ANNUAL REVIEW

NCSC Annual Review 2024

Looking back at the National Cyber Security Centre's eighth year and its key developments and highlights, between 1 September 2023 and 31 August 2024.

Post-quantum cryptography

Migration to post-quantum cryptography (PQC) may feel daunting, but it also promises major opportunities. The NCSC explains how it will help organisations plan their migration.

Cryptography is everywhere.

It protects our data when we access online services and shops. It's used when you electronically sign legal documents. It's a critical part of our military and emergency services' communications and the smooth running of the UK's critical national infrastructure (CNI). Yet it's also invisible to almost all users, even though cryptography underpins every online service, and every aspect of the UK's infrastructure.

Quantum computers of the future, with their potential to offer capability unachievable by any conventional computers, pose a threat to much of the cryptography that underpins the security of our digital infrastructure. Although such computers are some years away, governments of all major nations are investing heavily in the development of quantum computing.

Migration to **post-quantum cryptography (PQC)** – cryptography that is resistant to attack by quantum computers – is the primary mitigation to this threat. There will be a global migration of IT and operational technology systems to use PQC. Major technology firms are already integrating PQC into some of their core products.

PUBLISHED

3 December 2024

REVIEWED

3 December 2024

VERSION

1.0

WRITTEN FOR

Public sector

Our priority at the NCSC is to ensure that the UK's migration to PQC is smooth and does not raise wider cyber risks to our central government systems and our CNI. However, as the national technical authority for cyber security, we also need to help system and risk owners across all sectors of the UK plan their PQC migrations. We can't solve all the challenges in migration for every organisation; the scale is far too large. So, our focus is on how we raise understanding, set examples of best practice and identify interventions the NCSC can make that have the most scalable impact. These are outlined below.

Providing access to cryptographic expertise

Addressing the quantum computing threat has, for many years, been a problem for mathematicians and cryptographers, and this summer, three post-quantum algorithm standards were finalised. However, migration to PQC is a much broader cyber security effort that needs expertise from cryptographers alongside systems integrators and engineers.

A challenge for migration to PQC is that preparatory effort in **cryptographic discovery** (the process of identifying sensitive data, and where the cryptography that protects it lives within a system) is not a simple activity. However, the UK has some world-leading specialist cryptography companies, who have a focus on PQC. The NCSC is currently building a pilot scheme to accredit some of these companies, and to help them find markets in the UK. This will also help some of our critical sectors access the expertise required to help them prepare for their migration.

As these initiatives encourage new companies in this sector to grow, they will need to be able to hire skilled talent from UK universities, and develop applied cryptographers, fusing expertise from a wide range of scientific disciplines, who understand how to build cryptographic systems in the real world. To enable this growth, we would be keen to see groups with deep expertise in the implementation of cryptography flourish within UK academia, so that all sectors of the economy will benefit.

Maintaining confidence in PQC

Migration to PQC, for many organisations, will take more than a decade and cover multiple investment cycles and changes of leadership. This means we need to understand the incentives that will encourage organisations to invest now; if everything is left until several years' time, migration will be poorly planned, rushed, more expensive, and likely introduce the sort of easy-to-exploit vulnerabilities we are too used to seeing.

The NCSC's work on market incentives will play a part in this. We know that our regulators understand their sectors better than we do, so our focus is to equip those regulators with the knowledge and advice that will enable them to set the right direction.

As well as building this initial momentum, we need to ensure that we help maintain confidence throughout migration. We are now in a period where mature implementations of the algorithms, built into modern protocols, are still evolving. In this early phase where organisations are *planning* their migration (rather than *deploying* PQC widely), we might expect to see some vulnerabilities; not in the underlying cryptography but in the *implementation* of the technology. There is a role for many groups, in the media, in academia, and in government, to discuss these cases maturely. The NCSC's role, as the authority within government on cryptography, will be to help our key partners navigate these discussions, and signal to the rest of the UK our confidence in PQC.

Learning from the early adopters

There are some sectors – finance is a good example – where working within international regulations (and keeping pace with competitors) means that planning is already well underway in many larger organisations. There are other sectors that are less well-resourced with significant legacy technology, for which direct upgrades to PQC will not be possible.

The NCSC's approach is to identify good practice and lessons learned in the faster-moving sectors. Since the differences between sectors are vast, we're not planning to set universal target dates for migration. Instead, we'll work with regulators to help them set suitable targets for each sector individually.

However, we do believe that planning for *all* sectors should get underway as soon as possible, using what we learn from early adopters to develop case studies and guidance for some of the harder migration problems. Where we identify aspects of migration within government (and within unregulated areas that are not fully understood), we will support pilot projects that help us provide the guidance that people need.

The benefits of secure migration

We intend to have accredited a small group of PQC consultancies by the end of March 2025. Alongside this, we will be running test projects within government focussing on the discovery activities that the NCSC recommends all organisations undertake; understanding where and how cryptography is used in all systems - theirs and their suppliers, the technologies that rely on it, and

the data it protects whether in transit or storage. We will also be refining our broader offer to UK industry and provide tailored advice to sectors of national importance to support transition to PQC.

Migration to PQC is a national technology change programme. It comes with significant potential cyber risk, and we have a strong responsibility to manage that. But it also promises major opportunities. All organisations should be focussing on activities that underpin PQC migration; clear system auditing, rationalising services, putting a greater focus on building systems that can be easily updated in future and growing new technical skills. These are all important for broader secure design and management, so if the migration is done well, we will all benefit, far beyond the cryptographic changes.

← Previous page

Chapter 04: Keeping pace with evolving technology

PUBLISHED

3 December 2024

REVIEWED

3 December 2024

VERSION

1.0

WRITTEN FOR

Public sector