Quantum and the Cybersecurity Imperative

The few past years mark another step in the ongoing evolution of cybersecurity. As organizations continue their digital transformation, cyber threats are evolving in parallel.

In addition to the usual attack vectors, AI is rapidly transforming cybersecurity – not just for the defenders but also for the attackers. Malicious actors are leveraging AI to automate attacks, evade detection, and exploit vulnerabilities with greater speed and sophistication. Likewise, the cybersecurity risks associated with IoT continue to grow. Each connected device represents a potential entry point for attackers, making IoT security a critical priority.

Then, the cherry on the cake: the foreseeable quantum threat, which force us to prepare for a major cryptographic change. Quantum computing is progressing rapidly, and while no one can predict exactly when it will break current encryption at scale, it's just a question of time until existing cryptographic methods will become obsolete.

And as it wasn't enough, we start to see some pressure from various national agencies obliging organizations to adopt quantum resiliency rather soon than later. As an example, just recently, the France's national cybersecurity agency announced they will stop certifying security products that do not include quantum-resistant encryption beginning in 2027. It is a de facto phase-out of older encryption across the systems that matter most.

This results in an urgent need to rethink cyber defences, which requires shifting from reactive prevention to proactive resilience. You have to stay ahead of rapidly evolving encryption standards with crypto-agile solutions that are truly quantum resilient. For this, we need to frame our future crypto architecture around 3 main pillars:

1. Crypto agility, which will be essential for adapting to evolving standards and addressing newly discovered vulnerabilities. A must have moving forward, and although this sounds like an obvious step forward, it will require a complete reshaping of most current crypto infrastructures.
   Furthermore, the goal is not about swapping algorithms; it's about preserving trust while cryptography changes.

2. Defence-in-depth, which is a cybersecurity strategy that uses multiple, independent, and overlapping security layers to better protect an organization and to ensure improved resilience.

3. Long lasting protection, which consists of building a resilient, long-term security posture, and which requires a combination of core architectural and technical practices. Addressing the HNDL attacks is a good example on how this concept can be concretely activated already today.

Forward-looking organizations now have the opportunity to use today to prepare for tomorrow's quantum impacts. The risk is you do little or nothing… until you are forced to. Standards are advancing, but readiness is not. The time is now. Although no one knows exactly when or where QC attacks will occur, the progression of technology makes the likelihood of their occurrence a true and major risk. The quantum clock is ticking, faster and faster. Quantum risk is no longer theoretical—it's an infrastructure and security challenge organizations need to address rather sooner than later.

Being a bit provocative, I would add that, regardless of whether you consider quantum to be a threat, or not, if you don't migrate to the newer algorithms, you'll simply be disconnected from the rest of the world…
There is no bad luck, only bad preparation and lack of anticipation. We have to adapt. Now.

This also represents a unique opportunity to improve our existing (legacy) crypto infrastructure. How? By moving to a new reference architecture, employing multiple quantum resistant mechanisms, incorporating guidance on use of symmetric key cryptography and employing high entropy (QRNG), PQC and QKD, all in a hybrid architecture, as hybridization will become the norm.

Finally, moving to quantum resiliency is not just a future migration problem; it's also a visibility and control problem today, where robust Key and Policy Management will become critical, as an essential building block of any crypto deployment moving forward, not only by enabling crypto agility across your organisation, but also by connecting and controlling all these quantum resistant mechanisms, centrally, and through some automated remediation processes.

In conclusion, there is an urgent need to fundamentally rethink our crypto architecture, to reframe it, in order to support flexible crypto deployment, to guarantee interoperability, enhanced control and visibility, and where key management, at scale, will become central.

By the time cryptographically relevant quantum computers arrive, resilience will depend on the concrete steps you take today. There is a need for any organization to begin its quantum-safe migration journey now, focusing on high-impact systems first. Develop your quantum-safe transition roadmap without any further delay. This will also help you to address some of the new AI and other attack vectors, which are equally, or arguably more, a threat to cyber security.

Also remember, the cost and difficulty of migrating from one algorithm to another, or of changing the size of the keys, should not be underestimated. This why crypto agility by-design must be considered to allow much quicker algorithm migration in the future. Start to implement it now.

Finally, organizations that embrace both quantum-resistant and quantum-native approaches will be best positioned to lead in a post-quantum world. This dual strategy not only mitigates risk but also signals technological leadership and regulatory foresight. Furthermore, by prioritizing crypto agility and modern key management now, you will be far better positioned to adapt—without disruption—as requirements evolve.

PQC and Key Management References:

NSA COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC) Symmetric Key Management Requirements

NIST Recommendation for Key Management (Initial Public Draft)

PQCC June 2026 Heatmap: Current State of PQC Standards and Adoption

QLABS Symmetric Key Management in the Era of NIST Standards

QLABS Innovative Approaches to Key Management

QLABS Key Management Best Practices