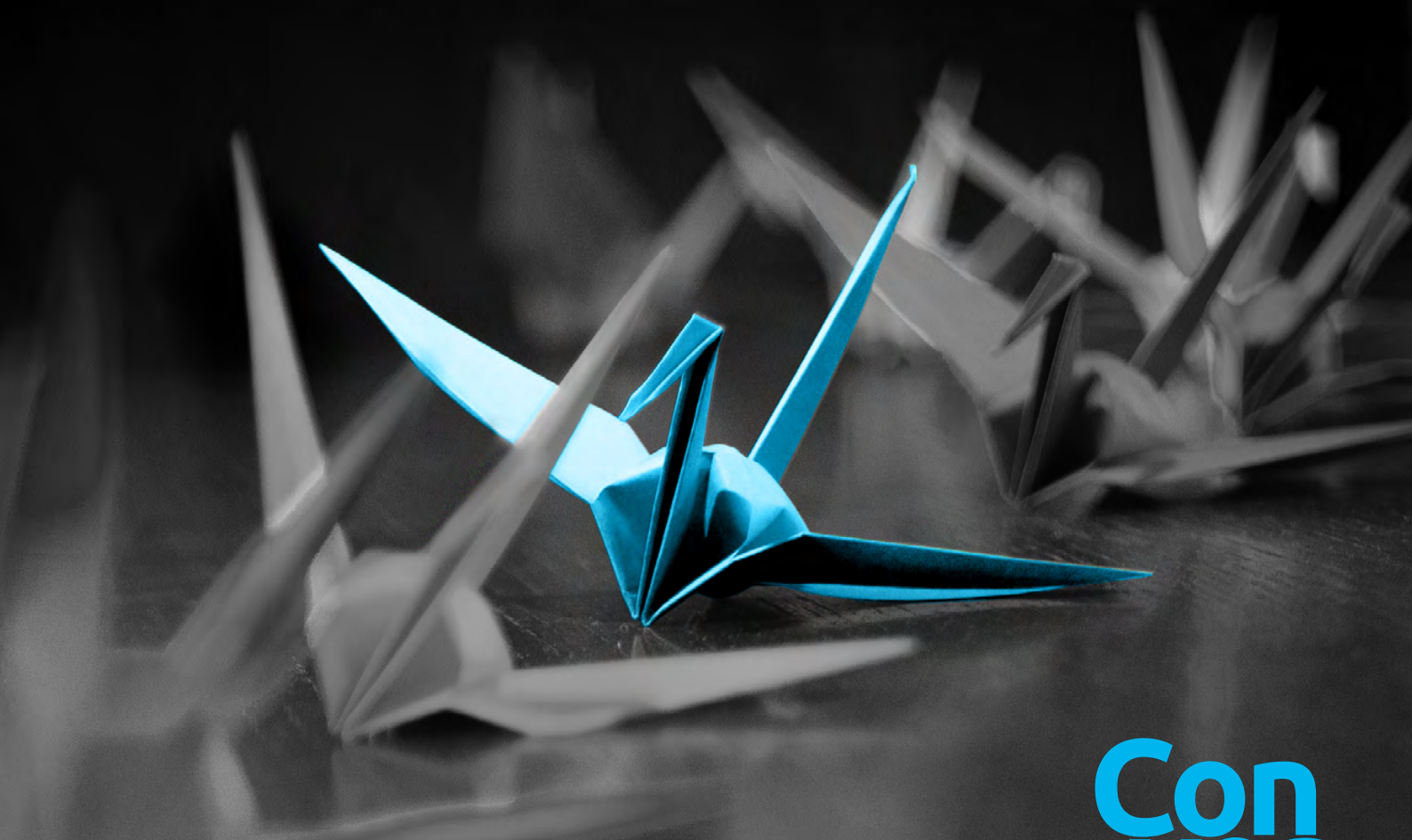
Capgemini RESEARCH INSTITUTE

Crafting Tomorrow

Leaders' perspectives on technology



Conversations FOR TOMORROW

N°10 — 2025

Executive conversations with...

MICHELE MOSCA

CEO

evolutionQ

BECOMING QUANTUM-SAFE

Michele Mosca is CEO and co-founder of evolutionQ, a cybersecurity company that pioneered quantum risk management and the BasejumpTM software product suite that enables scalable cryptographic resilience. Prior to co-founding evolutionQ, Michele co-founded the Institute for Quantum Computing while being a Professor of Mathematics at the University of Waterloo, Canada. He is a founding member of the Perimeter Institute for Theoretical Physics and his work on quantum computing and quantum-safe cryptography is widely cited.

Can you begin by telling us about your journey into the quantum-safe cryptography space?

Michele Mosca: I've been working at the intersection of cryptography and quantum computing since the 1990s – before the two were overtly connected. Over the past decade, I've shifted toward commercialization. Initially through services and, over the past five years, by building out a product company to address the need for cryptographic modernization, including quantum readiness and overall readiness for a cryptographic zero-day.

Michele Mosca
CEO, evolutionQ

How would you describe the current state of awareness around quantum-safe cryptography?

Michele Mosca: Awareness has definitely increased, owing in part to organizations such as Google and IBM. But we're still not where we need to be. Most people see this as a "one-problem-one-solution" situation. What they need to understand is that the quantum threat is just a visible example of

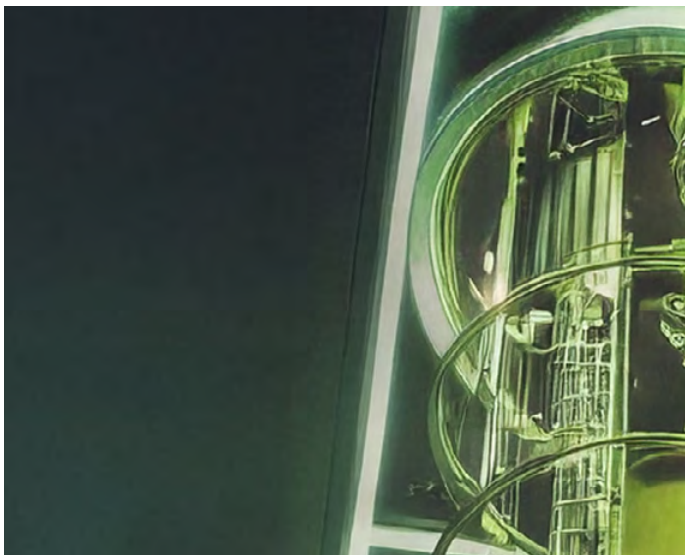
> **"The quantum threat is just a visible example of the things that could go wrong with our cryptographic foundations. We don't know the limits of quantum computing"**

the things that could go wrong with our cryptographic foundations. We don't know the limits of quantum computing and, with AI accelerating, it's becoming even more difficult to predict future vulnerabilities.

There are two waves of awareness. First, we must recognize that there is a threat. Second, and more profoundly, we have to accept that it's not going to go away. On the contrary, code-breaking threats will keep evolving, and our systems must be resilient by design. Just as we moved from passwords to multi-factor authentication, our key exchange and cryptographic practices must also become layered and agile. But agility alone is not enough. If your infrastructure is hijacked and money is stolen, you must be resilient.

"There are two waves of awareness. First, we must recognize that there is a threat. Second, and more profoundly, we have to accept that it's not going to go away"

> **Transitioning to quantum-safe cryptographic infrastructure is a complex, multi-year process"**



Why do you think there is an urgency to address the quantum threat?

Michele Mosca: A few key risks drive urgency. Firstly, transitioning to quantum-safe cryptographic infrastructure is a complex, multi-year process. Organizations that underestimate this challenge risk rushed, poorly executed migrations that could leave critical systems exposed and lead to prolonged operational disruption. Or they might be too late, and systemic quantum-enabled attacks start before they are ready. There's no free lunch: every unit of crypto-procrastination translates either into a unit of catastrophic risk or a unit of rushed migration risk.

Another risk is already becoming a reality: "harvest now, decrypt later" attacks. Although a cryptographically relevant quantum computer does not yet exist, malicious actors are collecting encrypted data with the intent to decrypt it once quantum computers become powerful enough to do so. If organizations fail to implement quantum-safe cryptographic strategies proactively, sensitive communications, financial transactions, and classified data may be at immediate risk.

And then, as regulators, partners, and other stakeholders push for quantum-readiness, there is compliance risk and the risk of simply not keeping up with the needs of your key stakeholders.

What are the main challenges in scaling and commercializing quantum-safe solutions?

Michele Mosca: Interestingly, the technical challenges while tough, are manageable. The harder part is getting timelines aligned across the ecosystem. Everyone from vendors to customers must commit to securing their systems by a certain date.

But some are still lagging, and we can't cater to the lowest common denominator anymore. It's time to separate the wheat from the chaff and improve our vendor ecosystem quality.

Another key issue is the lack of a clear mandate. If regulators and customers demanded resilience and set clear expectations, it would accelerate adoption. But too many are still debating when "Q-Day" will be, rather than acknowledging the urgency. That question was valid 10 years ago, but now it's outdated. Today, we need to focus on getting this done. The threat is already too close for comfort.

How do you create a sense of urgency around this threat?

Michele Mosca: Organizations need to understand that the quantum threat isn't far off in the future. It's already affecting them today, as in the "harvest now, decrypt later" threat. They must also consider the time required for a proper migration to quantum-safe technology.

This will quickly pivot from "doesn't matter" to "you better have it done." Adequate preparation will be a real business differentiator. One investor told me, "It's a dollar to get ready before left of boom, and hundreds of millions right of boom." That captures the stakes.

One of the major obstacles is self-imposed. A lot of this is driven by cool technological tactics that are unconnected with business objectives. The real goals are business continuity, resilience, trust, and risk reduction.

Why is the industry's focus on crypto inventory slowing progress, and what is the correct approach?

Michele Mosca: People are embarking on the gargantuan task of inventorying their cryptography but can't remember why they are doing it. They must use it to understand and mitigate business risk. Some even say, "I can't do my risk assessment yet because I haven't done my inventory." That's missing the point.

I'll give an example. Someone from Ericsson showed one slide in Toronto recently, it explained how 5G works and said: "The biggest threat is firmware updates." Boom. In 30 seconds, there's your biggest quantum risk. They didn't spend years scanning software just to produce massive data tables.

When cleaning your house, you don't need to dust every chandelier before you deal with the corpses in the dining room. Inventory is a part of mature crypto management, but don't let it stall your risk assessments. Act on the most obvious risks.

Have you heard of any post-migration concerns around latency, performance, or compatibility with legacy systems?

Michele Mosca: Around 80% of the time, you'll be fine. Even on a phone. But what if you're in an internet of things (IoT) scenario or other constrained environments? Then, it becomes a problem. And you better find out in advance. If you need lightweight PQC and it doesn't exist, then what?

Some experienced applied cryptographers are realizing that, most of the time, PQC is the answer. Just upgrade your PKI [public key infrastructure] to post-quantum PKI and you're good. But, in a few cases, we're seeing situations where PKI might be overkill. Here, we should revisit assumptions.

There are use cases where we did PKI because that's what we knew. But, in controlled, exclusive systems, it's worth asking why we're still using PKI. It's slow, consumes energy, and is vulnerable to cryptanalysis. In these cases, maybe it's time to leverage symmetric key solutions, which are faster and more secure in the long term.

Michele Mosca
CEO, evolutionQ

"Every unit of crypto-procrastination translates either into a unit of catastrophic risk or a unit of rushed migration risk"