B2B Exception for “Free Security Updates” under the CRA

Overview

We support the Cyber Resilience Act’s objective of improving cybersecurity across the lifecycle of products with digital elements. Manufacturers should have clear obligations to identify, assess, and remediate vulnerabilities, and business customers should receive the information and support necessary to manage cybersecurity risk.

However, in the B2B context, the CRA’s requirement that security updates be provided “free of charge” should not override negotiated commercial arrangements between sophisticated business entities. Enterprise customers often operate complex, regulated, and highly customized environments. They negotiate support, maintenance, update, and baseline-upgrade arrangements based on product criticality, deployment model, operational risk, regulatory obligations, and internal change-management requirements.

For these reasons, the CRA should preserve freedom of contract for sophisticated B2B parties by allowing manufacturers and business customers to agree on security update, support, maintenance, and baseline-upgrade models appropriate to the product and deployment environment.

Therefore, we would propose the following new CRA-related amendment to the Digital Omnibus that would enable a contractually agreed B2B exemption:

CRA, Annex 1, Part 2 (8): *"where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a ~~tailor-made~~ product with digital elements, free of charge”*

+ Recital (64): *Manufacturers should make their products with digital elements available on the market with a secure by default configuration ~~and provide security updates to users free of charge~~. (...).*

Argumentation:

1. Security remediation should not force a choice between free support across historical versions or free baseline upgrades

A mandatory free-update obligation creates a difficult practical problem for manufacturers of complex B2B products.

When a vulnerability affects an older version, the manufacturer may face two unattractive options:

- develop, test, and maintain a separate security fix for that older version; or

- provide a free path to a newer supported version or baseline that may include broader maintenance, cumulative fixes, architectural changes, compatibility updates, or functional value.

Either path can disrupt negotiated B2B support models. Maintaining security fixes for older versions requires separate engineering, regression testing, validation, and release management. It can fragment scarce cybersecurity expertise and delay remediation. Maintaining dozens or hundreds of historical baselines can actually reduce security quality. But providing a free move to a newer baseline may effectively require the manufacturer to provide broader upgrade value outside the negotiated support arrangement.

This is particularly challenging for enterprise products where baseline movement may involve:

- compatibility testing
- upgrade planning
- customer-specific validation
- regulated change windows
- software stack dependencies
- hardware or firmware compatibility
- operational support
- paid maintenance or support entitlements (including feature and function upgrades)

These can be highly integrated, and in the B2B context, may not be realistically separable. The better cybersecurity outcome is often achieved by moving customers to hardened, supportable baselines. But in sophisticated B2B environments, the commercial terms for that movement - including whether it is included in support, separately licensed, or part of a broader maintenance arrangement - should be subject to contract.

In a nutshell: The CRA should not force manufacturers either to maintain security fixes across numerous historical versions or to provide broader baseline upgrades for free. In B2B environments, sophisticated customers and manufacturers should be able to contractually define how security remediation, supported baselines, upgrade paths, and maintenance obligations are handled.

2. Security remediation often requires broader maintenance, not isolated patching

In complex enterprise products, security remediation often cannot be cleanly separated from functional maintenance. Vulnerabilities may arise from architectural assumptions, performance optimizations, concurrency models, API behavior, cryptographic integrations, or hardware/software interactions.

As a result, fixing a security vulnerability may require:

- refactoring functional code

- modifying APIs or interfaces
- updating cryptographic libraries
- changing data-handling logic
- revising firmware or hardware/software interactions
- moving customers to a later maintenance baseline

Existing guidance that allows security updates to be combined with functional updates where separation is not technically feasible is helpful. But that nuance does not solve the B2B commercial problem. If the combined update must be provided for free, the manufacturer may still be required to provide broader functional maintenance, cumulative releases, or architectural improvements outside the negotiated support arrangement.

The issue is therefore not merely whether security and functional updates can be technically separated. The issue is that when they cannot be separated, the mandatory free-update rule may require broader maintenance or functional value to be provided outside the negotiated B2B support arrangement.

In a nutshell: A “free security update” requirement can become, in practice, a requirement to provide functional maintenance for free. That is particularly problematic in B2B environments where support, maintenance, baseline movement, and lifecycle obligations are negotiated and priced as part of the customer relationship.

3. Mandatory free updates disrupt negotiated enterprise support models

A mandatory requirement to provide security updates free of charge risks separating one element of a broader support package from the commercial arrangement that funds and governs that package.

In enterprise environments, support arrangements often include more than the update artifact itself. They may include:

- vulnerability analysis
- compatibility review
- deployment planning
- upgrade assistance
- validation support
- rollback planning
- customer-specific troubleshooting
- operational support
- accountability for patch decisions

Requiring the security-update element to be provided for free may interfere with negotiated commercial models that price support based on complexity, duration, deployment environment, and risk profile.

In a nutshell: In B2B markets, security updates are often part of an integrated support and maintenance relationship. A mandatory free-update rule risks unbundling that

relationship in a way that does not reflect how enterprise customers and manufacturers allocate responsibility in practice.

4. Negotiated support is a transparent way to fund cybersecurity investment

Cybersecurity investment in enterprise products is long-term, specialized, and resource-intensive. It includes:

- vulnerability response teams
- secure development processes
- cryptographic expertise
- supply-chain analysis
- software composition analysis
- code auditing
- hardware and firmware assurance
- testing infrastructure
- long-term product maintenance

Paid enterprise support contracts provide a transparent mechanism to fund this work. They allow customers to select a level of support appropriate to their risk profile and allow manufacturers to maintain the teams and infrastructure required to deliver secure products over time.

If security updates must be provided for free outside negotiated B2B support arrangements, the costs do not disappear. They are shifted elsewhere, including into upfront product pricing, cross-subsidized across customers, or absorbed in ways that may reduce future cybersecurity investment.

Sophisticated customers may prefer to pay for defined security-update and support commitments rather than absorb uncertain costs through higher upfront prices or one-size-fits-all bundles.

In an nutshell: Cybersecurity investment must be funded sustainably. In B2B markets, negotiated support contracts are a transparent and efficient way to fund long-term vulnerability response and security maintenance.

5. The rule should not favor cloud or subscription models over other B2B deployment models

The practical burden of a mandatory free-update rule is not evenly distributed across product and business models.

Cloud and subscription models often already embed support and security updates into recurring fees. By contrast, perpetual, on-premises, infrastructure, embedded, industrial, sovereign, and hybrid products frequently use separate support and maintenance arrangements.

Those products may involve:

- customer-controlled deployment
- long validation cycles
- regulated change windows
- hardware/software integration
- customer-specific configurations
- third-party operational dependencies

A mandatory free-update rule may therefore unintentionally favor cloud-native or subscription-based models over other deployment models that sophisticated enterprise and public-sector customers deliberately choose.

This is particularly important where customers select non-cloud or non-subscription models for legitimate reasons, including operational resilience, sovereignty, performance, latency, regulatory control, or internal risk-management requirements.

In a nutshell: The CRA should remain neutral across business models. It should not unintentionally favor cloud or subscription models over perpetual, on-premises, infrastructure, embedded, or sovereign deployment models used by enterprise and public-sector customers.

6. Mandatory free updates may distort B2B support and maintenance aftermarkets

A mandatory free-security-update rule may also distort competition in support and maintenance aftermarkets.

If security maintenance must be bundled into the initial product transaction, customers may have fewer meaningful choices among:

- manufacturer support
- third-party maintenance providers
- certified integrators
- customer-managed support models
- specialized remediation providers

This is not only a vendor concern. It is also a customer-choice concern. Enterprise customers often want flexibility to decide who supports their systems, what level of service they require, and how cybersecurity obligations are allocated.

In a nutshell: A mandatory free-update rule may unintentionally reduce competition in B2B support and maintenance markets by forcing security maintenance into the original product transaction rather than allowing customers to choose among support models.

7. Regulation should reward proactive security work, not penalize it

Well-designed cybersecurity regulation should encourage early vulnerability discovery, responsible disclosure, and timely remediation.

However, if every newly discovered vulnerability creates either an unfunded obligation to patch older versions or an obligation to provide free baseline upgrades, manufacturers may face incentives to:

- reduce proactive vulnerability research
- narrow the scope of internal testing
- reduce the number of supported product configurations
- shorten lifecycle commitments where legally permissible

In a nutshell: Regulation should reward early discovery and remediation, not create economic penalties for identifying more vulnerabilities. A B2B exception would help preserve incentives for proactive cybersecurity investment and disclosure.

8. A clear B2B exception would reduce uncertainty and focus resources on security

Without a B2B exception, manufacturers and customers must draw difficult lines around:

- what counts as a “security update”
- what counts as a “functional update”
- whether an update must be separated
- when a baseline upgrade must be free
- whether support services can remain chargeable
- how historical versions must be maintained

This uncertainty does not necessarily improve cybersecurity outcomes. It may instead divert resources from targeted security work toward compliance classification, documentation, and dispute management.

In a nutshell: A clear B2B exception would reduce uncertainty and allow manufacturers and customers to focus resources on effective vulnerability handling rather than on artificial distinctions between security updates, functionality updates, baseline upgrades, and support services.