digicert

Table of Contents

2

2 Maturity Levels

4

4 Risks

4 Education

4 Engagement

5

5 Risks

6 Education

6 Engagement

6

6 Risks

7 Education

8 Engagement

8

8 Risks

8 Education

9

9 Resources

Hardware Security Modules

Identifying custom key generation implementations

It's important to determine if your organization uses Hardware Security Modules (HSMs) for custom key generation, and how those HSMs are used. You

organization's HSMs are capable of upgrade to quantum-safe encryption. You'll also want to verify the timeline for those upgrades. Be sure the HSM updates and practices align with your organization's timeline and plans for deployment of quantum security. DigiCert recommends industry leaders Gemalto and Utimaco for the best in quantum-safe HSMs.

PQC Novice Engagement

As your knowledge grows, it's important to engage in certain tasks, in order to move from PQC Novice to PQC Apprentice. This checklist will help you work toward protecting your organization from quantum computing threats.

- Make an effort to understand how encryption across your entire network is the foundation of best practices in security. Get a sense of your entire network, so you can see the scope of your encryption needs as you move to add quantum-

PQC Apprentice Education

What is crypto-agility?

In order to move from PQC Apprentice to Practitioner, this professional must learn crypto-agility. Both what it is, and what it is not.

Crypto-agility focuses on visibility and dynamic movement. It is awareness of every place encryption is used within your organization (like protocols, libraries,

of how these encryption technologies are deployed, and the ability to quickly identify and remediate issues when they arise. True crypto-agility means possessing the capabilities necessary for seamlessly replacing outdated crypto via automation when the time comes.

Crypto-agility is not the ability to use different algorithms for critical functions (like hashing, signing, or encrypting). It's also not the ability to choose which algorithm to use for a particular function (like SHA-1 or SHA-256).

Enemies in disguise

In addition to developing crypto-agility, the PQC Apprentice must understand the potential for threats from seemingly friendly sources. No amount of

and information are shared with companies or entities that are unsecured against quantum attacks.

To move from PQC Apprentice to PQC Practitioner, you'll need to evaluate how vendors, partners and third parties introduce vulnerability to the organization. Make sure you'rilityour third-party
providers and discussing how they plan to test and secure against quantum threats.

PQC Apprentice Engagement

As a PQC Apprentice, you have a solid understanding of the impending quantum threat. Now it's time to deepen your knowledge and develop a plan. This checklist will help you work toward protecting your organization from quantum computing threats.

As a PQC Practitioner, you may feel ready to begin testing. With a fair amount of quantum computing knowledge, and a plan in place, the next logical step is pitting your security measures against possible threats. But where should you begin? And what options are available, despite the fact that there's no current PQC standard?

PQC Practitioner Education

Working with hybrid in a testing environment

With your skills in crypto-agility, you already have

organization's systems. The next step in your education is understanding how to incorporate testing technologies into your security practices using hybrid RSA/PQC. Both ISARA and DigiCert offer PQC test kits that include everything you'll need to create and test

cryptographic algorithm paired with a classical encryption algorithm, so you'll be able to test the viability of deploying post-quantum hybrid TLS certs while maintaining backwards compatibility. By building and testing in a sandbox environment, you'll gain

of your organization is on the line. In a test environment, you can watch hybrid certs interact with current applications, and seek solutions before you deploy your live PQC security system.

Data sensitivity

One of the most challenging threats to organizations today is the theft of secure information that's vulnerable to quantum attacks. Criminals are stealing and hoarding data, even though it's currently encrypted, in anticipation of future hacking solutions with quantum technology.

It's important, as you develop your PQC knowledge and planning, to decide what organization is the most sensitive or of the highest value. This information needs to be guarded with PQC security measures, so that it's safe not only by today's encryption standards, but by tomorrow's, too. Combating this future threat

Data breache

For detailed information on the cost of data breaches, look at the latest Ponemon Institute study: https://securityintelligence.com/ponemon-cost-of-a-data-

is no easy task. It requires conversations with your

As you consider which of your organization's assets

like personal client records and intellectual property. Personal client records represent a huge risk to

reputation. Intellectual property has been amongst the most attractive targets from conventional hackers over the past two decades, especially from criminals inside China and Russia, where harvesting foreign intellectual property has become an important part of national economic and security strategies.

PQC Practitioner Engagement

As a PQC Practitioner, you're ready to begin testing the security system you plan to deploy. Now it's time to test. This checklist will help you work toward protecting your organization from quantum computing threats.

- Meet with key people inside your organization to identify which assets and information need to

  client records and intellectual property, along with recommendations from your CIO, CTO, and other knowledgeable members of your org's team. Set

  of PQC deployment.
- Select a PQC test kit and learn about testing options and processes. Make a plan for building

-

  log vulnerabilities and incompatibilities. Prepare a

PQC Master

The PQC Master has completed setup of all documented standards for use of encryption within their organization. This professional understands and currently incorporates crypto-agility into their practices.

For more information on Post-quantum Encryption, please visit our ongoing blog series
to bring quantum-safe security practices to your organization today, reach out to Tim Hollebeek at tim.hollebeek@digicert.com.

di