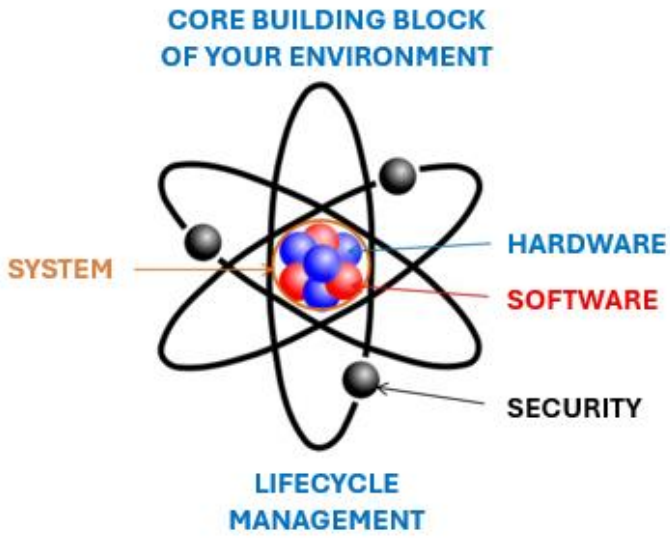
# The FUTURE is now
# LIFECYCLE Management

The days of implementing a server solution and leaving it untouched for 10+ years is over. Lifecycle Management needs to be baked-in right from the start. We are used to the regular and automated updates to our mobile device's Operating System, Firmware, and Applications but not to our Enterprise environments. Extended support on hardware and software components may leave you with the false sense of being covered, but it actually leaves you exposed and vulnerable to cyber-attacks among other considerations. Many projects look at a 5-year lifespan when being implemented but often don't consider the viability of the software components during this timeframe.

After a product reaches the point in time where the last update or patch has been applied, and it enters into extended support, it is no longer even being checked for potential security vulnerabilities yet alone patched. Before this happens, you should have a plan in place to update your environment considering all aspects of the Lifecycle.




Let's compare the core building block of your environment to an Atom. The Nucleus is your System and the Electrons orbiting around it is your overlying datacenter security infrastructure (Physical, Network, Policies, Tools, etc.).

The Nucleus is your System, the Server and Storage infrastructure with various Hardware and Software components (the Protons & Neutrons). The Hardware includes all Hardware component, Firmware, and Firmware-based products. The Software includes Application Software as well as System Software, such as the Operating System, management, and availability products.

All of these, Hardware, Software, and the Firmware components have Security aspects to them. You must make sure that this Core Building Block, the Atom, remains Secure, within the overarching datacenter security infrastructure, for the entire lifespan of implementation.

Author: E. Bruce Turgeon – bringing over 30 years of IT Industry experience with IBM Power Systems to help Businesses to Acquire and IBM Business Partners to Solution Modernized and Rightsized Architectures that are Optimized and Cost Effectively to deploy.

Q-SEC

We have seen Enterprises that have requested 3rd party support for environments that they implemented more than 10-years ago, and for which the original vendors no-longer offer support. Not only that, but they have previously been Cyber-Attacked and had to deal with Ransomware.

These are environments that have, to some degree, been neglected and allowed to get to an unacceptable state of support and vulnerability.

Even worse, is that after 10 or more years, it is difficult to find the internal resources that understand the environment. Rather than focusing on understanding and fixing what is in-place, there is a desire to re-platform the entire solution. This typically prompts a complete re-build of the environment from the ground up that can span multiple years.

## Lifecycle Management

*At Q-Speed Enterprise Consulting Inc., we do just that, we implement your solutions with Lifecycle Management up front and center. We are there with you for the entire Lifespan of your deployment, helping to guide you through updates, migrations, and even with adding enhanced functionality over time, through regularly scheduled meetings and checkpoints twice a year or based on your requirements.*

It does not matter if you are considering On-Premises or Cloud environments, Lifecycle is still key and needs to be accounted for in your implementation. Re-platforming or moving to the Cloud still requires a Lifecycle mindset to keep Hardware, Software and Firmware current, supported, and up-to-date on security patches. Newer versions of these products also typically include more security tolerant capabilities.

Cloud computing is still relatively young, so it is not clear what happens when the infrastructure is updated by the Cloud provider. Clients should be aware, and not assume that they can indefinitely keep running on out-of-date and end-of-life equipment and realize that it does cause concern for security vulnerabilities.