NAAC GRADE A+ ACCREDITED UNIVERSITY

REVA RACE — REVA Academy for Corporate Excellence

REVA UNIVERSITY
Bengaluru, India

RACE WEEKLY INTELLIGENCE BRIEF

RETiNA

AI · CYBERSECURITY · CLOUD · LEADERSHIP

THIS WEEK'S COVER:

SOMEONE IS ALREADY STEALING YOUR 2035 SECRETS

A quantum computer that can break today's encryption doesn't exist yet. It doesn't have to. Adversaries are copying your encrypted data now — KYC files, contracts, health records, IP — to decrypt the day it does. The theft is silent, undetectable, and already underway. The fix, migrating to new cryptography, is a multi-year programme with deadlines that land this quarter. Q-Day isn't a research story any more. It's a procurement problem.

ALSO INSIDE

The World in 5 · Signal · Hyperfocal · Three Forces · Perspectives · The Quantum-Readiness Playbook · Metric of the Week · Fun Fact · CANDID · Book Shelf · Research Radar · RACE Pulse

ISSUE #18 · WEEK OF 31 AUGUST–6 SEPTEMBER 2026

Visit our website
race.reva.edu.in

RETiNA
AI · CYBERSECURITY · CLOUD · LEADERSHIP

NAAC GRADE A+ ACCREDITED UNIVERSITY
REVA RACE REVA Academy for Corporate Excellence

REVA UNIVERSITY
Bengaluru, India

- **From the Editor's Desk**
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

FROM THE EDITOR'S DESK

Most security deadlines move away from you as you work. This one moves toward you, and part of the damage is already done.

Here is the uncomfortable mechanic at the centre of this issue. Nearly all the encryption protecting data in motion today- the RSA and elliptic-curve cryptography behind your HTTPS, your VPNs, your payment rails, your digital signatures- rests on a maths problem a large enough quantum computer can solve. That computer does not exist yet; credible estimates put a cryptographically relevant machine somewhere in the 2030–2035 window. At Davos in January, IonQ's CEO warned Q-Day could arrive within three years; Google likened quantum today to where AI sat five years ago, just before it accelerated. Bain found roughly 70% of executives expect quantum-enabled attacks within five years.

The trap is called Harvest Now, Decrypt Later. An adversary does not need the quantum computer today to hurt you today. They copy your encrypted traffic now passively, invisibly, at nation-state and increasingly at criminal scale and store it until the machine arrives. Any data that must stay secret past roughly 2030 is therefore already at risk, the moment it leaves your network. For a bank's KYC archive, a pharma company's trial data, or a contract with a ten-year life, the breach has, in effect, already happened. You just cannot see it yet.

The good news is that the defence is settled, not speculative. NIST finalised the replacement algorithms in 2024 (FIPS 203, 204, 205). The work now is migration and that is a multi-year engineering programme, not a patch. Which is why the deadlines matter: NIST retires the old FIPS 140-2 validation on 21 September 2026; the US CNSA 2.0 acquisition gate lands 1 January 2027; and India is not behind here, the National Quantum Mission's task force has published a quantum-safe roadmap, the RBI has stood up a Q-SAFE committee for the financial system, and a national PQC testing-and-certification programme is targeted for December 2026, with a Cryptographic Bill of Materials mandatory from FY2027–28. This issue turns all of that into the five moves a leadership team can start this quarter, because the one thing you cannot buy later is the years the migration takes.

- From the Editor's Desk
- **The World in 5**
- Signal
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

🌍 THE WORLD IN 5

GLOBAL HEADLINES A CXO SHOULD BE ABLE TO REFERENCE

Five signals from the past fortnight, worth a note at your next leadership table.

The Threat: Harvesting is happening now, not in 2035

The quantum computer is years away; the attack is not. "Harvest Now, Decrypt Later" is a passive, undetectable collection of encrypted data today for decryption once a cryptographically relevant quantum computer exists. Regulators now treat it as present-tense: India's national task force says all transition planning should proceed under an "assume breach" principle. If your data must stay confidential past ~2030, its exposure window is already open.

2. The Intent-Action Gap is enormous

DigiCert's July 2026 readiness survey of 1,001 enterprises found 87% are now planning, testing or implementing post-quantum cryptography, but only 7% have even half their digital certificates on quantum-safe or hybrid algorithms, barely up from 5% a year earlier. Intent has scaled; deployment has not. Awareness is not a control.

3. The Deadlines converge this quarter

Advisory guidance is turning into procurement teeth. NIST retires FIPS 140-2 validation to "Historical" on 21 September 2026; the EU's national-strategy milestone lands 31 December 2026; the US NSA's CNSA 2.0 acquisition gate opens 1 January 2027, with full migration mandated by 2030. These dates affect contracts being signed today, not a distant roadmap.

4. India: a national roadmap, and a regulator moving

Under the National Quantum Mission, a DST task force published "Implementation of a Quantum Safe Ecosystem in India" (Feb 2026): pilots in banking and finance first, a National PQC Testing & Certification Program targeted for December 2026, and Cryptographic Bill of Materials submissions mandatory from FY2027–28. Separately, the RBI has constituted a Q-SAFE committee to examine quantum risk across the financial system. The direction of travel is set.

5. What Survives, And What Doesn't

Not all cryptography breaks. Symmetric encryption such as AES-256 stays effectively safe, quantum only weakens it modestly. It is public-key cryptography (RSA, ECC, ECDH, ECDSA) that Shor's algorithm defeats: exactly what protects data in transit, key exchange and digital signatures. So the migration is targeted, not total, which is precisely why knowing where your public-key crypto lives is the whole game.

Source:

https://csrc.nist.gov/projects/post-quantum-cryptography

https://dst.gov.in/quantum-safe-ecosystem-in-india

https://www.digicert.com/news/quantum-security-deployment-remains-stuck

https://csrc.nist.gov/projects/cryptographic-module-validation-program

https://fintech.rbi.org.in/

https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/

https://m.economictimes.com/news/international/global-trends/q-day-may-arrive-within-3-years-warns-ionq-ceo-at-world-economic-forum-davos/amp_articleshow/127039283.cms

- From the Editor's Desk
- The World in 5
- **Signal**
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

SIGNAL

THE AUTHENTICITY COLLAPSE — BY THE NUMBERS

7%
of organisations have even half their digital certificates on quantum-safe crypto (DigiCert, Jul 2026)

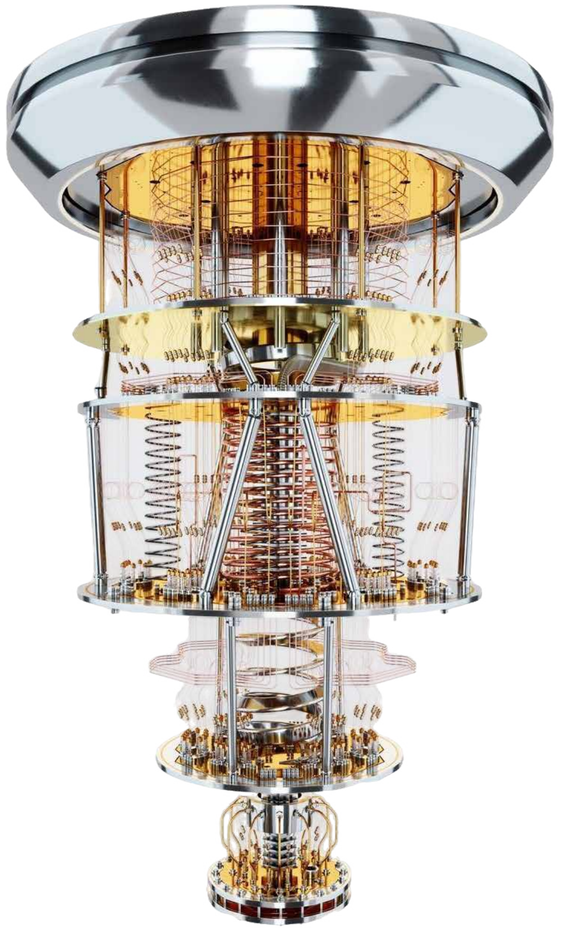
87%
say they are planning or testing PQC- the gap between those two numbers is the exposure

1994
the year Shor's algorithm was published, we have had 30+ years' warning that this was coming

~70%
of executives expect quantum-enabled cyberattacks within five years (Bain, Jan 2026)

2030
the migration deadline (US CNSA 2.0; India NQM high-priority) and it is a multi-year programme

Dec 2026
India's target for a National PQC Testing & Certification Program; CBOM mandatory FY2027–28



Source:

https://www.digicert.com/news/quantum-security-deployment-remains-stuck
https://csrc.nist.gov/projects/post-quantum-cryptography
https://csrc.nist.gov/projects/fips-140-3-transition-effort
https://dst.gov.in/quantum-safe-ecosystem-in-india
https://fintech.rbi.org.in/

- From the Editor's Desk
- The World in 5
- Signal
- **Hyperfocal**
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

HYPERFOCAL

You Cannot Detect the Theft That Has Already Happened

Every breach playbook a CISO owns assumes you find out. An alert fires, a log shows an exfiltration, and the six-hour reporting clock starts. Harvest Now, Decrypt Later breaks that assumption at the root. Copying encrypted traffic as it crosses a network leaves no trace on your systems, triggers no alert, and needs no vulnerability; the attacker simply keeps a copy of what you already sent in the open. There is nothing to detect, because from your side nothing failed. The data was encrypted. That was supposed to be enough.

It stopped being enough the moment a credible timeline appeared for a machine that can undo the encryption retroactively. This is the mental shift leaders keep missing: the risk is not 'our data might be stolen when quantum arrives.' It is 'data we transmit today is being banked against a decryption date we do not control.' The deadline is therefore not in the future. For anything with a long confidentiality life, identity and KYC records, medical files, source code, M&A and legal documents, state secrets, the deadline was the day you first sent it under RSA or elliptic-curve encryption. RETINA has argued before that you cannot detect your way out of deepfakes; here the point is sharper. You cannot detect this at all.

Which leaves exactly one strategy: change the lock before the key exists, starting with the doors that matter most. The replacement locks are ready; NIST standardised them in 2024, but fitting them across an enterprise's certificates, VPNs, payment systems, embedded devices and third-party dependencies is slow, and most organisations cannot even list where their cryptography lives. That inventory gap, not the algorithms, is why the 7% figure is so low. The work is unglamorous and it is long, and the only version of it that fails is the one that starts on Q-Day instead of this quarter.

RETINA TAKE

The organisations that come through Q-Day intact will not be the ones that reacted fastest when a quantum computer was announced. They will be the ones that treated a threat with no alarm as real anyway — inventoried their cryptography, migrated their longest-lived secrets first, and made the swap routine — while it was still cheap, quiet, and years ahead of the headline.

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- **Panorama**
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

PANORAMA

THREE FORCES — AND THE MOVE EACH ONE DEMANDS

FORCE 1

The Maths Is Settled; Only the Timeline Is Open

This is not a research question waiting on a breakthrough. Shor's algorithm has been known since 1994; it is understood exactly how a large quantum computer breaks RSA and elliptic-curve cryptography. NIST has already published the replacements (FIPS 203/204/205), and symmetric encryption like AES-256 survives. The only genuine unknown is when a capable machine arrives, and Harvest Now, Decrypt Later means you must act well before it does. Waiting for certainty is choosing to migrate under fire.

The Move: Stop treating quantum as a horizon-scanning item and start treating it as a scheduled engineering programme. The technology risk is resolved; the execution risk is all that's left, and execution takes years.

FORCE 2

The Deadline Is Retroactive

Because harvesting happens today, the clock is set by your data's shelf-life, not by Q-Day. Data that must stay confidential for ten years and is transmitted now under classical crypto is already exposed to a machine that arrives in eight. A bank's KYC archive, a hospital's records, an insurer's actuarial models, an IP portfolio, all carry secrecy horizons that run straight through the danger zone. Averages are useless here; a single long-lived record sent in the clear is the whole liability.

The Move: Classify your data by how long it must stay secret, not by how sensitive it feels today. Anything whose confidentiality must outlast ~2030 goes to the front of the migration queue.

FORCE 3

You Can't Migrate What You Can't See

The reason only 7% of organisations are substantially migrated is not the algorithms; it is that almost no one has a map of where their cryptography actually lives. It is buried in certificates, libraries, hardware modules, embedded devices, and critically, in third-party and vendor products you don't control. India's roadmap makes this concrete by mandating a Cryptographic Bill of Materials; vendor readiness will gate how fast anyone can move. Crypto-agility — the ability to swap algorithms without re-architecting- becomes a first-class design requirement.

The Move: Commission a cryptographic inventory (a CBOM) now, and write PQC-readiness and a documented upgrade path into every vendor contract. You cannot outsource the deadline, only the parts you forgot you depended on.

Source: https://csrc.nist.gov/projects/post-quantum-cryptography
https://www.digicert.com/news/quantum-security-deployment-remains-stuck
https://dst.gov.in/quantum-safe-ecosystem-in-india
https://cloudsecurityalliance.org/artifacts/a-practitioners-guide-to-post-quantum-cryptography

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- **Perspectives**
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

PERSPECTIVES

DEEP TECH — ANALYSIS BY THE RACE TEAM

Quantum Computers Are Not Yet Available; India's Stack Is Already Sitting on the Target

Sridhar Govardhan
Group CISO, Angel One,
Mentor, RACE, REVA University

https://www.linkedin.com/in/sridhargovardhan/

Last year, Indian citizens lost ₹22,845 crore to cybercrime, a 206% increase in twelve months, according to the Ministry of Home Affairs in the Lok Sabha. Over 36 lakh financial fraud cases were reported, and only approximately 2.2% of the lost money was recovered. That is the cyber threat to which India is already losing, openly, in the daylight. Post-quantum cryptography is the one we are not yet losing to, but quietly, in the background, adversaries are already copying our encrypted traffic and waiting for the day a quantum computer can decrypt it. That day is sometimes called "Q-day." For the data harvested today, the countdown started the moment it left your server.

Here is what makes the wait strategy effective. Anything you encrypt today with RSA or elliptic-curve crypto can be copied, stored, and decrypted later once a cryptographically relevant quantum computer exists. This is called "harvest now, decrypt later," and the Indian data estate is uniquely exposed to it. The UIDAI has issued over 142 crore Aadhaar numbers of biometric identities tied to bank accounts, mobile SIMs, welfare benefits, and income tax filings. Aadhaar authentication currently runs on RSA-2048 encryption. UPI alone processed 21.6 billion transactions in December 2025 and 228 billion across the year, with a cumulative value crossing ₹300 lakh crore. Every single one of that transaction depends on a TLS handshake running classical public-key crypto. Add the GST Network, Income Tax e-filing, MCA21, DigiLocker, e-Sign, the National Smart Metering Programme (250 million meters planned), defence communications, and patient records under the Ayushman Bharat Digital Mission, and the shape of the problem becomes impossible to ignore. India's digital public infrastructure is one of the most ambitious projects built anywhere in the last decade. Almost all of it is held together by cryptography, which a quantum computer will eventually be able to break.

The math on "how worried should I be" is deceptively simple. Michele Mosca's theorem says: if X + Y > Z, you're already in trouble. X is the duration for which the data must remain confidential. Y is the duration of the migration to quantum-safe crypto. Z is the number of years until a quantum computer can break RSA-2048. For a 20-year-old land record, a 30-year mortgage, an Aadhaar number tied to a lifelong identity, or a 25-year patent filing, X is a minimum of 20. Conservative estimates for Y run for 7–10 years. The only way to stay safe is if Z is more than 30 years out, that is, a working quantum computer so far away that we can ignore it. Most expert estimates place Z

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- **Perspectives**
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

PERSPECTIVES

DEEP TECH — ANALYSIS BY THE RACE TEAM

between 10 and 20. Do the arithmetic for almost any long-lived Indian dataset: the answer is already "yes, you're in trouble." This one-line calculation is the single best argument for why preparedness cannot be a 2030 problem.

So, what does preparedness look like? Three concrete things.

First, build a cryptographic inventory of every RSA, ECDSA, and DH key in your stack, every cert, every handshake, and every HSM slot. The average large Indian enterprise has thousands of these, and most security teams cannot confidently name even a fifth of them.

Second, classify by data longevity and exposure: prioritize systems that handle long-lived secrets, customer PII, financial transactions, or code signing. A session cookie and a 30-year loan record are not the same problems.

Third, build crypto agility - structure your code so that swapping an algorithm is a configuration change, not a six-month engineering project. Regarding mitigation, you can start this week. Cloudflare, Google, and AWS all support hybrid post-quantum TLS today, combining a classical algorithm with ML-KEM to obtain quantum resistance without breaking compatibility. It is turned on for a non-critical service. The added latency is approximately 1–2 milliseconds, and the handshake grows from roughly 5 KB to approximately 17 KB. Watch your monitoring, see what breaks, and then expand. Talk to your HSM, PKI, and CDN vendors and ask for their PQC roadmap in writing. If they cannot produce one, that is your answer to the question. The National Quantum Mission, with its ₹6,003 crore budget, signals that the government has at least acknowledged the threat. The organizations, public or private, that use the next two to three years well will be the ones still doing business with global clients when PQC becomes a procurement requirement. Those who wait will be explaining to the RBI, the SEBI, or a European customer in 2034 why they are still using RSA-2048, while their Aadhaar, UPI, and tax data are decrypted, in bulk, by someone who started collecting it a decade earlier.

RETINA TAKE

Quantum risk is the purest test of whether an organisation can act on evidence rather than alarms. There will be no siren for Q-Day — only, one day, the news that the machine exists and that a decade of harvested data can now be read. The discipline that protects you is boring, it is slow, and the only wrong time to start it is the day you can finally point to the threat.

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- **The Quantum-Readiness Playbook**
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

THE QUANTUM-READINESS PLAYBOOK

MIGRATING BEFORE THE KEY EXISTS

Five moves, ordered from fastest to most strategic, that any leadership team can act on.

MOVE 1

BUILD A CRYPTOGRAPHIC INVENTORY (CBOM)

You cannot migrate what you cannot find. Commission a Cryptographic Bill of Materials for every place public-key cryptography is used across applications, certificates, VPNs, key stores, hardware modules, and embedded and third-party products. This is the single step that gates all the others, and the reason most organisations are stuck at single-digit readiness. India's roadmap makes the CBOM mandatory from FY2027–28; treat that as your starting gun, not your finish line.

The Move: Fund the inventory this quarter. 'We don't know where our crypto is' is the honest status of most enterprises, and it is a project, not an answer.

MOVE 2

TRIAGE BY DATA SHELF-LIFE, NOT SENSITIVITY

Because harvesting is already happening, prioritise by how long each dataset must stay secret. Map your longest-confidentiality assets, KYC and identity records, health data, IP, contracts, cryptographic keys themselves, and migrate those first, because they are the ones being banked today for later decryption.

The Move: Rank data by secrecy horizon. Anything that must stay private past ~2030 is already exposed and goes to the front of the queue.

MOVE 3

GO HYBRID, NOT BIG-BANG

You do not rip out classical cryptography overnight. The proven path is hybrid, running a NIST post-quantum algorithm (ML-KEM for key exchange) alongside the existing one, so a break in either still leaves you protected. Start with data in transit (TLS), where Harvest Now, Decrypt Later bites first, and where hybrid deployment is already field-tested.

The Move: Pilot hybrid PQC on your highest-value data-in-transit path now. It de-risks the migration and buys protection immediately, without betting everything on one switchover.

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- **The Quantum-Readiness Playbook**
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

THE QUANTUM-READINESS PLAYBOOK

MIGRATING BEFORE THE KEY EXISTS

MOVE 4

MAKE VENDOR PQC-READINESS A PROCUREMENT GATE

Most of your cryptographic exposure sits inside products you buy, not code you wrote. If a vendor cannot show a post-quantum roadmap and a documented upgrade path, they are selling you a liability with a delivery date. Bake PQC-readiness and CBOM disclosure into every relevant contract from now on; India's task force explicitly puts the burden on suppliers to lead.

The Move: Add a PQC-readiness clause to procurement today. 'When will your product be quantum-safe, and how will you prove it' belongs in every security review.

MOVE 5

Assign an owner and build crypto-agility

This is a multi-year, cross-functional programme, not a project a team does once. Give it a named owner, map it to the real deadlines (21 Sep 2026, CNSA 2.0 in 2027, 2030 migration, India's Dec-2026 certification milestone), and — most importantly — architect for crypto-agility so the next algorithm change is a configuration, not a rebuild. There will be a next one.

The Move: Name the owner and treat algorithm-swapping as a permanent capability, not a one-off. The goal is an organisation that can change its cryptography on demand, quietly, and on its own schedule.

Source:

https://csrc.nist.gov/projects/post-quantum-cryptography
https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved
https://cloudsecurityalliance.org/artifacts/a-practitioners-guide-to-post-quantum-cryptography
https://dst.gov.in/quantum-safe-ecosystem-in-india
https://csrc.nist.gov/projects/fips-140-3-transition-effort

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- **Metric Of The Week**
- **Fun Fact**
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

METRIC OF THE WEEK

ONE NUMBER, PROPERLY UNDERSTOOD

7% of organisations have even half their digital certificates on quantum-safe cryptography

What it is: DigiCert's July 2026 Quantum Readiness Outlook, surveying 1,001 enterprise IT and security leaders, found that while 87% are planning, testing or implementing post-quantum cryptography, only 7% have migrated even half their certificates to quantum-safe or hybrid algorithms, up barely two points from 5% a year earlier.

Why it matters now: The distance between 87% and 7% is the distance between intent and protection, and it is not closing. Awareness has saturated; deployment has stalled, because the hard part is not deciding to act but finding and replacing cryptography across a real enterprise. That gap is exactly what Harvest Now, Decrypt Later feeds on.

How leaders use it: Ask your security leader one question: what percentage of our certificates and key exchanges are quantum-safe today? If the answer is a number, you have a programme. If the answer is 'I'd have to find out,' you have just discovered Move 1.

Source:
https://www.digicert.com/news/quantum-security-deployment-remains-stuck

FUN FACT

SOMETHING TO REPEAT AT DINNER

The algorithm that will one day break most of the world's encryption was invented in 1994 — by mathematician Peter Shor, on a machine that still cannot run it at scale. We have had more than thirty years' notice of this specific attack: longer than the commercial internet has existed, longer than most of the data now being harvested has been alive. The quantum threat is often called sudden. It is the opposite. It may be the most thoroughly forewarned catastrophe in the history of computing — which makes being unprepared for it a choice, not a surprise.

Source: https://dblp.org/rec/conf/focs/Shor94 | https://csrc.nist.gov/projects/post-quantum-cryptography

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- **Candid**
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

CANDID

CXO VOICE — IN CONVERSATION THIS WEEK

Dr Soumyo Maity
Distinguished Product Security Leader,

https://www.linkedin.com/in/soumyam/

Q1. 'Harvest Now, Decrypt Later' means data leaving an organisation today could be read in a decade. How should a board weigh a threat that triggers no alarm and whose damage, if it comes, has already been done?
We're used to a security question: "Have we been breached?"
We say "Yes" once we detect it.

Harvest Now, Decrypt Later (HNDL) is a security question where the honest answer is "we will not find out for a decade, and by then the remedy will be irrelevant."

So, I've stopped asking when quantum computers will break RSA, because nobody knows. I ask the two questions instead that my team can answer,
1. How long must this data stay secret, and
2. How long will it take us to migrate to new cypher suites?

If those two added together exceed the time we've got to break RSA (That date in future is termed Q-Day), we are already late – better we race to migrate. This simple arithmetic usually works across boards. And here's the part boards find genuinely uncomfortable for our longest-lived data; the loss event may have already occurred. We just can't observe it. CISA, the NSA and NIST confirm that adversaries are already extensively harvesting now and they will decrypt later.

If someone really persuades on Q-day, some forecasts place cryptographically relevant quantum computers in the 2028–2031 window. The Global Risk Institute's Quantum Threat Timeline Report — the 2025 edition puts a cryptographically relevant quantum computer at 28–49% within ten years, up from 19–34% the year before, based on a survey of 26 leading researchers.

Q2. The replacement algorithms have existed since 2024, yet only a fraction of enterprises have migrated. Is the real bottleneck technical, or is it that firms simply don't know where their own cryptography lives?
NIST PQC Guidance says FIPS203, FIPS204 and FIPS205 should be put into use now, and announced RSA and elliptic curve to be tentatively deprecated after 2030, disallowed by 2035. So the standards are done and the clock is published.

The bottleneck is that most organisations cannot answer a very simple question: where is RSA running in our estate right now? Obtaining an AIBOM is difficult but the most pressing problems to be solved immediately.

Before my team is lost with fancy quantum jargons and fancier cipher names, I make it clear, "What we deliver is not Kyber or SPHICS+, the deliverable is the ability to change algorithm again in five years -- crypto agility."

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- **Candid**
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

CANDID

Cloudflare published that Client-side post-quantum traffic went from under 3% in early 2024 to over 60% by early 2026 — because browsers and TLS libraries switched it on by default and no human had to do anything.

But in Server-side, it is around 10%. That gap between 60% and 10% is the entire story of this migration. Where it was automatic, it happened. Where someone had to find the cryptography and own it, it stalled. The reason is that cryptography isn't in one place. It's in firmware, in boot chains, in HSMs, in PKI, in codesigning, in third-party binaries we don't have source for.

Q3. Most of an enterprise's cryptographic exposure sits inside vendor products it doesn't control. How should 'prove your product is quantum-safe' change the way organisations buy technology?
Most of the cryptographic risk sits inside products we didn't write, can't inspect and can't patch. Which means our migration timeline isn't really ours — it's the union of the vendors' timelines. That's an uncomfortable thing to say out loud, but it's true for almost every enterprises.

So 'quantum-safe' has to stop being an adjective on a datasheet and become an artefact we can test. Four things, concretely,

- A machine-readable cryptographic bill of materials generated by tooling, not a PDF questionnaire.
- Name the certified algorithm and parameter set
- Support hybrid mode, classical and post-quantum together.
- And prove you can disable every legacy algorithm — including in boot and firmware signing — and still function. This one is where most vendor claims quietly fall apart.

Q4. India has a National Quantum Mission roadmap, an RBI Q-SAFE committee, and a testing-lab target for December 2026. What has to happen for that national intent to translate into migrated systems rather than published plans?
India has gone considerably further than plans. The National Quantum Mission roadmap, from the DST task force carries hard dates. Critical infrastructure: cryptographic inventory and CBOM procurement clauses by December 2027, high-priority migration by December 2028, full adoption with post-quantum-only trust chains by December 2029, Enterprises by 2030. That is tighter than NIST's own 2035 endpoint. It's arguably the most aggressive published timetable outside the Western bloc.

So, India's enforcement challenge is not the deadlines but the metrics and testing capacity. RBI's Q-SAFE is still on track. And, I would say Indian digital policy is worth respecting; we delivered UPI, Aadhaar, GST.

Quantum-safe migration has the design document and now the mandate. What it doesn't yet have is the published metric. If nobody can say in 2028 what percentage of government-facing TLS is running hybrid ML-KEM, and just a self-attestation will carry this all the way to 2030, we'll arrive with excellent documentation and unchanged systems.

Note: CANDID features direct contributions from CXO leaders.
To contribute, contact: retina@reva.edu.in

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- **Book Shelf**
- Research Radar
- RACE Pulse
- RACE Programs

BOOK SHELF

RETINA'S READ OF THE WEEK

RETINA RECOMMENDS · THIS WEEK'S THEME

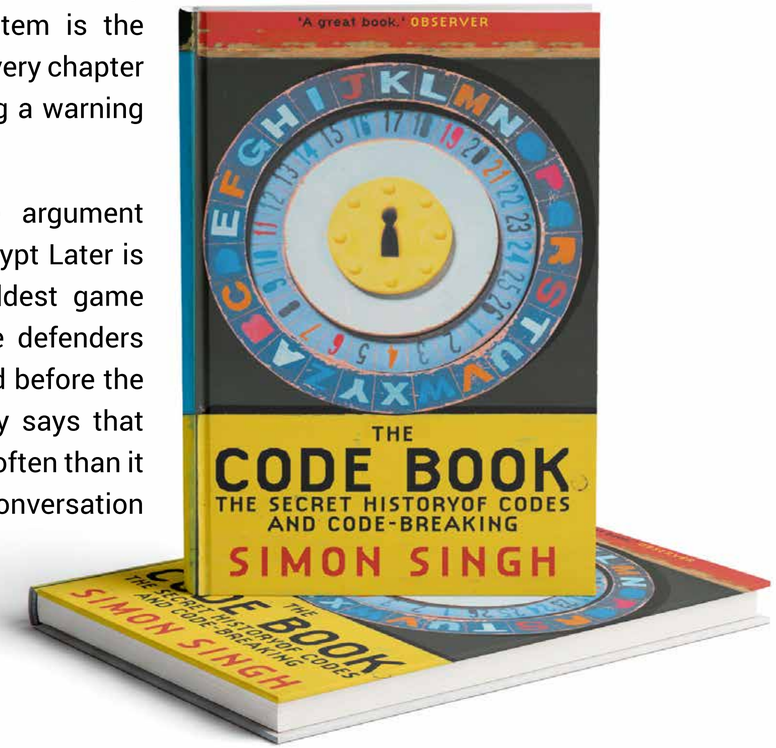
The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography

Simon Singh · Doubleday, 1999

Singh tells the whole history of secret-keeping as a single, unbroken arms race: every code ever considered unbreakable was eventually broken, and each break reshaped wars, monarchies and markets. Read a quarter-century after publication, its final chapters land differently than they did in 1999, what Singh presented as a distant frontier, quantum computing's threat to cryptography, is now the operational deadline on this week's cover. The book's oldest lesson is its most useful one for a board: 'unbreakable' is always temporary, and the only durable strategy is to be ready to change the lock.

It is not a technical manual, and that is the point. What it gives a leadership team is intuition, for why cryptography is infrastructure rather than a feature, why the people who won these contests were the ones who moved before they were forced to, and why complacency about a 'secure' system is the recurring villain of the entire story. Every chapter is, in effect, a case study in ignoring a warning until it was too late.

Pair it with this issue and the argument completes itself. Harvest Now, Decrypt Later is simply the newest move in the oldest game Singh describes, and, for once, the defenders have the replacement cipher in hand before the attackers have the weapon. History says that advantage is rare, and wasted more often than it is used. Read it before your next conversation about the migration budget.



- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- **Research Radar**
- RACE Pulse
- RACE Programs

RESEARCH RADAR

RACE PUBLICATIONS THIS WEEK

EDITOR'S NOTE

Two new IEEE publications from RACE, one hardening cloud-connected devices in real time, one forecasting revenue under real-world volatility. Standard format: a concise technology summary followed by clear enterprise relevance.

Automated IoT Security Configuration Audit Framework in AWS Cloud for Real-Time Threat Detection

Rahul Mohan; Nishanth Kumar Pathi; Rashmi Agarwal

Most IoT breaches start with a misconfiguration nobody caught in time. This framework closes that window by stitching AWS IoT Core, Device Defender, Lambda, Security Hub and SNS into one continuous audit-and-remediation loop — finding vulnerabilities and fixing critical ones automatically in minutes, not hours, with minimal human intervention. In testing it cut misconfiguration-identification time by 93% and held an average 3.5-second response on critical incidents while staying stable as device counts grew.

Enterprise Relevance: For any business running a fleet of connected devices, this is the shape of defence that keeps pace with machine-speed risk — continuous configuration audit, automated fix, and centralised compliance rather than periodic manual review. It's the same principle this issue's cover demands: when the attack surface moves faster than people, the control has to be autonomous by design.

2025 International Conference on Emerging Technologies in Computing and Communication (ETCC) · Bangalore · IEEE
https://ieeexplore.ieee.org/document/11108388

Data Science · Time-Series Forecasting · Agritech

Revenue Forecast for an Agritech Platform Using Time Series

Naveen Kumar S; J. B. Simha; Kiran Kumar K. V.

Agricultural revenue is hard to predict, seasonal, volatile, and poorly served by generic models. Structured with the CRISP-DM methodology, this work applies SARIMA to capture the seasonal swings and nonlinear behaviour specific to agri-markets, and reports upper and lower confidence intervals rather than a single fragile point estimate — reaching ~95% average accuracy with MAPE under 0.05.

Enterprise Relevance: For any seasonal, demand-volatile business, not only Agritech, the takeaway is method over magic: match the model to the data's actual structure and forecast in ranges, not false-precision single numbers. Confidence intervals turn a prediction into a planning tool a board can actually act on.

2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) · IEEE
https://ieeexplore.ieee.org/document/10914758

Enterprise Relevance: For any seasonal, demand-volatile business, not only Agritech, the takeaway is method over magic: match the model to the data's

Explore the full RACE research archive at https://raceresearch.reva.edu.in. For collaboration, licensing or research-partnership enquiries: race@reva.edu.in

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- **RACE Pulse**
- RACE Programs

RACE PULSE

EVENTS · COMMUNITY · WHAT'S COMING

RACEx360 SEASON 2

25 SEPTEMBER 2026 · TAJ WEST END, BENGALURU

RACEx360 Emerging Technology Conference 2026

One day, one stage, four frontiers.

REVA Academy's Emerging Technology Conference returns, in partnership with The Economic Times — 750+ builders, buyers and decision-makers across four tracks that matter: GenAI & Agentic AI · Cloud & Platform Engineering · Cybersecurity in the AI Era · Deep Tech & Sustainability.

Not a day of slides — a day of proof: an Innovation Experience Zone with live demos across AI, robotics, cybersecurity, cloud and quantum; live build sessions; an AI Hackathon and Cybersecurity Challenge; and keynotes that close with a 90-day action plan you can take back to your team.

The evening turns gold with the Top 10 Women Tech Leaders India Awards 2026, now in its 4th edition — India's only annual awards programme dedicated to women technology leaders.

Early Bird 4,000 + GST until 15 August · Standard 5,000 + GST. Passes cover all four tracks, the Expo Hall and the Experience Zone.

GET YOUR PASS:
https://race.reva.edu.in/racex360-season-2

BECOME A SPONSOR:
https://race.reva.edu.in/racex360-sponsorship

In partnership with ET The Economic Times

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- **RACE Pulse**
- RACE Programs

RACE PULSE

EVENTS · COMMUNITY · WHAT'S COMING

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- **RACE Pulse**
- RACE Programs

RACE PULSE

EVENTS · COMMUNITY · WHAT'S COMING

SEPTEMBER 2026 BATCH ·

APPLY BY 10 AUGUST 2026

Applications open for all six RACE Master's & PG Programmes — Business Analytics (#1 India), Artificial Intelligence (#3 India), Cybersecurity (#5 India), and Cloud Architecture & Security.

Weekend format. AICTE/UGC approved. Industry mentors from Amazon, Microsoft, AWS, EC-Council, Terralogic, IBM and more.

To know more, call:
+91 89040 58866

enquiry@race.reva.edu.in ·
Apply now: race.reva.edu.in

NEW BATCH

Certified Agentic AI Engineer

26 SEPTEMBER 2026

Practical expertise in LLMs, AI agents, multi-agent systems, agentic workflows, governance and capstone-based implementation. Real-world use cases, deployable solutions.

To know more, call:
+91 89040 58866

Apply now:
https://race.reva.edu.in/certified-agenticai-engineer

RACE SANDBOX

SATURDAY 12 SEPTEMBER 2026

Run your career simulation, live on campus. Sit in a live Master's class, walk the AI, Cybersecurity and Cloud labs, watch participants and alumni demonstrate real projects, and take a 1:1 on where your career goes next. Experience today, decide your tomorrow.

9:30 AM – 2:00 PM
RACE, REVA University, Bengaluru

Reserve your slot:
+91 89040 58866 ·

enquiry@race.reva.edu.in ·
https://race.reva.edu.in/

RETiNA
AI · CYBERSECURITY · CLOUD · LEADERSHIP

- From the Editor's Desk
- The World in 5
- Signal
- Hyperfocal
- Panorama
- Perspectives
- The Quantum-Readiness Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- **RACE Programs**

NAAC GRADE A+ ACCREDITED UNIVERSITY

REVA RACE REVA Academy for Corporate Excellence

REVA UNIVERSITY
Bengaluru, India

Master's & PG Programmes

New Batch: September 2026 · 12–24 months · Weekend · For Working Professionals

#1 IN INDIA · ANALYTICS INDIA MAGAZINE

ANALYTICS

PG Diploma / M.Sc. in
BUSINESS ANALYTICS
AWS Academy · Microsoft Azure

12–24 Months

#3 IN INDIA · TECHGIG

ARTIFICIAL INTELLIGENCE

M.Tech. in
ARTIFICIAL INTELLIGENCE
AWS Academy · Microsoft Azure

24 Months

#3 IN INDIA · TECHGIG

ARTIFICIAL INTELLIGENCE

PG Diploma / M.Sc. in
ARTIFICIAL INTELLIGENCE
AWS Academy · Microsoft Azure

12–24 Months

#5 IN INDIA · ANALYTICS INDIA MAGAZINE

CYBERSECURITY

M.Tech. in
CYBERSECURITY
EC-Council · Microsoft Azure · Terralogic

24 Months

#5 IN INDIA · ANALYTICS INDIA MAGAZINE

CYBERSECURITY

PG Diploma / M.Sc. in
CYBERSECURITY
EC-Council · Microsoft Azure · Terralogic.

12–24 Months

CLOUD

PG Diploma / M.Sc. in
CLOUD ARCHITECTURE & SECURITY
AWS Academy · Microsoft Azure

12–24 Months

Short-Term Certification Programmes

100 Hours · Project-Driven · Customisable for Organisations

AGENTIC AI | 4–6 weeks
AGENTIC AI SYSTEMS DESIGN
Multi-agent systems using LangChain, LangGraph, CrewAI. Capstone: deployed autonomous agent.

AI ENGINEER | 8–12 WEEKS
AI ENGINEERING CERTIFICATION
Data pipelines, model training, LLMs, deployment. Real production projects every batch.

CLOUD | 8–12 WEEKS
CLOUD ARCHITECTURE & DEVSECOPS
Multi-cloud, IaC, secure CI/CD on real AWS/Azure/GCP environments. Not demos.

CYBERSECURITY | 8–12 WEEKS
CYBERSECURITY & SOC OPERATIONS
Threat detection, incident response, SIEM/SOAR. Hands-on in RACE's live Security Operations Centre.

DATA & AI | 12 WEEKS
DATA SCIENCE & BUSINESS ANALYTICS
Statistics to ML to BI. Python, SQL, Power BI, Tableau on real business datasets.

LEADERSHIP | 8–12 WEEKS
TECHNO-FUNCTIONAL LEADERSHIP
Executive presence, decision-making, leading tech-driven teams. Built for mid-to-senior managers.

Enroll with us · race@reva.edu · race.reva.edu.in

NAAC GRADE A+ ACCREDITED UNIVERSITY

REVA RACE

REVA Academy for Corporate Excellence

RETiNA

AI · CYBERSECURITY · CLOUD · LEADERSHIP

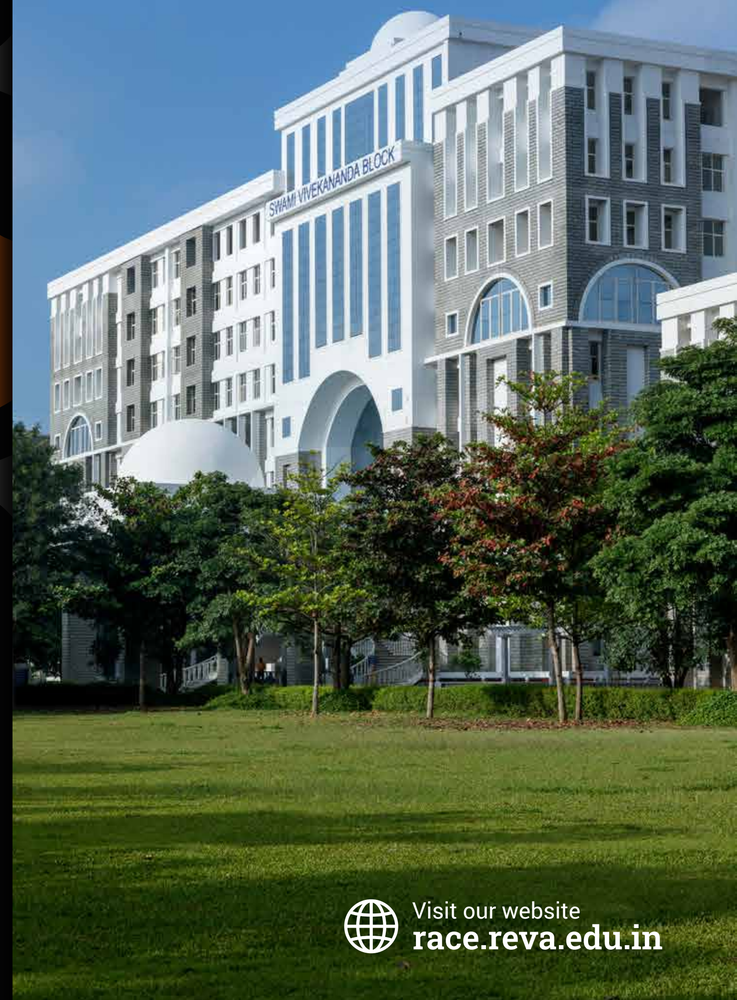
THIS WEEK, ASK YOUR LEADERSHIP TEAM

"What percentage of our data-in-transit and digital certificates are quantum-safe today and of the data we send in the clear right now, how much still has to stay secret past 2030?"

REVA Academy for Corporate Excellence,
REVA University
Rukmini Educational Charitable Trust
Kattigenahalli, Yelahanka, Bangalore, Karnataka, India, 560 064
Phone: +91 89040 58866

RETINA PUBLISHES EVERY SUNDAY · FORWARD TO A CXO YOU RESPECT

REVA UNIVERSITY
Bengaluru, India



Visit our website
race.reva.edu.in