

POST-QUANTUM SECURITY LEADERSHIP BRIEF

Preparing your organisation for post-quantum security (2026–2030)

Post-Quantum Security Leadership Brief

Table of Contents

Introduction 1

What Is Changing (And Why It Matters) 2

Where Organisations Are Exposed 3

A Practical Framework For Action 4

What This Means For WordPress-Based Systems 5

Leadership Questions To Ask Now 6

Your Ready-to-Use Worksheets 7

System Visibility Snapshot 8

Data Risk Snapshot 9

Vendor Readiness Tracker 10

About the Author 11

Introduction

Most organisations don't think about encryption until something breaks.

But the systems that protect your data today are already on a known timeline.

A new generation of quantum computers is expected to break many of the encryption methods used across the internet. This includes the systems that protect sensitive data and verify identity.

Government agencies such as the Australian Signals Directorate and major technology companies like Google have already set timelines for transitioning to post-quantum cryptography (PQC).

This resource is designed to give you a clear, practical understanding of:

- What is changing
- Where your organisation may be exposed
- What you should be doing now

The goal is not to turn you into a security expert.

It's to help you ask the right questions and make better decisions.

This is not something you need to solve today. But it is something you should start understanding now.

— Wil Brown

Zero Point Development

Disclaimer: WordPress® is a trademark of the WordPress Foundation. This resource is not affiliated with or endorsed by the WordPress Foundation or Automattic.

What Is Changing (And Why It Matters)

Today's internet relies on encryption to:

- Protect data in transit (websites, APIs)
- Verify identity (logins, digital signatures)

Quantum computing introduces a new risk.

It will be able to break many of these systems.

Why This Matters Now

This is not just a future problem.

Sensitive data can already be:

- Captured today
- Stored by attackers
- Decrypted later

This is known as "store now, decrypt later".

For organisations managing long-term data, this creates real exposure.

The Post-Quantum Timeline

The Australian Signals Directorate (ASD) outlines a clear transition window[1]:

- By 2026 → Have a transition plan
- By 2028 → Begin migration
- By 2030 → Complete transition

Large technology providers are already moving.

This means organisations will need to adapt as platforms evolve, not the other way around.

[1] https://www.cyber.gov.au/business-government/secure-design/quantum/planning-for-post-quantum-cryptography

Where Organisations Are Exposed

Most risk sits below the surface.

Common exposure points include:

- Websites and web applications
- Authentication systems (logins, SSO, APIs)
- Cloud platforms and SaaS tools
- Data storage and backups
- Third-party integrations

These systems often rely on cryptography that will need to change.

A Practical Framework For Action

The ASD recommends a structured approach using the LATICE model.

1. Locate

Identify where cryptography is used across your systems.

Start with:

- Websites and applications
- Cloud services
- Vendor platforms

2. Assess

Understand:

- What data you hold
- How sensitive it is
- What happens if it's exposed

3. Triage

Prioritise:

- Identity systems
- High-value data
- Public-facing platforms

4. Implement

Work with:

- Trusted vendors
- Standardised solutions

Avoid building your own cryptographic systems.

5. Communicate and Educate

Make sure:

- Someone owns this internally
- It's part of your risk planning
- Teams understand what's changing

What This Means For WordPress-Based Systems

Many organisations rely on WordPress as part of their digital infrastructure.

WordPress doesn't handle encryption directly.

It depends on:

- Hosting providers
- Cloud platforms
- Browsers
- Third-party integrations

Where To Pay Attention

Authentication

- Logins
- LMS platforms
- Membership systems

Data

- User records
- Certifications
- Form submissions

Vendors

- Hosting providers
- CDN and security layers
- SaaS integrations

Key point

WordPress is not the risk.

Lack of visibility into how it's supported and secured is.

Leadership Questions To Ask Now

Use these questions to guide internal discussions.

Systems

- Do we know where cryptography is used?
- Which vendors handle our security?

Data

- What sensitive data do we store long-term?
- What would happen if it were exposed in 5–10 years?

Vendors

- Have we asked about their PQC roadmap?
- Are we dependent on legacy systems?

Governance

- Who owns this internally?
- Is it part of our risk planning?

Your Ready-to-Use Worksheets

These worksheets are designed to make it easier for organisations to put these ideas into action.

Printable worksheets:

- ✅ System Visibility Snapshot
- ✅ Data Risk Snapshot
- ✅ Vendor Readiness Tracker

Use these to support internal discussions, planning, and vendor conversations.



System Visibility Snapshot

System	Vendor	Handles Sensitive Data?	Authentication Type	Notes

Data Risk Snapshot

Data Type	Stored Where	Retention Period?	Risk Level (Low/Med/High)

Vendor Readiness Tracker

Vendor	Service	PQC Roadmap Known?	Action Needed

About the Author

I'm Wil Brown, a WordPress consultant, developer, and educator who's been helping organisations build and manage websites since 2005.

Through Zero Point Development, I work with research, education, and non-profit organisations to:

- Understand their digital systems and dependencies
- Reduce long-term risk
- Ensure their platforms remain stable, secure, and adaptable

My focus is not just building websites.

It's helping organisations make better decisions about the systems they rely on.



If you'd like help understanding your current setup and where your risks sit:

👉 **Book a strategy session at zeropointdevelopment.com and I'll help you understand where your risks sit.**

zeropoint DEVELOPMENT