Episode 103

The Clock Is Ticking: Navigating Quantum Risk and the Path to Crypto Agility

Host	Dr. Dave Chatterjee, Duke University
Guest	Peterson Gutierrez, Vice President of Information Security, Barracuda Networks
Podcast Portal	https://www.cybersecurityreadinesspodcast.com/

Summary

In Episode 103 of the Cybersecurity Readiness Podcast Series, Dr. Dave Chatterjee is joined by Peterson Gutierrez—Vice President of Information Security at Barracuda Networks and a 28-year cybersecurity veteran with experience spanning private industry, the Big Four, and New York City Cyber Command—to examine one of the most consequential and underestimated challenges facing security leaders today: the quantum computing threat and what it truly means to become cryptographically agile.

Opening with a vivid scenario—a healthcare organization whose encrypted data is exfiltrated today and decrypted after a quantum breakthrough years from now—Dr. Chatterjee introduces the concept of Q Day risk: the danger is not a dramatic breach tomorrow, but decisions made today that leave organizations exposed later. The episode moves beyond the industry's fixation on which post-quantum algorithm to adopt, making the case that algorithm selection is the wrong problem to solve. The right goal is crypto agility: the organizational discipline to abstract encryption from code and adapt continuously as the cryptographic landscape evolves.

Framed through Dr. Chatterjee's Commitment–Preparedness–Discipline (CPD) lens, the conversation delivers a clear and actionable message: crypto agility is not a technical upgrade—it is a leadership, architecture, and governance challenge that requires executive ownership, modular system design, proactive vendor engagement, and continuous organizational discipline before Q Day makes inaction catastrophic.

Discussion Highlights

The Industry Is Asking the Wrong Question

The dominant industry conversation around post-quantum cryptography (PQC) centers on algorithm selection—which NIST-approved standard to adopt. Gutierrez argues this is a misallocation of energy: the majority of organizations will converge on the same published standards anyway. The more important challenge is becoming crypto agile—building the organizational capacity to abstract encryption from underlying code and replace algorithms rapidly as threats evolve. While Q Day is real and approaching, the long-term objective must be a continuously adaptive cryptographic posture, not a one-time migration.

What Cryptographic Fragility Looks Like in Practice

Dr. Chatterjee draws on his RSA Conference experience to illustrate the real-world symptoms of cryptographic fragility: expired certificates that bring down services, library patching that breaks dependent systems, multi-year algorithm replacement timelines, crypto-inflexible vendor architectures, the absence of centralized cryptographic asset inventory, and the harvest now, decrypt later (HNDL) exposure. Gutierrez reinforces this with the expired certificate analogy: organizations that have lived through the pain once and built a playbook recover quickly; those that have not are left scrambling. These accumulated lessons are precisely the muscle that must now be applied at quantum scale.

A Six-Step Framework for Managing the PQC Transition

Dr. Chatterjee proposes a structured six-step approach to the transition, which Gutierrez endorses and enriches:

- Step 1 — Cryptographic Discovery and Inventory: Map every certificate, key, and algorithm across on-premises, cloud, and third-party systems using automated scanning tools. Shadow IT is a critical blind spot; administrative controls must enforce accountability for unapproved cryptographic assets.
- Step 2 — Prioritization: Focus remediation where a breach would hurt most—long-lived sensitive data, Internet-facing APIs, critical infrastructure, and key exchange mechanisms where PKI is in use.
- Step 3 — Build Crypto Abstraction Into New Systems: Design agility in from the start rather than retrofitting legacy systems. New services should require a crypto abstraction layer; legacy systems are addressed on a risk-prioritized schedule.
- Step 4 — Establish Crypto Governance: Assign clear ownership per business domain with accountability to a central crypto governance council. Fragmented ownership is explicitly identified as a root cause of fragility.
- Step 5 — Conduct Crypto Agility Drills: Regular, real-time exercises that measure and improve response readiness—particularly critical given that HNDL threats leave no detection signal in the moment.
- Step 6 — Engage Vendors Early: Ensure supply chain partners share the same cryptographic posture. Given the acceleration of supply chain attacks, a vendor's fragility is an organization's risk.

Crypto Agility Is a Leadership Challenge, Not a Technical One

Dr. Chatterjee applies the CPD framework to crypto agility, emphasizing that the challenge transcends technical execution:

- **Commitment:** Executive ownership of crypto risk cannot be delegated to IT or security. The C-suite must sponsor dedicated funding and mandate for crypto agility initiatives. Board-level visibility into quantum and AI-driven threat exposure is essential—and must be communicated in business risk terms, not technical jargon.
- **Preparedness:** Organizations must build modular architectures that enable plug-and-play algorithm replacement, deploy automation to update cryptography at enterprise scale (with deliberate human oversight), and extend vendor and supply chain alignment to crypto agility standards.
- **Discipline:** Crypto agility is a continuous program, not a project. This requires lifecycle management of keys, certificates, and algorithms; automated rotation mechanisms; enterprise-wide policy enforcement with no exceptions for legacy systems; and regular drills with updated, rehearsed playbooks.

Speaking to the Board: Business Risk, Not Technical Complexity

Both speakers emphasize that Q Day must be communicated to leadership in business terms. Gutierrez warns that cryptography conversations can quickly slide into technical jargon that loses board members. The right framing connects quantum risk to business exposure: loss of customer trust, loss of contracts, reputational damage, and regulatory consequences. Organizations that cannot articulate their PQC posture will face scrutiny from partners and customers first—before any technical incident ever occurs.

Crypto Agility as a Program, Not a Project

Gutierrez draws a sharp distinction that anchors the closing discussion: organizations that treat PQC as a project with a defined endpoint are fundamentally misunderstanding the challenge. Crypto agility requires standing up a program—one with active governance, continuous participation, evolving playbooks, and the organizational muscle memory to respond as the threat landscape changes. The quantum computing environment is evolving now; organizations must evolve with it.

What Winners Will Look Like in Five Years

Drawing on the RSA Conference panel discussion, Dr. Chatterjee identifies three characteristics of organizations that will be ahead in five years:

- They treat cryptography as a dynamically managed capability—not a configuration set at deployment and left unchanged.
- They maintain real-time crypto visibility—knowing at any point what algorithms are running, where, and when certificates expire.
- They have embedded crypto agility as a design principle in enterprise architecture—not bolted on as a security add-on after the fact.

Actionable Recommendations

- Reframe PQC as Crypto Agility. Shift organizational focus from selecting the right algorithm to building the sustained capability to adopt any algorithm quickly. The long-term competitive advantage is adaptability, not compliance with today's standard.
- Build a Cryptographic Asset Inventory Now. Identify every certificate, key, and algorithm in use across all environments—including shadow IT and third-party systems. You cannot manage what you cannot see.
- Establish a Crypto Governance Council. Assign ownership and accountability by business domain, reporting to a central council. Fragmented ownership is the root cause of cryptographic fragility.
- Design Crypto Abstraction Into New Systems From Day One. Require all new services to use a crypto abstraction layer that enables algorithm replacement without re-engineering. Do not retrofit—build agility forward.
- Conduct Regular Crypto Agility Drills. Test organizational response readiness under realistic conditions, particularly for harvest now, decrypt later scenarios that leave no real-time detection signal.
- Engage Vendors and Supply Chain Partners on Cryptographic Posture. Your partners' fragility is your risk. Incorporate PQC alignment into vendor onboarding and ongoing relationship management.

- Communicate Quantum Risk in Business Terms to Leadership and the Board. Translate technical exposure into strategic business risk—revenue, trust, partnerships, and regulatory standing. Executive sponsorship requires executive comprehension.
- Execute a 30–60–90 Day Action Plan. In the first 30 days, implement governance and stop the bleeding by enforcing administrative controls on all new cryptographic assets. In 60 days, complete discovery and build the cryptographic bill of materials. In 90 days, engage engineering teams on migration planning and integrate PQC into incident response and business continuity frameworks.
- Apply the CPD Framework to Crypto Governance. Use Commitment, Preparedness, and Discipline as the organizing structure to build a crypto agility program that sustains itself as quantum capabilities evolve.

Time Stamps

00:00	Opening and strategic framing — the Q Day scenario
03:51	Peterson Gutierrez introduction and welcome
04:06	Guest professional highlights and career journey
07:03	Industry framing: algorithm selection vs. crypto agility
08:39	Why crypto agility — not algorithm selection — is the right goal
10:23	Cryptographic fragility in real enterprises: RSA conference insights
12:26	Paradigm shift: governance, ownership, and crypto bill of materials
14:07	Six-step framework for managing the PQC transition
17:39	Guest response: discovery, shadow IT, prioritization, and maturity
20:46	CPD framework applied: crypto agility as a leadership challenge
23:30	Commitment pillar: executive sponsorship and board engagement
25:19	Speaking the language of business risk to leadership
27:00	Preparedness pillar: modular architecture, automation, and vendor alignment
28:23	Guest perspective on preparedness and harvest now, decrypt later
29:40	Discipline pillar: lifecycle management, drills, and playbooks
33:30	Guest on discipline: program vs. project mindset and muscle memory
34:45	Characteristics of winners five years from now
37:16	Guest closing advice: 30–60–90 day action plan for CISOs
39:31	Closing remarks and final thanks

Memorable Quotes

“It’s not about a dramatic breach tomorrow. It’s about decisions today that determine whether your organization becomes exposed later.” **— Dr. Dave Chatterjee**

“Q Day is on the horizon, and the long-term goal should be crypto agility—abstracting encryption from code and being able to quickly adapt to the changing environment within cryptography.” **— Peterson Gutierrez**

“You can’t protect what you cannot see.” **— Peterson Gutierrez**

“Crypto agility is not merely a technical upgrade—it is a leadership, architecture, and operational discipline challenge.” **— Dr. Dave Chatterjee**

“You shouldn’t be standing up a project. You should be standing up a program for crypto agility—because it is continuous.” **— Peterson Gutierrez**

“Your partner’s fragility becomes your risk.” **— Dr. Dave Chatterjee**