

# PKI ADMIN

## THE RACE AGAINST QUANTUM TIME



ERIK HART 2024

KEYFACTOR

# READY, SET, QUANTUM

Ready or not, the race to quantum-safe readiness is on. No, there's no doomsday clock winding down to zero and your RSA keys won't spontaneously combust overnight. But here's the reality: the cryptographic standards that safeguard data across every corner of your business - networks, applications, workloads, servers, and devices - is now under threat, with profound real-world consequences.

Thought you could leave this problem for the next PKI admin? While you're sipping margaritas, courtesy of your retirement fund? Think again. Whether quantum computers pose a threat in two years or ten, new standards are here, timelines for migration are set, and "harvest now, decrypt later" attacks already pose a real and current threat.

**SO, BUCKLE UP, BECAUSE YOU'RE  
ALREADY ON THE RIDE.**

That's why we crafted this comic. Inside these pages, we'll serve up practical insights with a side of hyperbole and humor. Consider it a "Hitchhikers Guide to the Post-Quantum Galaxy." Because, let's face it, your job is serious enough. So, grab your towel and don't panic, let's dive in.

# BREAKING BAD... ENCRYPTION

By cybersecurity standards, RSA and ECC - the cryptographic algorithms that protect most of the world's communications - are ancient relics. But these algorithms have stood the test of time, still encrypting our data like it's 1999, and doing it well.

That's all about to change. There's a new 'boogeyman' in town, and it's coming to crash the crypto party. In the next decade, quantum computing is expected to turn RSA's midlife crisis into an existential meltdown.

That's right, our trusty (and, admittedly dusty) RSA is going the way of the dodo, the Betamax, and unironic mullets. If you thought the move from SHA-1 to SHA-2 was fun, you're in for a real treat.

So, how do we stop quantum computers from breaking soon-to-be bad encryption? It's time to embrace cryptographic agility.

IT'S TIME TO ENCRYPT  
LIKE IT'S 2030.



# PKI ADMIN IS BACK!

He's the hero nobody asked for, but everyone needs. Like many in his role, he didn't choose a life of PKI; it chose him...in the form of a Slack message that snowballed into a job responsibility. By day, he's 'just another IT guy', but when a certificate expires, he leaps into action, vanquishing HTTP errors in a flash.

In the last edition, PKI Admin emerged victorious. Armed with nothing but a keyboard sticky with energy drink residue and a browser history full of Stack Overflow, he stepped up his automation game and brought order to PKI chaos.

Just when he thought he'd take a vacation (ha!), a new threat emerged. It's the plot twist everyone saw coming and no one prepared for.

Now our hero faces his biggest challenge yet, answering the call to get his organization quantum-ready before time runs out! Will he succeed? Maybe. Will he finally get that long-overdue raise?

Don't hold your breath.



## PKI Admin (alias)

Speaks fluent X.509, but struggles with small talk

Has a pet goldfish named "TLS 1.3"

No formal PKI training, but has a Ph.D. in Googling error messages

Social media consists entirely of desperate posts on tech forums at 2 AM



PRESENT DAY. 2 AM.



**BREAKING!**

**NIST ANNOUNCES NEW PQC STANDARDS,  
THE RACE TO READINESS IS ON**

**Zzzz**



DREAM STATE. SOMETIME IN THE 2030S.

HUH? I THOUGHT I'D BE RETIRED ON A BEACH,  
NOT FACING A POST-QUANTUM APOCALYPSE

TAKE ME BACK! I PROMISE  
I'LL STOP THIS! JUST LET  
ME GO BACK!

# IT'S NOT A WARNING, IT'S A WAKE-UP CALL

Okay, so maybe our hero needs to lay off the late-night caffeine and crypto forums. But beneath this quantum-induced (and slightly exaggerated) nightmare lies a very real wake-up call. Quantum computing isn't a theory, it's a reality. And hitting 'snooze' on your quantum-safe security strategy isn't an option.

WHERE DOES PKI ADMIN GO FROM HERE?





## KEY TAKEAWAY

# STOP HITTING 'SNOOZE' ON YOUR QUANTUM-SAFE STRATEGY

#1

## QUANTUM-SAFE STANDARDS ARE HERE

In 2024, the National Institute of Standards and Technology (NIST) published its first set of PQC standards, including FIPS 203, 204, and 205. These quantum-safe algorithms are much, much different, with bigger keys, bigger signatures, and new concepts like key encapsulation. The time to test, educate, and familiarize yourself is now.

#2

## ALGORITHM END OF LIFE IS COMING

Regardless of when a quantum computer becomes capable of breaking modern encryption, NIST has already set the timer on migration for US agencies. By 2030, widely used methods like RSA, ECDSA, EdDSA, and ECDH will be deprecated, and by 2035, they will be completely disallowed. Other regulatory and industry bodies have begun to roll out similar timelines.

**#3**

## MIGRATION WON'T HAPPEN OVERNIGHT

Still haunted by SHA-1 to SHA-2? The shift to PQC is monumental by comparison. [IBM estimates](#) a 12-year journey to full quantum-safe integration for your business, including time needed to identify cryptographic assets and dependencies, align with partners, educate and upskill teams, and implement new standards. This isn't just an IT project, it's a career-defining initiative.

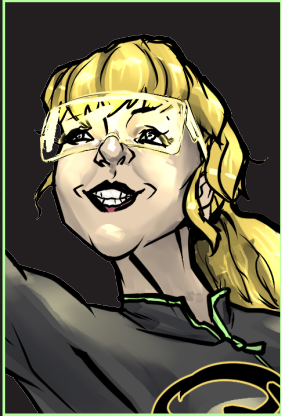
**#4**

## THE THREAT ALREADY EXISTS

Data not secured today using PQC is vulnerable to "harvest now, decrypt later" attacks, whereby bad actors steal data and store it until a cryptographically relevant quantum computer becomes available. Sensitive data that retains value for years poses the highest risk, putting more urgency behind the need to adopt quantum-safe standards.

# ENTER QBIT!

Meet Qbit. She's a superhero with the power of superposition. Living in multiple times and places at once can be dizzying, but her mission is clear: stop the cryptocalypse. Is she a caffeine-fueled hallucination or a superhero sent from the future? We'll never know. One thing's for sure; PKI Admin must succeed.



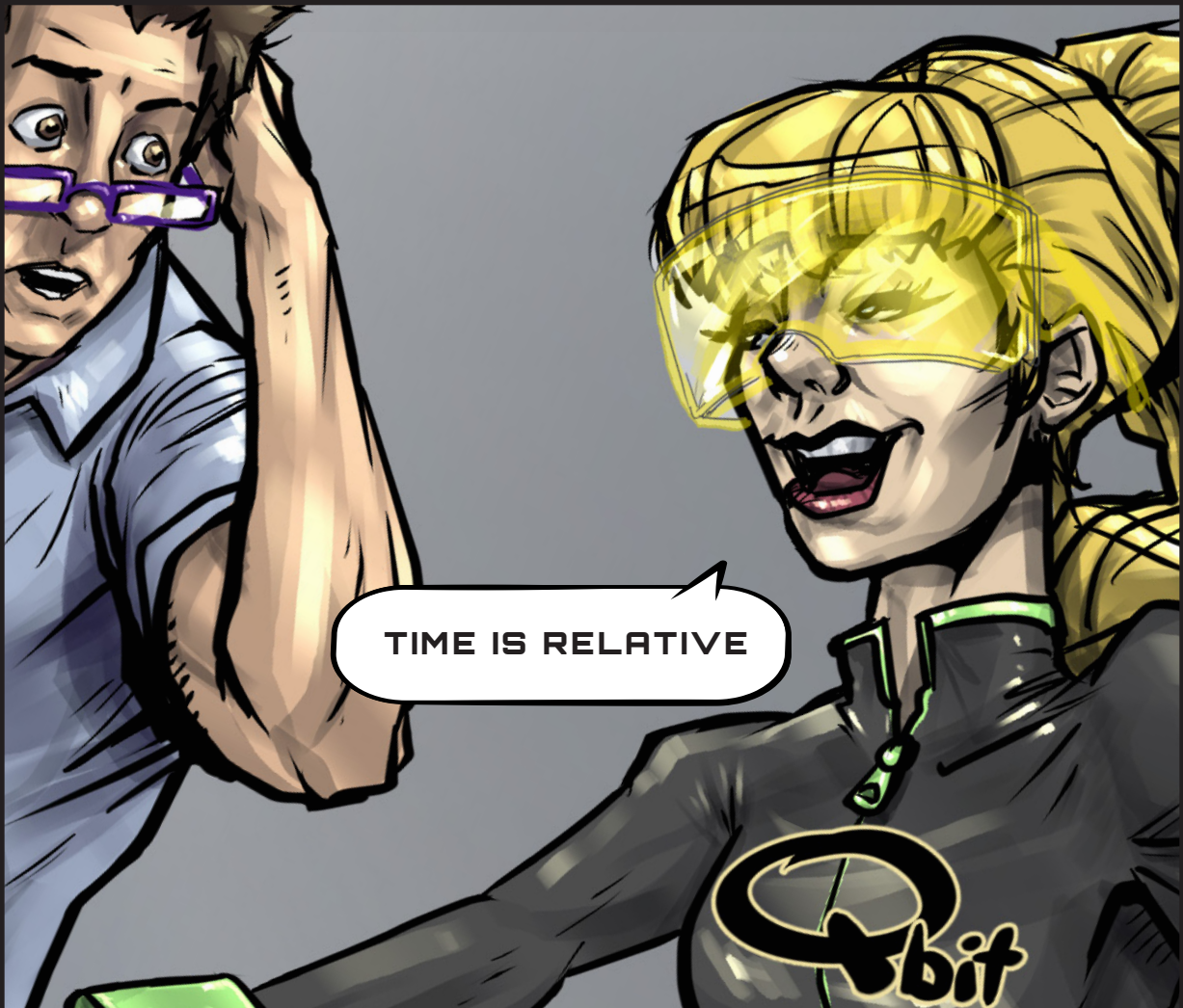
### **Qbit (alias)**

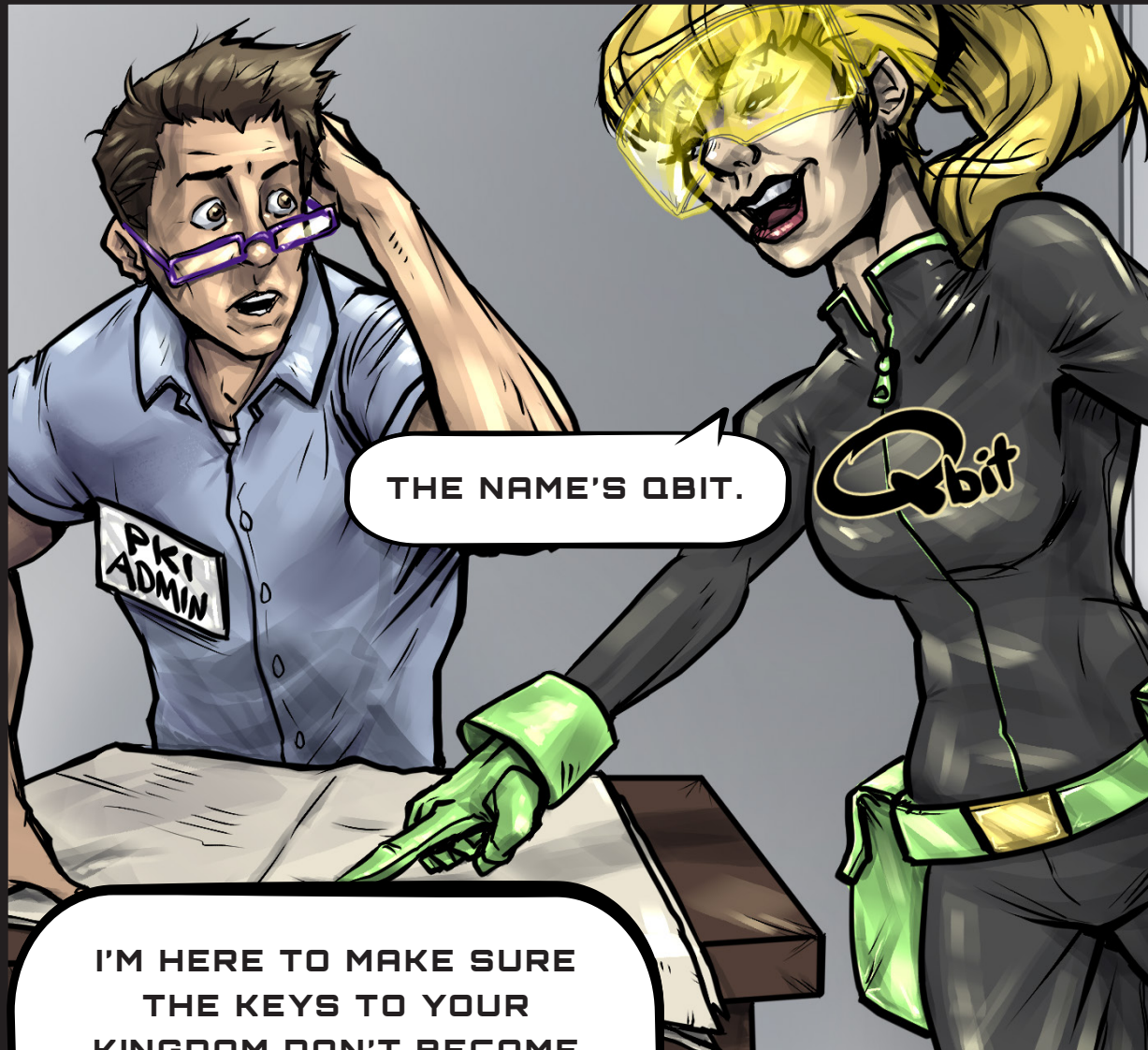
Lives in the past, present, and future - simultaneously

Has the uncanny ability to predict zero-day vulnerabilities

Can factor large numbers in her head, but only when no one is looking

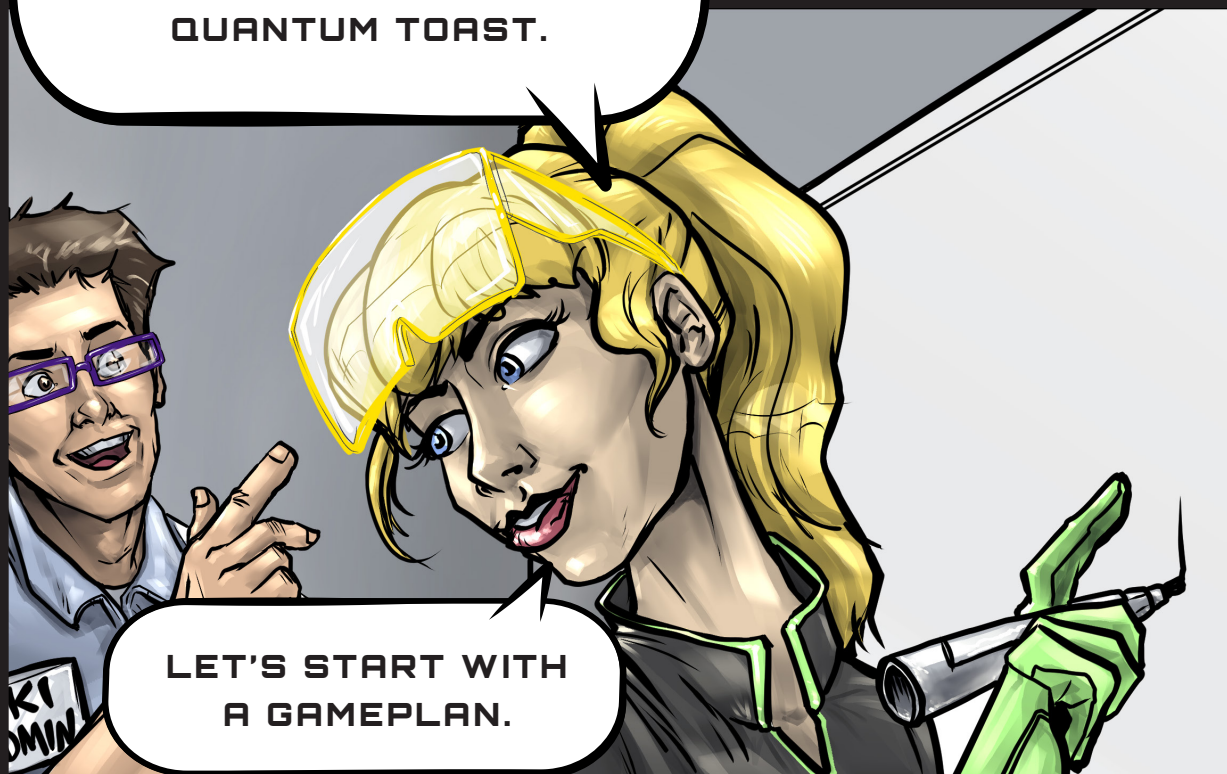
Somehow knows the exact state of every certificate without observing them





THE NAME'S QBIT.

I'M HERE TO MAKE SURE  
THE KEYS TO YOUR  
KINGDOM DON'T BECOME  
QUANTUM TOAST.



LET'S START WITH  
A GAMEPLAN.

# TICK TOCK GOES THE QUANTUM CLOCK

So, the clock is ticking, but where do you start? Well, not everyone has a quantum-powered superhero on speed dial. Fortunately, NIST and other acronym-loving agencies offer sound advice to get you started on your journey. We've distilled their wisdom down to four digestible steps to kickstart your quantum makeover.

## KEY TAKEAWAY

## START YOUR JOURNEY TO QUANTUM-SAFE SECURITY - LIKE, RIGHT NOW

#1

### ESTABLISH YOUR CRYPTOGRAPHIC INVENTORY

The first step is to conduct an audit of your existing PKI infrastructure, algorithms, and protocols. Use automated tools that can help you build a centralized inventory by scanning certificate authorities (CAs), servers, appliances, file systems, network interfaces, source code, and binary files.

**#2**

## ASSESS YOUR RISK EXPOSURE

Now you can begin to understand your cryptographic dependencies, and map the connection between data, systems, and applications to the certificates, algorithms, and protocols that protect them. You can also begin to determine what systems need to be upgraded or replaced.

**#3**

## PRIORITIZE HIGH VALUE & LONG-LIVED ASSETS

The transition to quantum-safe isn't a one-and-done exercise, it's a multi-year project. Start by prioritizing digital certificates used to protect your most sensitive and long-shelf-life data, critical infrastructure and hardware, roots of trust, and firmware for long-lived devices.

**#4**

## CONSULT WITH YOUR THIRD-PARTY VENDORS

Don't forget about cryptography embedded in your third-party products and services. Engage with your vendors to understand their timeline for migrating to quantum-safe cryptography, and the implications it will have on performance, compatibility, and ease of integration.

RIGHT. AND OUR DEADLINE  
FOR Q-DAY IS WHEN...?

Q-DAY ISN'T JUST ONE  
DAY, IT'S EVERY DAY  
FROM NOW ON. EVERY DAY  
WILL BRING NEW THREATS  
AND CHALLENGES.

APR

# 'Q-DAY': BECAUSE ONE DOOMSDAY WASN'T ENOUGH

Sure, quantum computers are real. But when can we really expect them to be a threat? Because you've got 'today' problems to deal with... like stopping that sysadmin from setting up a Bitcoin mining rig in the server room for 'research purposes.' Tomorrow can wait, right? Not exactly. Experts debate when 'Q-Day' will arrive, but one timeline is certain: current algorithms have an expiration date, and it's approaching quickly.

2025

2030

2035

NIST to deprecate RSA and Elliptic Curve (ECC) algorithms in 2030

[Learn more](#)

NIST to disallow RSA and Elliptic Curve (ECC) algorithms in 2035

[Learn more](#)

2029

Gartner predicts quantum computing will render traditional cryptography unsafe

[Learn more](#)

2031-2039

Most experts predict quantum computers will be capable of breaking today's encryption between 2031 and 2039



COMPANY HOLIDAY PARTY, 2025.



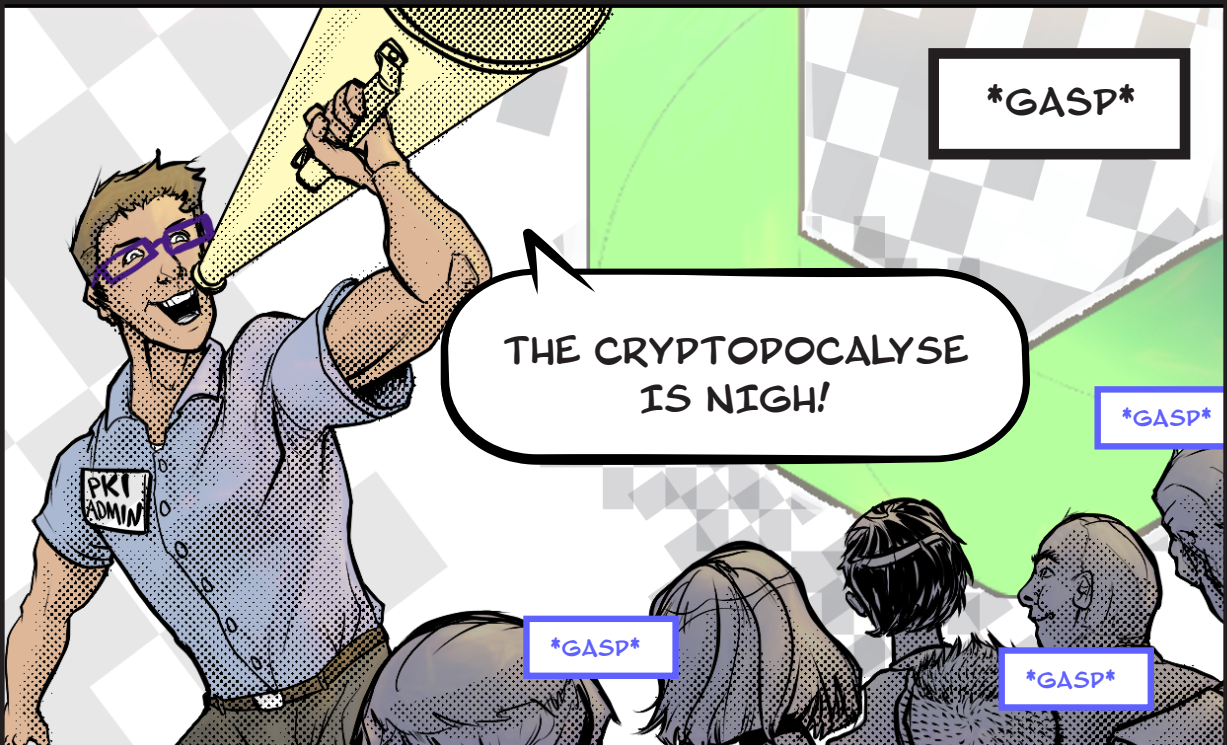
\*GASP\*

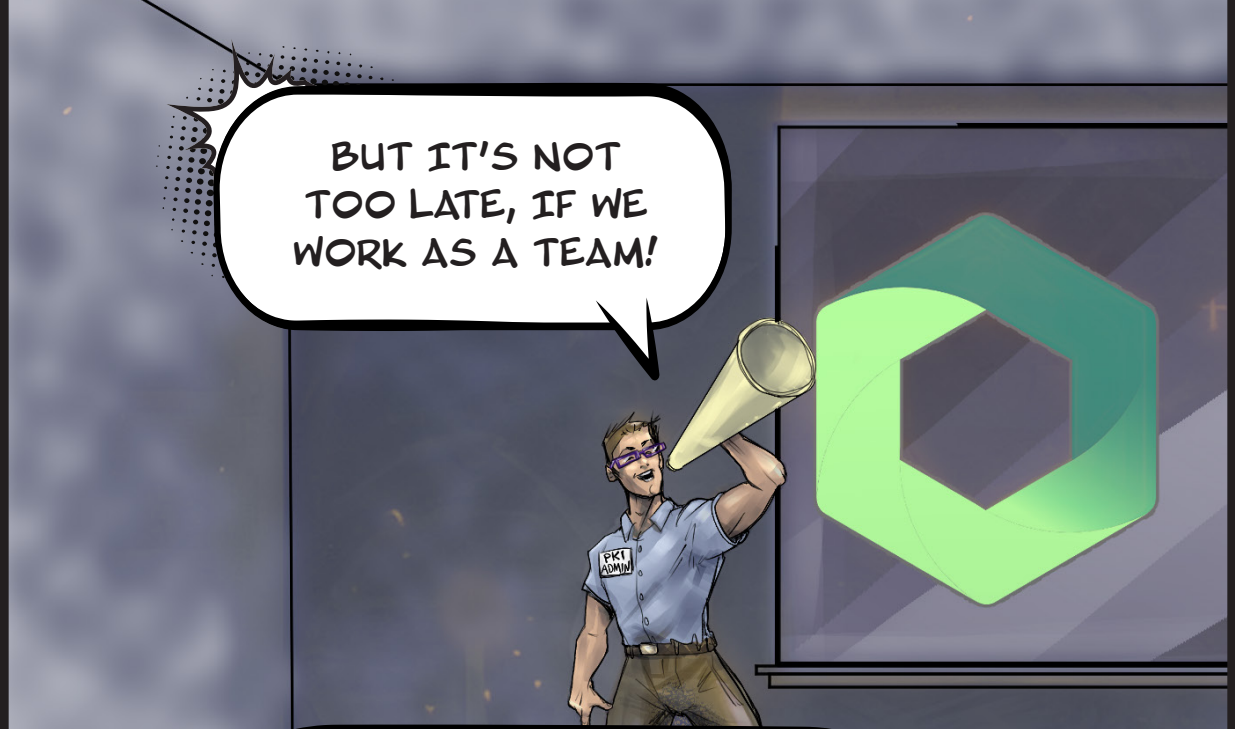
THE CRYPTOPOCALYPSE  
IS NIGH!

\*GASP\*

\*GASP\*

\*GASP\*





BUT IT'S NOT  
TOO LATE, IF WE  
WORK AS A TEAM!



SORRY, HE MEANS WELL...

IS THAT THE  
NEW INTERN?

NO, I THINK THAT'S  
THE COFFEE MACHINE  
REPAIR GUY

# TAKING THE QUANTUM LEAP: IT'S A TEAM SPORT

Ok, so maybe you shouldn't crash the company holiday party like an unhinged doomsday prophet. Point is, taking the quantum leap isn't a solo mission, it's a team sport. Armed with quantum-inspired zeal and a dash of cryptographic common sense, you're ready to lead the charge. It's time to rally the troops, but first, read the room.

## KEY TAKEAWAY

## CREATE A CULTURE OF QUANTUM-READINESS

#1

### EDUCATE AND EQUIP YOURSELF

Get to know the new cryptographic algorithms and standards and how they'll integrate with your systems. Tap into a growing number of resources, like [Keyfactor PQC Lab](#). Not only do you become a champion for change, but your skills also become invaluable to the business.

**#2**

## SHARE KNOWLEDGE AND EXPERTISE

Build awareness by embedding education on quantum-safe security principles in ongoing training and meetings. Become a go-to source by staying in tune with the latest news and emerging standards, and keeping your teams up to speed when impactful updates are announced.

**#3**

## ESTABLISH A CENTER OF EXCELLENCE

Lead the charge, but don't ride solo. Build your cross-functional team, often called a "Crypto Center of Excellence" (CCOE), to define and execute a transition plan, lead proof of concepts, and translate learnings into best practices and policies for the organization.

**#4**

## GAIN BOARD-LEVEL SUPPORT

The board doesn't care about algorithms and protocols, they care about one word - risk. You and your CISO play a critically important role in advocating for quantum-safe security by conveying business risks and operational impacts, not the intricacies of a qubit.

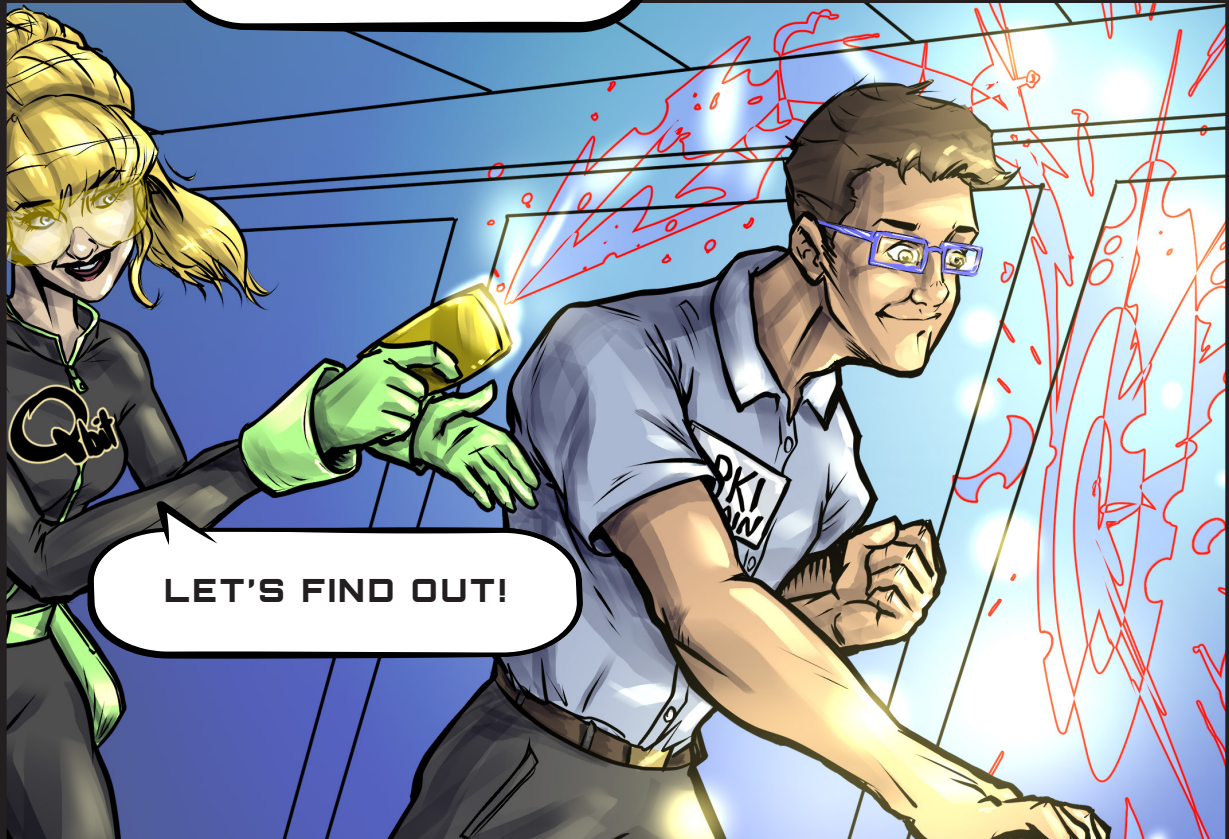
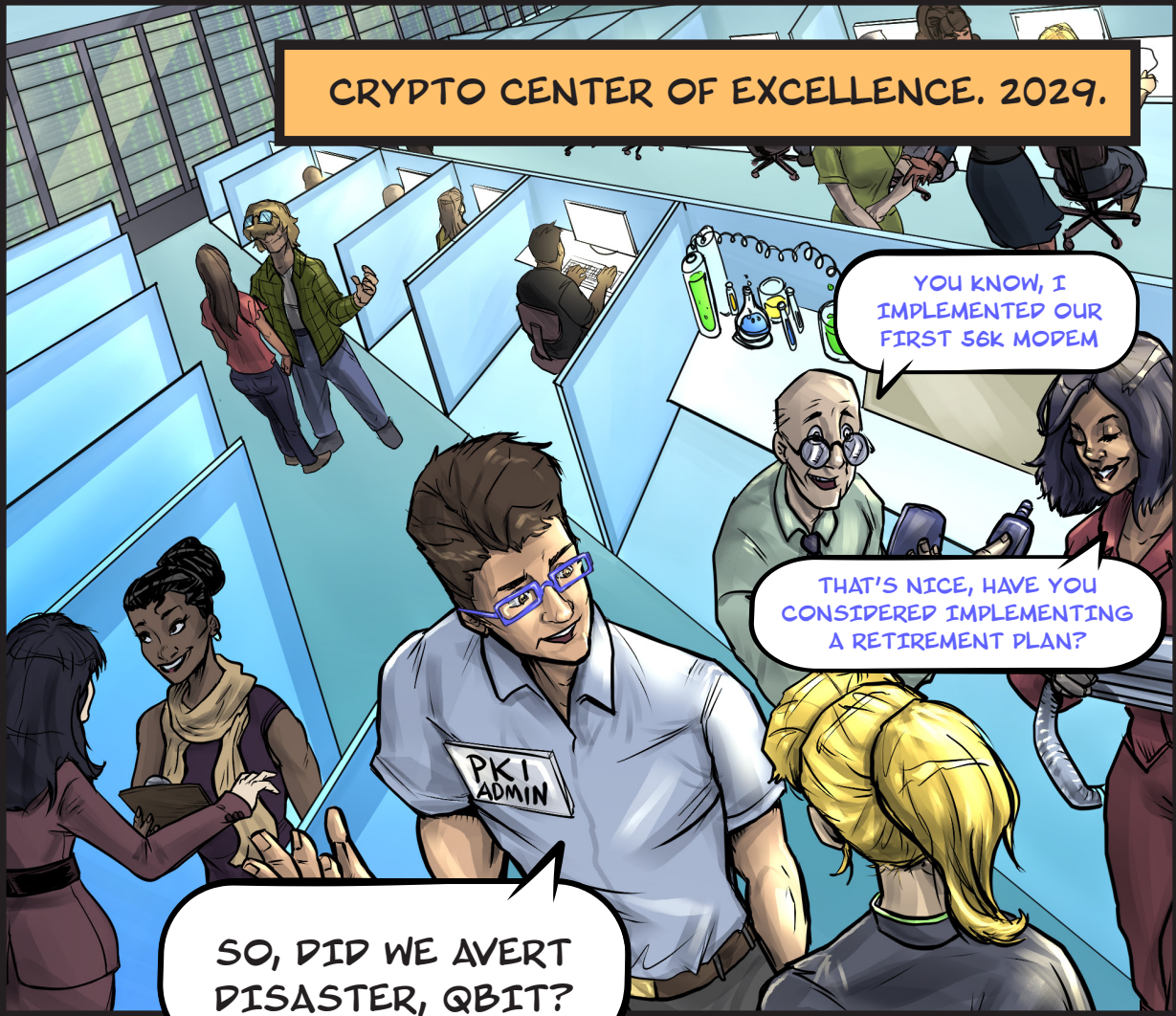
CRYPTO CENTER OF EXCELLENCE. 2029.

YOU KNOW, I IMPLEMENTED OUR FIRST 56K MODEM

THAT'S NICE, HAVE YOU CONSIDERED IMPLEMENTING A RETIREMENT PLAN?

SO, DID WE AVERT DISASTER, QBIT?

LET'S FIND OUT!



# QUANTUM SHIFT, ENGAGE

Congratulations! You've assessed the risks, rallied the troops, and crafted a plan. What's next? It's time to put that quantum-safe transition plan into action. Brace yourself for a rollercoaster of trial, error, and the occasional 'why did we start this' moment. But hey, that's why we embarked on this quantum journey early - because losing this race isn't an option.

## KEY TAKEAWAY

# UPGRADE, IMPLEMENT, AND ENABLE CRYPTO-AGILITY

#1

## UPGRADE YOUR TRUST INFRASTRUCTURE

Evaluate your PKI, HSM, digital signing, key and certificate management systems to ensure that your teams are equipped with the tools they need to test and implement new quantum-safe standards, now and into the future. Working with the right vendors is critical.

**#2**

## BEGIN TESTING AND IMPLEMENTATION

Complete proof of concepts and system upgrades in alignment with risk assessments, vendor roadmaps, and evolving standards (e.g., NIST). Test the new cryptographic protocols and evaluate the potential impact on systems and performance before migrating PQC to production.

**#3**

## ADOPT MONITORING AND AUTOMATION

Manual certificate management processes are already cumbersome; quantum-safe migration will render them obsolete. Implement tools to monitor your environment and automate migration of quantum-safe certificates without disrupting business operations.

**#4**

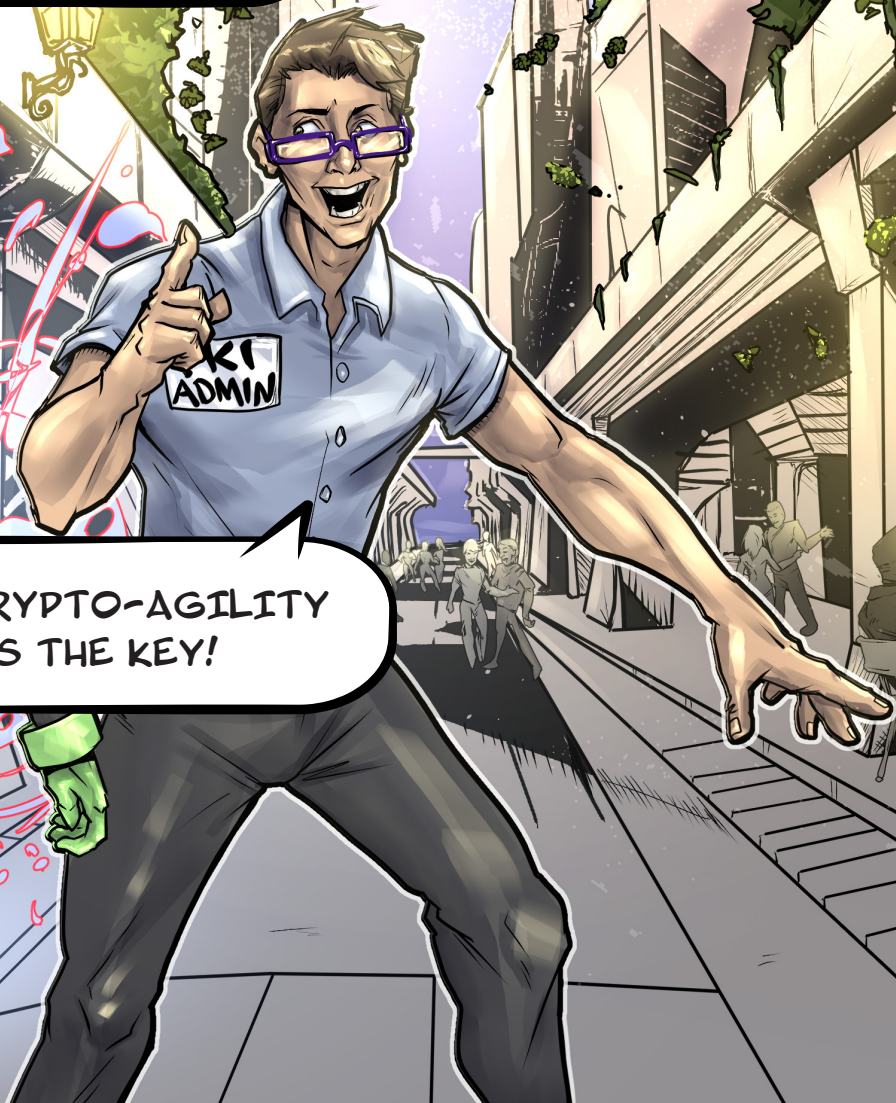
## STAY VIGILANT, STAY AGILE

Crypto-agility isn't a technology, it's a strategy. It's a proactive approach to encryption that focuses on the ability to quickly adapt cryptography to changing environments and risks. An effective strategy is founded on a strong policy framework and governance model.

QUANTUM CITY. 2036.

SEE! THE FUTURE IS  
BRIGHT WHEN WE'RE  
QUANTUM-READY...

AND CRYPTO-AGILITY  
IS THE KEY!





# **CRYPTO-AGILITY: YOUR KEY TO SUCCESS**

Not all heroes wear capes. Sometimes, they wear purple glasses and arm-wrestle with application owners over certificate renewals. We get it, managing PKI won't earn you a Nobel Prize - more likely a 2 AM alert about a downed server. But as a PKI admin, you're the unsung guardian of digital trust. Your mission, should you choose to accept it (let's face it, you don't have much choice), is to navigate the journey into the quantum era - safely.

## **WINNING THE RACE WITH CRYPTO-AGILITY**

Agility is "the power of moving quickly and easily." So, crypto-agility is the ability to move quickly and easily with your cryptography. And it's not just about stopping the cryptopocalypse.

Crypto-agility is essential to safeguarding your business in a world of constant change - when an algorithm suddenly fails, a CA is compromised or distrusted, a crypto-library bug surfaces, a wildcard certificate expires, you name it. These things aren't apocalyptic events, they're pains and challenges you deal with every day.

A sound strategy, backed by the tools, policies, and people to support it, ensures that you can adapt quickly, without painfully slow processes or operational disruptions that land you in a world of hurt with the CIO.

So, if you're ready to face your quantum nightmares, why not take the next step? Visit Keyfactor PQC Lab and get hands-on with free tools and resources, learn from industry experts, and discover solutions to accelerate your journey to quantum safety.



Visit Keyfactor PQC Lab

Get started ↗



Keyfactor  
PQC Lab

## KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.

For more, visit [keyfactor.com](https://keyfactor.com) or follow [@keyfactor](https://twitter.com/keyfactor).



# GOT PKI PROBLEMS?

Explore the first edition of our comic, "PKI Problems," featuring real-life PKI pitfalls and fiery Reddit rants.

Grab your copy here.

[Download now ↗](#)

# KEYFACTOR



## THANK YOU

WRITER     Ryan Sanders  
CONTRIBUTOR     Chris Hickman  
ILLUSTRATOR     Matt Erkhart  
DESIGNER     Rachel Govert