ISSUE 10

THIS WEEK IN QUANTUM SECURITY

By
Joel Van Dyk
Quantum Security Advisor and Strategist

August 25, 2026

This week produced another broad mix of developments across quantum computing and quantum security, with hardware, cloud infrastructure, policy, cryptographic migration and quantum communications all moving at once.

IBM is tackling the physical engineering challenge of scaling quantum systems. Google Cloud has published a detailed post-quantum roadmap through 2029. Microsoft is pushing organisations to use threat modelling to understand cryptographic dependencies before migration. Oracle and Quantinuum are bringing quantum hardware into mainstream cloud infrastructure, while the United States is beginning to translate post-quantum policy into sector-specific programmes for critical infrastructure.

The useful thread through all of this is implementation. Quantum security is moving further into the systems, platforms and operational environments organisations already depend on. That continues to reinforce the importance of crypto-agility: not simply selecting the right algorithm today, but building environments that can change safely as the mathematics, standards and threat landscape evolve.

The Week's Key Developments

IBM tackles the physical problem of scaling quantum computers

One of the most interesting developments this week came from IBM, but it was not another qubit-count announcement.

IBM has been showing a new modular approach to the cryogenic infrastructure required to operate superconducting quantum processors. The problem is fairly straightforward to describe and much harder to solve. Quantum processors need to operate at temperatures very close to absolute zero, and as IBM tries to connect larger numbers of processors, the physical wiring between them becomes longer and increasingly susceptible to noise.

IBM's answer is a set of smaller cryogenic cabinets that can be connected through shielded cryogenic tunnels. The idea is to allow multiple processors to communicate while keeping the connections cold and reducing the noise introduced by long cable runs. IBM says the architecture could make it possible to scale beyond the limits of a single refrigeration system.

What I find useful about this story is that it reminds us how much of quantum computing is an infrastructure problem. Qubits and error correction understandably get most of the attention, but useful

systems will also depend on whether engineers can cool, connect, control and operate processors reliably at scale.

Read: The Register — IBM says super-chill boxes connected through cryogenic tunnels could help quantum computers scale

Google Cloud puts a 2029 date on post-quantum readiness

Google Cloud has published one of the more useful enterprise PQC roadmaps I have seen recently.

The company says it is targeting full post-quantum readiness across Google Cloud by 2029 and has broken that work into practical areas including protection against store-now-decrypt-later attacks, future signature forgery and the underlying cryptographic-agility capabilities required to keep changing algorithms over time.

Some of that migration is already visible. Google Cloud has been introducing hybrid post-quantum key exchange and support for NIST-standardised algorithms across parts of its infrastructure, while broader authentication, PKI, identity and hardware-backed changes are expected to continue through the remainder of the decade.

The practical point for enterprise teams is that migration is becoming a shared-responsibility problem. Google can make its infrastructure quantum-safe, but customers still have to understand their own applications, client software, keys and configurations. That is why vendor roadmaps need to be mapped against an organisation's own cryptographic inventory.

Read: Google Cloud — PQC in Plaintext: Google Cloud's post-quantum cryptography roadmap

Microsoft brings threat modelling into PQC migration

Microsoft's latest post-quantum guidance makes a related point from a different direction.

Its recent work focuses on threat modelling as part of the migration process. The recommendation is that organisations do more than identify which algorithms are in use. They should understand where vulnerable cryptography sits, which systems depend upon it, who owns those systems, what third parties are involved and what the operational consequences of changing it might be.

That is an important distinction. A cryptographic inventory may tell you that an application uses RSA. Threat modelling tells you what breaks when you replace it.

For anyone who has worked through a large enterprise migration, this will sound familiar. The difficult part is rarely finding a technically better component. It is understanding all of the relationships around the old one well enough to change it safely.

This also brings us back to crypto-agility. An organisation cannot be agile if it does not understand the dependencies around its cryptography.

Read: Microsoft — Post-Quantum Cryptography resources and threat-modelling guidance

Enterprise spending on quantum is becoming harder to dismiss

A useful piece of reporting from The Wall Street Journal this week looked at the amount of money large companies are now putting into quantum. According to Boston Consulting Group data cited by the Journal, enterprise spending on quantum technology reached approximately $300 million in 2025, with 62% of the 275 large companies surveyed investing at least $1 million annually. Companies including Allstate, HSBC

and EY are developing internal teams, use cases and infrastructure before the technology reaches full commercial maturity. (The Wall Street Journal)

Allstate's approach is particularly interesting. CEO Tom Wilson's argument is essentially that companies should not repeat what happened with generative AI, where many organisations waited until the technology had already moved into the mainstream before building the people and infrastructure needed to use it effectively. (The Wall Street Journal)

That does not mean every company needs a quantum computer. It does mean that organisations with complex optimisation, materials, financial modelling or cryptographic requirements should probably understand the technology before somebody like a regulator or the board asks them for a strategy.

For financial institutions, that work has two sides. There is the opportunity to use quantum computing, but there is also the responsibility to prepare the cryptographic infrastructure that may eventually be threatened by it.

Read: The Wall Street Journal — Businesses Are Spending Big on Quantum

The commercial quantum sector is beginning to show more differentiation

The latest earnings results have given us a much better picture of the sector than stock-price movements alone.

IonQ reported second-quarter revenue of $80.1 million, nearly four times the level of a year earlier, and raised its 2026 revenue guidance to $280 million to $290 million. The company has also completed the acquisition of SkyWater Technology, giving it semiconductor-manufacturing capability as part of a much broader strategy spanning computing, networking and sensing. (Barron's)

Rigetti reported $5.14 million in quarterly revenue, compared with $1.8 million a year earlier, with system sales contributing to the improvement. It continues to operate at a loss, but the fact that actual system orders are beginning to show up in revenue is a useful indicator of where the commercial market is going. (Barron's)

Quantinuum also reported its first quarterly results since becoming public, with second-quarter revenue of $8 million and $81 million in year-to-date bookings. Its new Oracle relationship adds another commercial route into enterprise computing. (Barron's)

Infleqtion reported revenue of $12.6 million, up 116% year over year, with much of that growth linked to government and NASA programmes. This is another reminder that the quantum market is not one market. Computing, sensors, clocks, networking and government research programmes are all developing on different commercial timelines. (Barron's)

I am still much more interested in repeat customers, bookings and deployments than in deciding which quantum stock will perform best. The useful question is whether customers are returning after the first experiment and paying for more.

That is where we will begin to see the difference between an interesting technology demonstration and a sustainable business.

Read: Barron's — Quantum computing earnings offered a reality check

The Quantum-GUARD Act puts the US electric grid directly into the migration conversation

US Senators Chris Coons and Mike Rounds have introduced the bipartisan Quantum Grid Utility Assurance and Resilient Defense Act of 2026, or Quantum-GUARD Act.

The bill would require the Federal Energy Regulatory Commission to consider quantum-related cybersecurity risks when reviewing electric-grid reliability standards. It would also direct the Department of Energy to establish a PQC sandbox where grid operators, technology vendors and government agencies could test post-quantum security technologies across both IT and operational-technology environments.

This is exactly the kind of sector-specific work I think we need.

Electric-grid infrastructure presents a very different migration challenge from a browser or a cloud application. Utilities operate devices with long lifecycles, strict availability requirements and complicated supply chains. Many systems cannot simply be taken offline for a software upgrade.

The sandbox element is therefore particularly useful. We need to know how PQC behaves inside the systems where it will actually be deployed, not simply whether the algorithm performs well in a laboratory.

Read: Senator Chris Coons — Quantum-GUARD Act announcement

Oracle and Quantinuum bring quantum hardware into the cloud

Oracle and Quantinuum announced a multi-year strategic partnership that will place Quantinuum's Helios quantum computer inside an Oracle Cloud Infrastructure AI data centre in the United States.

OCI customers are expected to be able to access Helios alongside Oracle's high-performance computing and GPU infrastructure, allowing developers to build hybrid quantum, classical and AI workflows without owning or operating the quantum hardware themselves.

The more interesting point for me is the deployment model. If quantum computing becomes useful to ordinary enterprises, this is probably how most of them will access it: through familiar cloud infrastructure alongside the classical systems they already operate.

It is also interesting that Oracle now appears on both sides of the transition. It is bringing quantum computing into OCI while also bringing post-quantum capabilities into long-term-support versions of Java.

Read: Oracle — Quantinuum and Oracle partner to accelerate hybrid quantum compute adoption on OCI

Read: Oracle — Post-Quantum Cryptography in Long-Term Support JDK Releases

Wireless quantum communication gets a new wavelength

Researchers led by the University of Oxford have demonstrated what they describe as the first wireless quantum key distribution system operating in the ultraviolet-C spectrum.

Most free-space QKD systems have used visible or infrared wavelengths, where sunlight creates background noise. UV-C is interesting because almost no natural sunlight at those wavelengths reaches the Earth's surface, potentially making it easier to isolate a quantum signal in outdoor environments.

This does not replace PQC, and I do not think it is useful to treat QKD and post-quantum cryptography as competing solutions. They address different use cases and have very different operational requirements.

What this work does show is that quantum communications continue to develop alongside post-quantum migration. For specialised environments, there may eventually be cases where the two are used together.

Read: Optica — Researchers harness UV-C wavelengths to advance wireless quantum communication

South Korea puts quantum into its national growth strategy

South Korea has included quantum computing in its new national "Seven Major SEED" technology initiative and set a target of developing a 100-qubit quantum processor by 2029.

The programme sits alongside strategic investments in areas including energy, space, biotechnology and advanced materials, making clear that the government sees quantum as part of its future economic and national-security infrastructure rather than as an isolated academic programme.

I would not read too much into a single qubit target because architecture and quality matter as much as raw numbers. The more important signal is the continuing number of governments treating quantum capability as national infrastructure.

Read: Reuters — South Korea unveils future-technology strategy including quantum processor target

Financial Security: Visa and BioCatch

Visa's $2.4 billion agreement to acquire BioCatch is worth including because it tells us something important about the wider security environment in which post-quantum migration is happening.

BioCatch uses behavioural and device intelligence to analyse thousands of signals, including typing behaviour, touch gestures, device handling and network activity, to identify scams, account takeover, money mules and application fraud. Visa says BioCatch serves more than 350 banks across 21 countries and protects hundreds of millions of users.

This is not a quantum acquisition, and I would not pretend that it is. It belongs in the briefing because financial security is becoming increasingly layered. Behavioural intelligence, AI-assisted fraud detection, identity, resilient cryptography and post-quantum infrastructure are all going to operate together.

For financial institutions, the future security architecture will not be defined by one new technology. It will be defined by how well those technologies work together.

Read: Visa — Visa to Acquire BioCatch

Global Signals

North America

Next week is particularly important for the research community because QCrypt 2026 runs in Ottawa from 24–28 August and includes work on QKD, security proofs, quantum cryptography beyond QKD and quantum-secure communications.

Read: QCrypt 2026

Europe

Europe's late-August calendar is extremely active.

The International Conference for Young Quantum Information Scientists takes place in Vienna from 24–28 August, while Superconducting Qubits and Algorithms 2026 runs in Gothenburg from 25–28 August.

The Gothenburg meeting is particularly worth watching because improvements in superconducting hardware, control and error mitigation influence the timelines security teams use when thinking about cryptographically relevant quantum computing.

Conference calendar: Quantum Technology — 2026 Conferences

Asia

Asia will host one of next week's most significant quantum meetings. AQIS 2026 runs from 24–28 August at KAIST in Daejeon, South Korea, covering quantum information processing, communication and cryptography.

South Korea's new national quantum strategy gives the meeting additional relevance this year. Elsewhere in the region, China, Japan and Singapore continue to pursue their own combinations of fundamental research, commercialisation and national capability building.

Read: AQIS 2026

Australia

Australia and Japan have strengthened their quantum partnership through a new collaboration involving Fujitsu, Monash University and CSIRO. Australian researchers and students will gain access to Fujitsu quantum systems and simulators in Japan, while the organisations are also exploring a shared quantum research and education facility at Monash.

The collaboration focuses on practical applications, workforce development and research infrastructure and identifies areas including optimisation, machine learning and cybersecurity.

This is the kind of ecosystem development that matters over the long term. Quantum capability depends not only on hardware but on whether countries have enough researchers, engineers and organisations able to use it.

Read: CSIRO — Fujitsu, Monash and CSIRO strengthen Australia-Japan quantum partnership

Africa

Africa remains less visible in the commercial quantum headlines, but that should not be confused with a lack of activity.

The more important issue remains capability building: research programmes, access to quantum tools, training, cybersecurity preparedness and participation in the standards and policy conversations that will determine how migration occurs globally.

This matters because post-quantum migration cannot become something designed entirely by North American and European organisations and then handed to the rest of the world. Financial systems, communications infrastructure and digital services operate internationally, which means interoperability and skills need to develop internationally as well.

The ITU Global Quantum Drill in Dubai next month will include regional participation from Africa and the Arab states, giving national incident-response and cybersecurity teams an opportunity to test quantum-readiness scenarios together.

Middle East

The ITU Global Quantum Drill takes place in Dubai on 17–18 September and remains one of the events I think security leaders should watch closely.

The value of the exercise is that it is not simply another awareness conference. It is designed around practical coordination between governments, CERTs, technical teams and standards organisations when faced with simulated quantum-related cybersecurity scenarios.

We need more of that. Migration plans are useful, but eventually organisations need to test whether those plans actually work.

Read: ITU — Global Quantum Drill 2026

Latin America

Brazil continues to develop its quantum research and training ecosystem through university and ICTP-SAIFR programmes covering quantum computing, error correction and cryptography.

Latin America receives considerably less commercial attention than North America or Europe, but the academic infrastructure matters. The long-term global quantum market will depend on where expertise is being developed, not simply where current investment is concentrated.

Read: ICTP-SAIFR Quantum Computing School

Collected Research Worth Reading

IBM — Modular cryogenic architecture for scaling quantum systems. The most interesting aspect is the engineering problem being addressed: connecting multiple processors while reducing the long, noisy connections that limit current architectures.

Read The Register

Google Cloud — PQC in Plaintext. Google's 2029 roadmap is particularly useful for organisations trying to understand how a major cloud provider is prioritising migration and how vendor roadmaps should feed into enterprise planning.

Read Google Cloud

Microsoft — Threat Modeling and Post Quantum Cryptography. This is practical guidance for moving beyond cryptographic inventory and understanding dependencies, ownership and migration constraints.

Read Microsoft

Optica — UV-C wireless quantum key distribution. This is an interesting communications development because it explores a wavelength where natural solar background is minimal, potentially improving outdoor free-space QKD.

Read Optica

FS-ISAC — Building Cryptographic Agility in the Financial Sector. I keep returning to this because the core lesson becomes more relevant with every new algorithm, standard and implementation change. Crypto-agility is not an optional feature of migration. It is what allows the organisation to keep migrating when the next change arrives.

Read FS-ISAC

Upcoming Conferences and Meetings

The week of 24 August is unusually busy across the global quantum calendar.

QCrypt 2026 — Ottawa, Canada — 24–28 August

This is probably the most directly relevant meeting for anyone working in quantum security. The programme covers QKD, security proofs, continuous-variable QKD, quantum cryptography beyond QKD, quantum communications and broader quantum-secure protocols.

QCrypt 2026

QCrypt programme

AQIS 2026 — KAIST, Daejeon, South Korea — 24–28 August

The Asian Quantum Information Science Conference covers quantum information processing, quantum computation, communication and cryptography. The venue is the KAIST Auditorium in Daejeon.

AQIS 2026

Young Quantum Information Scientists Conference — Vienna, Austria — 24–28 August

YQIS brings together early-career researchers working across quantum information science. These meetings are useful for seeing emerging research themes before they move into larger commercial or policy discussions.

Quantum Technology conference calendar

Superconducting Qubits and Algorithms — Gothenburg, Sweden — 25–28 August

This meeting focuses on superconducting hardware, control, algorithms and related work. It is worth monitoring because progress in hardware quality, control and error mitigation continues to affect estimates of the timeline towards useful and eventually cryptographically relevant quantum computing.

Quantum Technology conference calendar

International Conference on Quantum Enhanced AI and Secure Computing — Chicago — 28–30 August

The AI/quantum/security intersection is becoming much more interesting following recent work in AI-assisted cryptanalysis. This meeting is worth watching for research that crosses those boundaries.

Quantum Engineering conference calendar

Theory of Quantum Computation, Communication and Cryptography — Sherbrooke, Canada — 31 August–4 September

TQC remains one of the serious theory meetings covering quantum computation, communication and cryptography. For security teams, it is useful because this is where developments in the underlying theory that may eventually affect cryptographic assumptions are discussed.

Quantum Technology conference calendar

Silicon Quantum Electronics Workshop — Incheon, South Korea — 31 August–3 September

This meeting is worth following on the hardware side, particularly for developments in silicon-based approaches to quantum computing.

Quantum Technology conference calendar

European Summer School on Quantum AI — Italy — 31 August–5 September

The growing overlap between quantum computing and artificial intelligence makes this increasingly relevant, especially as AI starts to play a larger role in quantum research, control and cryptanalysis.

Quantum Technology conference calendar

ITU Global Quantum Drill — Dubai, UAE — 17–18 September

This remains one of the most practically relevant events on the calendar for security leaders. Rather than focusing solely on presentations, it uses simulated quantum-related cybersecurity scenarios to exercise coordination between governments, national CERTs, technical teams and standards organisations.

ITU Global Quantum Drill

— Joel Van Dyk