process execution, lateral movement patterns, credential abuse. A quantum-enabled adversary who has derived a private key may leave none of these. They authenticate using what appears to be a legitimate key, operate within the permissions that key grants, and exit without deploying malware or triggering behavioral anomalies [28]. The dwell time in such a scenario is bounded primarily by operational objectives rather than detection capability. Irumudomon [34] documents that IR teams already face significant detection delays in conventional environments; quantum-enabled silent compromise extends those delays in ways that conventional security telemetry alone cannot address.

Forensic integrity presents a third complication. Encrypted forensic images, encrypted log archives, and cryptographically signed audit records are treated as trustworthy during investigations precisely because their integrity appears to be guaranteed. If the encryption or signing mechanisms protecting that material become breakable, an adversary with quantum capabilities could decrypt a stored forensic image, alter its contents, re-encrypt it, and leave no detectable evidence of modification. This means that the chain of custody practices and evidence preservation standards developed for conventional breach environments require review.

IR planning should therefore expand to address trust-specific questions that do not appear in current playbooks: which cryptographic assets are exposed, whether trust anchors remain valid, whether exfiltrated data carries long confidentiality requirements, and when response requires certificate revocation at scale, trust chain rebuilding, or notification of vendors and dependent parties. Mass certificate revocation in particular is a response action that most organizations have never executed, and the coordination required is genuinely novel.

Consider an organization that discovers, through CT log monitoring, that a certificate for one of its API domains was issued by an unrecognized certificate authority. Under conventional threat assumptions, the explanations are a misconfigured internal CA, shadow IT, or phishing-related certificate abuse. Under quantum transition assumptions, the possibility that a trusted CA's private key was compromised by a capable adversary must also be on the table. If the CA's key has been derived, every certificate it has issued must be treated as potentially forged, and the revocation scope extends to the CA's entire issuance history. That scale of response requires pre-existing runbooks, pre-established communication channels, and organizational authorization structures to implement decisions quickly. Most organizations do not have those in place.

6. SOC Readiness in Hybrid Cryptographic Environments

Widespread quantum-enabled breakage of deployed RSA or ECC has not occurred. But the migration period has begun, and hybrid environments are already creating conditions that SOC teams need to monitor. Certificate issuance anomalies, TLS downgrade events, PQC negotiation failures, and KMS access irregularities all carry signals relevant to quantum transition risk, and none of them appear in standard SOC detection playbooks. The gap is not primarily a technology gap; most existing SIEM platforms can ingest certificate transparency logs, TLS handshake metadata, and key management system audit events with modest configuration effort. The gap is one of awareness, prioritization, and analytic framing.

Certificate transparency logs are underused as a security telemetry source in most environments. Every publicly trusted certificate is logged to CT infrastructure at issuance, making CT monitoring a near-real-time feed of certificate activity for organizational domains [38]. Anomalies can indicate unauthorized trust establishment, supply chain compromise, or, in a quantum context, forged certificates issued using derived private keys. TLS telemetry complements this by revealing what cipher suites and key exchange algorithms are actually being negotiated in production, which matters during migration because the difference between a hybrid TLS deployment and a successful pre-quantum-only downgrade may appear only in handshake metadata [14], [15], [37]. Key management system logs close the loop by exposing what is happening to the keys themselves: export attempts, deletion scheduling, and unusual API access to cryptographic material are indicators that may precede a larger compromise [27].

Behavioral monitoring of encrypted traffic requires a shift in interpretive framing. Large outbound encrypted data transfers have always been a detection priority, but under HNDL assumptions, the significance of such events depends heavily on what data was involved and how long it needs to remain confidential. Without data longevity and sensitivity context, SOC analysts cannot make that distinction, and cannot assess whether an event represents a bounded incident or a potential future strategic compromise [30], [32].

Hybrid deployments make analysis more demanding because not all anomalies are adversarial. PQC negotiation failures during a phased rollout are expected. The challenge is distinguishing expected migration noise from deliberate downgrade attacks or exploitable misconfigurations, which requires both technical pattern recognition and organizational context. Developing that capacity requires deliberate investment in analyst training and tabletop exercises that simulate hybrid migration scenarios.

Table 1 SOC telemetry sources and their quantum-era significance

Telemetry Source	What to Monitor	Quantum-Relevant Significance
Certificate Transparency Logs	Unauthorized issuances, unexpected CAs, revocation anomalies, unusual renewal patterns [38]	Early indicator of PKI compromise or quantum-enabled certificate forgery; baseline required before incidents occur
TLS Handshake Logs	Deprecated cipher suites, negotiation failures, fallback to pre-quantum algorithms, hybrid key exchange errors [14],[15]	Distinguishes benign rollout errors from downgrade attacks and PQC misconfigurations during the migration period
Key Management System Events	Export attempts, deletion scheduling, unauthorized access to key material, API anomalies	Nation-state actors target KMS infrastructure to extract private keys; unauthorized key export is almost always malicious [27], [28]
Encrypted Data Transfer Volume	Large outbound transfers, archive access patterns, backup system anomalies, sustained collection from high-value systems [30],[32]	HNDL collection indicators; evaluated against data longevity and regulatory sensitivity to assess strategic compromise risk

7. Cryptographic Agility as a Readiness Requirement

Cryptographic agility is the capacity to identify, replace, and govern cryptographic mechanisms across an organization's technology stack without requiring full-scale system replacements or extended operational outages. In architectures designed for it, changing a cryptographic algorithm is an administrative operation; in architectures that were not designed for it, it is a multi-year engineering program. The distinction matters enormously in the quantum transition, because organizations that lack cryptographic agility will find that they cannot respond to the migration deadline they now face, and cannot respond effectively to cryptographic incidents if one occurs during the migration period.

The foundational requirement is inventory. Most organizations do not have a complete accounting of where RSA or ECC appears in their environments. Without a complete and continuously maintained cryptographic asset inventory, the organization cannot prioritize migration intelligently, cannot assess the blast radius of a suspected cryptographic compromise, and cannot determine whether a given incident has exposed a high-value key or a low-risk one. Mosca [22] established the fundamental problem: migration must be completed before capable quantum hardware emerges, and that requires making prioritized decisions now under conditions of uncertainty about the timeline. An inventory is the precondition for any of those decisions being defensible.

Beyond inventory, agility requires modular cryptographic libraries that allow algorithm replacement without application rewrites, centralized certificate lifecycle management, and explicit algorithm policy. The Open Quantum Safe project's liboqs library [19] provides a reference implementation framework that supports this modularity for PQC algorithms, but organizational value depends entirely on whether surrounding governance structures exist. Governance without inventory is guessing; inventory without governance is a spreadsheet that no one acts on.

Vendor and supply chain dependencies deserve particular attention. Many organizations' most significant cryptographic exposures are not in systems they control directly but in systems and services controlled by third parties. Procurement and third-party risk management functions must be engaged to extend PQC requirements into vendor contracts. An organization that has migrated its own infrastructure but continues to depend on vendors running vulnerable cryptographic mechanisms has not actually reduced its exposure; it has relocated it.

The regulatory landscape reinforces this point directly. The EU Cyber Resilience Act, Regulation (EU) 2024/2847 [36], entered into force in December 2024 and applies fully from December 2027. It requires manufacturers of products with digital elements sold on the EU market to support updates to cryptographic mechanisms over the product lifecycle, which is a legal codification of cryptographic agility as an engineering requirement rather than a security best practice.

One pattern that consistently undermines cryptographic agility programs is the gap between the inventory and the action it is supposed to enable. Organizations conduct certificate discovery exercises but struggle to translate that inventory into migration decisions because ownership, risk context, and business dependency information was not captured. An inventory that records algorithm type and expiration date but not system owner, data classification, or

business impact is an incomplete instrument. Building that context into the discovery program from the start is what separates a cryptographic inventory from a cryptographic governance program.

8. Software Supply Chain Integrity and Post-Quantum Trust

Quantum-enabled cryptographic failure extends into software supply chains in ways that deserve separate treatment. Code signing, package repository verification, firmware update authenticity, and CI/CD artifact validation all depend on RSA or ECC [3]. This means that a quantum-capable adversary who can derive signing keys gains the ability to distribute malicious software through trusted delivery channels without triggering signature verification failures. The consequences reach beyond encrypted communications into the mechanisms by which software is delivered, updated, and trusted.

The 2020 SolarWinds compromise reached approximately 18,000 organizations through a trusted software update mechanism. Investigators identified the compromise through a combination of behavioral anomalies and partial cryptographic evidence from the build environment. A quantum-enabled version of that attack removes the cryptographic evidence entirely. Signed updates would pass all verification checks because the signatures would be mathematically valid. Attribution would depend entirely on post-deployment behavioral analysis, which typically requires the malicious payload to have executed and produced observable effects before detection begins [16], [17]. The 2025 Bybit supply chain attack, which resulted in a $1.5 billion theft through targeted compromise of a trusted interface, illustrates how consequential supply chain attacks have become even without quantum capabilities. Quantum capabilities would expand the attack surface available to such operations considerably.

For IR teams, this means two things. First, the scope of cryptographic asset discovery must include signing infrastructure: code signing certificates, certificate authorities that issue signing certificates, package signing keys, and firmware signing mechanisms. These assets are often managed outside the security team's visibility. Second, IR playbooks must explicitly address the scenario where a software update or package delivered through a trusted channel is suspected of containing malicious code that passed signature verification. That scenario requires broad distrust of signed artifacts from a specific publisher, coordinated rollback, and investigation of the signing infrastructure itself.

The relationship between supply chain trust and post-quantum migration also runs in the other direction. Organizations deploying new PQC libraries through their software distribution infrastructure are implicitly relying on the integrity of that infrastructure. If the signing keys protecting the distribution channel for PQC libraries are themselves vulnerable to quantum-enabled forgery, an adversary could substitute malicious implementations of PQC algorithms for legitimate ones, creating an update that appears to improve security while actually introducing a backdoor. Monitoring code signing certificate lifecycles, validating build artifact provenance, and treating unexpected changes in signing key material as high-priority anomalies should be standard practice.

9. Practical Priorities for Defenders

Three priorities follow from the preceding analysis, ordered by operational dependency.

9.1. Discovery

Discovery comes first. Before migration can be prioritized and before incidents can be scoped, the organization needs to know where RSA and ECC appear. Automated certificate discovery tools can cover the publicly visible surface. Software composition analysis tooling extended to flag PQC library readiness, consistent with ENISA guidance [23] and NSA CNSA 2.0 requirements [25], covers the software dependency layer. Questionnaires and contractual requirements must cover vendor dependencies that cannot be assessed directly.

The output should be a tiered risk register that ranks assets by algorithm type, data longevity, business criticality, and migration feasibility. Under Lenstra and Verheul's key lifetime analysis [6], systems handling data with confidentiality requirements beyond ten years should be treated as the highest HNDL priority. Discovery should also map cryptographic dependencies, not just assets. Building dependency mapping into the discovery process rather than attempting to reconstruct it under incident pressure is the difference between a response team that can make revocation decisions confidently and one that must spend the first hours of a response conducting basic discovery work.

9.2. Securing the Transition

Securing the transition is the second priority, and it runs in parallel with migration itself. Hybrid deployments should be treated as security-monitored activities rather than engineering projects: CT log monitoring and KMS alerting should be in place before hybrid certificates are issued, PQC negotiation telemetry should be baselining before hybrid TLS is deployed, and downgrade resistance should be explicitly tested [14], [26]. Deploying hybrid TLS using ML-KEM per FIPS 203 [7] on externally facing services ahead of full internal migration is a practical near-term measure; it adds quantum-resistant key encapsulation to perimeter communications without requiring complete algorithm replacement across internal systems.

9.3. Preparing the Response

Preparing the response is the third priority. IR playbooks need to address certificate revocation at scale, trust-anchor validation, suspected signature forgery, encrypted data theft involving long confidentiality lifetimes, and coordinated recovery of communications, identity, and software trust functions. Tabletop exercises should specifically test the organization's ability to execute mass revocation, rebuild PKI trust chains, and communicate certificate-related impacts to vendors and dependent parties under realistic time pressure [1], [34]. Finding decision bottlenecks and coordination gaps during a rehearsal is considerably less costly than finding them during an active incident.

Table 2 Practical priorities for quantum transition readiness

Priority	Key Actions	Owner	Timeline
1. Discover Exposure	Automated certificate discovery classified by algorithm, expiry, and data longevity [11]. HNDL data map for stores with 10+ year confidentiality requirements [6]. SCA tooling extended to PQC library readiness [23],[25]. Vendor migration questionnaires.	PKI / Security Architecture / Data Governance	0-30 days
2. Secure the Transition	CT log monitoring and KMS alerting deployed before hybrid certificate issuance [38],[27]. PQC negotiation telemetry baselined before hybrid TLS rollout [14]. Hybrid TLS (ML-KEM per FIPS 203 [7]) on perimeter services. Downgrade resistance tested.	SOC Engineering / Security Engineering / Procurement	0-90 days
3. Prepare the Response	IR playbooks updated for certificate revocation at scale, trust-anchor validation, and HNDL impact assessment [1],[13]. Tabletop exercise simulating trust-layer compromise including mass revocation. Executive briefing on quantum readiness posture and regulatory obligations [31].	IR Team / CISO / Legal and Compliance	30-90 days

10. Discussion

The argument running through this article is narrower than the full scope of quantum computing's security implications, and deliberately so. Quantum computing intersects with many distinct strategic areas, but a paper that attempts to address all of these at once rarely addresses any of them well. The contribution here is more specific: quantum-enabled cryptographic failure is already producing operational conditions that IR and SOC teams need to respond to, independent of when capable quantum hardware fully emerges, because the migration itself creates the conditions.

The evidence for this is not speculative. OWASP sets end-of-2030 as the target for high-risk systems, NSA's CNSA 2.0 phases in quantum-resistant algorithms from 2027, and NIST's draft roadmap deprecates RSA and ECC by 2030 and disallows them by 2035 [9], [11], [25]. Migration has begun, hybrid environments are being deployed, vendors are publishing PQC library updates, and certificate authorities are preparing to issue post-quantum certificates. The HNDL threat is not waiting for quantum hardware; it is running on conventional computers today, collecting data that will be decrypted later. Mandiant [30] and Verizon [32] document the collection campaigns, and IBM's breach cost research [31] quantifies what is at stake financially. The operational burden is real now.

What this analysis does not do is claim that quantum hardware will emerge by a particular date, or that the migration will be completed before capable machines exist. Those claims cannot be substantiated. What can be substantiated is that the adversarial timeline is decoupled from the engineering timeline, that HNDL collection is already underway, and

that the migration period itself creates a window of elevated risk that will persist for years. Practitioners who treat preparation as contingent on demonstrated quantum capability are, in effect, choosing to prepare after the fact.

There is also a broader professional implication worth acknowledging. IR curricula, certification programs, and practitioner frameworks were built on assumptions of cryptographic stability. The quantum transition does not make those questions permanently unanswerable, but it does require that they be asked explicitly rather than assumed. The profession's shared knowledge base, its detection patterns, playbook templates, forensic practices, and governance frameworks, will need to evolve accordingly.

11. Conclusion

RSA and ECC are not going to be broken tomorrow. But they are going to be broken, and the preparation required to maintain security through that transition is substantial, time-consuming, and operationally complex enough that organizations which have not started are already behind. NIST provided the standards in August 2024. OWASP aligns on a 2030 target for high-risk systems, with NSA and NIST timelines pointing to the same 2027–2035 window. The migration pathway is clear. The primary remaining variable is organizational will to treat this as a present operational security problem rather than a future engineering concern.

For IR and SOC practitioners, the most immediate obligation is developing visibility into the trust layer: certificate transparency monitoring, TLS telemetry, KMS alerting, and data longevity context for encrypted exfiltration events. None of these require new technology investments; they require configuration, training, and integration into existing detection workflows. The playbook updates required are more demanding, because rehearsing mass certificate revocation, trust-chain rebuilding, and quantum-aware forensic evidence handling requires organizational coordination that takes time to develop. Starting that work now means that when an incident occurs, response is bounded by preparation rather than by the time it takes to understand the problem for the first time.

The adversaries most likely to acquire quantum capabilities earliest are the same nation-state actors already conducting HNDL collection campaigns against high-value targets. That alignment reflects a strategic understanding, already apparent in adversarial behavior, that the value of encrypted data today is a function not only of its current inaccessibility but of its future decryptability. Defenders who wait for visible quantum capability before responding will find that the collection of the data they are trying to protect has already been accomplished. Preparation before that point is the appropriate response to an adversarial timeline that is already running.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] ISO/IEC 27035-1:2023. Information Technology - Information security incident management - Part 1: Principles and process. Available from https://www.iso.org/standard/78973.html

[2] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120-126. Available from https://dl.acm.org/doi/epdf/10.1145/359340.359342

[3] Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. Proc 35th Annu Symp Found Comput Sci. 1994;124-134. Available from https://cc.ee.ntu.edu.tw/~rbwu/rapid_content/course/QC/Shor1994.pdf

[4] Aaronson S. Quantum Computing Since Democritus. Cambridge: Cambridge University Press; 2013.

[5] Preskill J. Quantum computing in the NISQ era and beyond. Quantum. 2018;2:79. Available from https://quantum-journal.org/papers/q-2018-08-06-79/pdf/

[6] Lenstra AK, Verheul ER. Selecting cryptographic key sizes. J Cryptology. 2001;14:255-293. Available from https://www.cs.ru.nl/E.Verheul/papers/PKC2000-2/PKC2000-2.pdf

[7] National Institute of Standards and Technology. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). Gaithersburg, MD: NIST; Aug 2024. Available from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[8] National Institute of Standards and Technology. FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA). Gaithersburg, MD: NIST; Aug 2024. Available from https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.205.pdf

[9] OWASP Foundation. A04:2025 – Cryptographic Failures. OWASP Top 10:2025; 2025. Available from https://owasp.org/Top10/2025/A04_2025-Cryptographic_Failures/

[10] Grover LK. A fast quantum mechanical algorithm for database search. Proc 28th Annu ACM Symp Theory Comput. 1996;212-219. Available from https://dl.acm.org/doi/epdf/10.1145/237814.237866

[11] Moody D, Perlner R, Regenscheid A, Robinson A, Cooper D. NIST IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards. Gaithersburg, MD: National Institute of Standards and Technology; Nov 2024. doi:10.6028/NIST.IR.8547.ipd. Available from https://csrc.nist.gov/pubs/ir/8547/ipd

[12] National Institute of Standards and Technology. SP 800-61r3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management NIST; 2025. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

[13] ISO/IEC 27035-2:2023. Information technology – Information security incident management - Part 2: Guidelines to plan and prepare for incident response. ISO; 2023.

[14] Stebila D, Mosca M. Post-quantum key exchange for the Internet and the Open Quantum Safe project. Proc 9th Int Conf Post-Quantum Cryptography. 2017;1-24. Available from https://eprint.iacr.org/2016/1017.pdf

[15] Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Internet Engineering Task Force; 2018. Available from https://datatracker.ietf.org/doc/html/rfc8446

[16] OWASP Foundation. A03:2025 - Software Supply Chain Failures. OWASP Top 10:2025; 2025. Available from: https://owasp.org/Top10/2025/A03_2025-Software_Supply_Chain_Failures/

[17] OWASP Foundation. A08:2025 – Software or Data Integrity Failures. OWASP Top 10:2025; 2025. Available from: https://owasp.org/Top10/2025/A08_2025-Software_or_Data_Integrity_Failures/

[18] ETSI TR 103 619: Cyber; Migration strategies and recommendations to Quantum Safe schemes Version 1.1.1. ETSI; 2020. Available from https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[19] Open Quantum Safe Project. liboqs: C library for quantum-safe cryptography. Available from: https://openquantumsafe.org

[20] National Institute of Standards and Technology. Post-Quantum Cryptography 2024. Available from: https://csrc.nist.gov/projects/post-quantum-cryptography

[21] National Institute of Standards and Technology. FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA). Gaithersburg, MD: NIST; Aug 2024.

[22] Mosca M. Cybersecurity in an era with quantum computers: will we be ready? Cryptology ePrint Archive, Paper 2015/1075; 2015. Available from https://eprint.iacr.org/2015/1075

[23] ENISA. Post-Quantum Cryptography: Current State and Quantum Mitigation. European Union Agency for Cybersecurity; 2021. Available from: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

[24] ENISA. Post-Quantum Cryptography - Integration study. European Union Agency for Cybersecurity; 2022. Available from: https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

[25] National Security Agency. Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ. NSA; 2022. Available from: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

[26] Bindel N, Herath U, McKague M, Stebila D. Transitioning to a quantum-resistant public key infrastructure. In: Lange T, Takagi T, editors. Post-Quantum Cryptography. PQCrypto 2017. Lecture Notes in Computer Science, vol 10346. Cham: Springer; 2017. p. 384-405. doi: 10.1007/978-3-319-59879-6_22

[27] Boneh D, Shoup V. A Graduate Course in Applied Cryptography. 2020. Available from: https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_5.pdf

[28] Bishop M. Computer Security: Art and Science. 2nd ed. Boston: Addison-Wesley; 2018.

[29] Bravyi S, Cross AW, Gambetta JM, Maslov D, Rall P, Yoder TJ. High-threshold and low-overhead fault-tolerant quantum memory. Nature. 2024 Mar;627(8003):778-782. doi: 10.1038/s41586-024-07107-7.

[30] Mandiant. M-Trends 2024: Insights into Today's Cyber Attacks. Mandiant; 2024.

[31] IBM Security. Cost of a Data Breach Report 2024. IBM; 2024.

[32] Verizon. 2024 Data Breach Investigations Report. Verizon; 2024.

[33] Barrett-Danes F, Ahmad F. Quantum computing and cybersecurity: A rigorous systematic review of emerging threats, post-quantum solutions, and research directions (2019-2024). Discov Appl Sci. 2025.

[34] Irumudomon O.I. A Qualitative Study of the Impact of Time from an Incident Responder's Perspective Within the United States Cybersecurity Industry [doctoral dissertation]. Colorado Technical University; 2024.

[35] Gidney C. How to factor 2048 bit RSA integers with less than a million noisy qubits. arXiv. 2025. DOI: 10.48550/arXiv.2505.15917

[36] European Parliament and Council of the European Union. Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union. 2024.

[37] Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Boston: Pearson; 2020.

[38] Laurie B, Langley A, Kasper E. Certificate Transparency. RFC 6962. Internet Engineering Task Force; Jun 2013 (obsoleted by RFC 9162, Dec 2021). Available from https://datatracker.ietf.org/doc/html/rfc6962