

W H I T E P A P E R

Cybersecurity Regulation Beyond the EU

How Switzerland and the United Kingdom Navigate the EU Cyber Resilience Act

May 2026

Regulatory Affairs & Technology Compliance

About This Paper

This white paper examines how Switzerland and the United Kingdom are responding to the EU's Cyber Resilience Act (Regulation EU 2024/2847, or CRA), which entered into force on 10 December 2024 and applies in full from 11 December 2027. Neither country is an EU member state, yet both face significant regulatory pressure — through trade dependencies, market-access requirements, and their own domestic digital security reform agendas. This paper considers the practical implications for manufacturers and software developers, the state of domestic cybersecurity product legislation in each jurisdiction, and the degree to which that legislation converges with or diverges from the CRA.

Executive Summary

The EU's Cyber Resilience Act (CRA) is the first horizontal cybersecurity regulation to apply across all product categories in the European single market. “Horizontal” means the CRA cuts across every sector simultaneously — it is not limited to medical devices or financial software, but applies to any product with a digital element regardless of industry. This contrasts with sectoral compliance, the previous model, where cybersecurity obligations existed only in specific regulated industries. Outside those sectors, manufacturers could largely self-regulate. The CRA ends that distinction by making cybersecurity a universal market-access requirement: meaning compliance is a prerequisite for selling in the EU at all, applied before products enter the market rather than as a penalty regime after the fact. By establishing these mandatory security requirements for all products with digital elements, the EU has set a standard that reaches well beyond its borders. Any manufacturer or software developer wishing to sell a product with digital elements in the EU must comply, regardless of where they are headquartered.

Switzerland and the United Kingdom sit in instructively different positions relative to the CRA. Switzerland has virtually no domestic product-specific cybersecurity legislation and is only now beginning to draft it. The UK enacted its own consumer connectable-device security regime (the PSTI Act) in April 2024 and is advancing a broader Cyber Security and Resilience Bill — but neither instrument is equivalent in scope or depth to the CRA, and their mutual recognition is not guaranteed. A note on terminology used throughout: the CRA’s formal scope is “products with digital elements” (PDEs) — any software or hardware with a direct or indirect data connection to a device or network. “Consumer connectable devices” is the narrower UK PSTI term: devices capable of connecting to the internet or a local network intended for consumer use. When this paper uses “connectable devices” it means the PSTI scope; when it uses “products with digital elements” or “PDEs” it means the wider CRA scope.

The central finding of this paper is that the CRA is establishing itself as the de facto standard for digital product security for any company seeking EU market access. The US and China are not legally bound by the CRA, and neither has adopted equivalent horizontal product cybersecurity legislation. The competitiveness question is real: unlike the AI Act — which has drawn fierce criticism as an innovation tax that disadvantages European companies — the CRA is a market-access rule that applies equally to all companies selling into the EU, whether European or foreign. A Chinese or US manufacturer that wants to sell connected products in the EU must comply with the CRA just as a German or Swiss one does. The compliance burden falls on all players seeking EU market access equally; it does not structurally favour EU incumbents. Swiss and UK businesses exporting to the EU must comply with the CRA as a condition of that access. Domestically, both countries are reforming their cyber legislation with explicit reference to the CRA — but neither is currently moving as fast or as comprehensively as the EU.

Key Findings

- The CRA applies to all manufacturers, importers, and distributors of products with digital elements placed on the EU market, irrespective of where those companies are based.

Swiss and UK firms are in scope from December 2027 for most obligations, and from September 2026 for vulnerability and incident reporting.

- Switzerland currently has almost no domestic product cybersecurity legislation. The Federal Council mandated its first draft bill in August 2025, with a consultation draft expected by fall 2026. The new legislation is explicitly designed with the CRA as its reference point.
- Switzerland does have a mandatory critical-infrastructure incident reporting obligation (under the revised Information Security Act) that came into force in April 2025, providing a partial parallel to CRA's reporting regime — but it applies to operators of infrastructure, not product manufacturers.
- The UK's PSTI Act covers consumer connectable devices and is narrower in scope than the CRA. It shares some requirements — default password bans, vulnerability disclosure, defined update periods — but lacks the CRA's breadth, SBOM requirements, CE marking, and lifecycle security obligations for software products. (“From December 2027” means obligations apply to products placed on the EU market from that date onwards; products already on the market before that date are not retroactively captured.)
- The UK's Cyber Security and Resilience Bill, introduced in November 2025, addresses critical infrastructure and managed service providers but is not a product security law. It does not replicate the CRA's manufacturer obligations.
- For Swiss and UK businesses selling into the EU, CRA compliance does not automatically satisfy domestic Swiss or UK law, and vice versa. The two frameworks overlap substantially but are not interchangeable — each requires separate compliance steps, as analysed in Section 5.3.

1. The CRA: What It Requires and Why It Matters Beyond the EU

Regulation (EU) 2024/2847 — the Cyber Resilience Act — was adopted by the European Council on 23 October 2024, published in the Official Journal on 20 November 2024, and entered into force on 10 December 2024. It is the first EU regulation to establish horizontal, cross-sector cybersecurity requirements for all products with digital elements (PDEs). “Horizontal” in EU legislative terminology means the regulation cuts across all industries simultaneously rather than being confined to one sector. Before the CRA, product cybersecurity obligations existed only in fragmented sector-specific rules; the CRA replaces that patchwork with a single instrument covering the entire EU market. It applies to hardware, software, and remote data processing solutions. The formal CRA definition of a “product with digital elements” (PDE) is any software or hardware product, including its remote data processing solutions and components, that has a direct or indirect data connection to a device or network. A smartphone, enterprise firewall, operating system, connected sensor, and password manager are all PDEs. Pure SaaS (software delivered entirely through the cloud with no downloadable component) is generally excluded, but any software with a downloadable or installable element — browser extensions, mobile apps, SDK libraries — falls within scope. The scope therefore covers everything from consumer smart home sensors and industrial control systems to standalone software applications. Full compliance is required from 11 December 2027, with earlier obligations on vulnerability reporting taking effect from 11 September 2026.

The CRA's essential requirements are grouped into two categories in Annex I. The first covers product security: products must be designed and developed securely, delivered free of known exploitable vulnerabilities, secured by default, built with attack surface minimisation, and capable of receiving security updates. The second covers vulnerability handling: manufacturers must operate coordinated vulnerability disclosure policies, maintain a Software Bill of Materials (SBOM), provide security updates free of charge for the declared support period, and report actively exploited vulnerabilities within strict timelines — 24 hours for early warning, 72 hours for full notification, 14 days for a final report. These three obligations are distinct in nature. “Delivered free of known exploitable vulnerabilities” is a design-time obligation: the product must be assessed before release and known flaws remediated. “SBOM (Software Bill of Materials)” is a transparency obligation: a machine-readable inventory of every software component in the product — every library, module, and dependency — so that when a new vulnerability is found in an upstream component, affected products can be rapidly identified and patched. “Provide security updates free of charge” is a post-market obligation: once a vulnerability is discovered during the declared support period, the manufacturer must issue a patch at no cost to users. On ENISA: ENISA (the European Union Agency for Cybersecurity, based in Athens) operates the CRA's single reporting platform. Reports go simultaneously to ENISA and to the national CSIRT (Computer Security Incident Response Team) of the relevant member state — in Germany, for instance, that is the BSI (Bundesamt für Sicherheit in der Informationstechnik). For a Swiss or UK manufacturer with no EU establishment, the relevant national CSIRT is that of the member state designated

by their authorised representative. Reporting is therefore both EU-level and national simultaneously — not one or the other.

Products are classified into three categories carrying different conformity assessment requirements. Standard products (the vast majority) may self-certify against harmonised standards. Important products — a defined list including browsers, VPNs, operating systems, and network management software — are split into Class I (self-assessment against standards) and Class II (mandatory third-party assessment). Critical products, including smartcard chips and hardware security modules used in sensitive infrastructure, require third-party assessment and certification under the EU's Common Criteria scheme. “Sensitive infrastructure” here refers to systems where compromise would have cascading national-scale consequences — national security, critical public services, financial market infrastructure, or large-scale data processing. The formal list of Critical PDE categories (Annex III of the CRA) includes hardware security modules, smart cards and secure elements, hardware for trusted execution environments, microprocessors with security-relevant features, and smartcard-based readers.

WHY NON-EU COMPANIES ARE DIRECTLY IN SCOPE

The CRA defines its scope by where a product is placed on the EU market — not where its manufacturer is established. A Swiss embedded-systems firm selling industrial controllers to a German integrator, or a UK software house distributing to enterprise customers in France via an online marketplace, is subject to the same obligations as an EU-based company. The regulation explicitly states that manufacturers outside the EU must appoint an authorised representative established within the EU.

CE marking under the CRA signals conformity and becomes a market-access requirement from December 2027. Products that do not bear the CE marking and carry the required technical documentation — including a declaration of conformity and an SBOM — cannot lawfully be placed on the EU market from that date. This is not a voluntary framework. It is a binding entry requirement for the world's largest single market.

Regulatory Intersections: CRA, RED, and PSTI Compared

Requirement / Concept	EU CRA	EU RED (Delegated Act)	UK PSTI
Scope	All PDEs — hardware, software, remote processing	Wireless/radio consumer devices only	Consumer connectable devices (wired + wireless)
Default password ban	Yes	Yes	Yes
Vulnerability disclosure	Mandatory CVD policy	Mandatory	Mandatory
Security update period	Mandatory (declared support period)	Yes	Mandatory (declared minimum period)
SBOM required	Yes	No	No
CE marking	Yes (from Dec 2027)	Yes (from Aug 2025)	No — UKCA marking instead
Third-party assessment	For Important/Critical PDEs	No	No
Incident reporting	ENISA + national CSIRT	No	No (voluntary NCSC schemes only)
Underlying tech standard	CRA Annex I / EN harmonised standards	ETSI EN 303 645 / EN 18031	ETSI EN 303 645
Superseded by CRA?	N/A — this is the CRA	Yes — from Dec 2027	No — independent UK law

The CRA sits alongside, and in some cases intersects with, other EU digital legislation including NIS2, the AI Act, the Data Act, and the Radio Equipment Directive (RED) Delegated Act. The RED is the EU's regulatory framework for wireless (radio) equipment. Its cybersecurity Delegated Act mandated security requirements for wireless consumer products from 1 August 2025 — requiring protection against network abuse, data privacy safeguards, and anti-fraud measures for Wi-Fi, Bluetooth, and cellular devices. The RED Delegated Act is the immediate EU-level predecessor to the CRA for wireless products and is closely related to PSTI in scope: both RED (for EU wireless products) and PSTI (for UK connectable products) share the same underlying technical standard, ETSI EN 303 645, as their primary reference. Think of them as parallel regional implementations of the same baseline: RED in the EU, PSTI in the UK, both for wireless/connectable consumer hardware. The CRA goes substantially further than both — extending to all PDEs, not just wireless hardware, and adding SBOM requirements, CE marking, third-party assessment, and full lifecycle obligations. The RED Delegated Act is expected to be repealed and superseded by the CRA from December 2027. For Swiss and UK companies, the CRA is only one layer of an increasingly dense EU digital-regulatory landscape. The compliance burden is real and, for smaller manufacturers in particular, potentially significant.

2. Switzerland: A Regulatory Gap and an Emerging Response

2.1 The Export Compliance Obligation

Switzerland is not a member of the EU or the EEA. EU regulations do not apply in Switzerland as a matter of domestic law, and the CRA is no exception. However, this distinction offers Swiss digital product manufacturers limited practical protection. Any company placing products with digital elements on the EU market — through direct sales, distributors, online marketplaces, or resellers — is subject to the CRA from December 2027, and to vulnerability reporting obligations from September 2026.

Switzerland's tech and industrial sectors are deeply integrated with EU supply chains. Precision engineering, medtech, industrial automation, and enterprise software are all areas where Swiss firms have material EU market exposure. For companies in these sectors, CRA compliance is not a future concern — it is an immediate programme of work. The conformity assessment infrastructure, SBOM tooling, vulnerability disclosure processes, and EU-authorised representative arrangements all need to be in place well before the December 2027 deadline.

Legal commentators have noted that awareness of the CRA among Swiss manufacturers remains uneven. Unlike the GDPR — which generated significant Swiss corporate attention because of its direct relevance to data handling by Swiss companies — the CRA's product-security focus means it has, until recently, registered primarily as a concern for technical teams rather than legal and compliance functions. This is changing, but speed matters: the September 2026 reporting obligations arrive within months.

THE AUTHORISED REPRESENTATIVE REQUIREMENT

Article 22 of the CRA requires manufacturers established outside the EU to appoint, by written mandate, an authorised representative established within the Union. This representative is legally responsible for ensuring the manufacturer's compliance documentation is in order and serves as the point of contact for EU market surveillance authorities. Swiss companies without a subsidiary or affiliated entity in the EU will need to establish or contract this representation before their products are placed on the EU market.

2.2 Swiss Domestic Legislation: A Late Start

Switzerland's domestic framework for product-specific cybersecurity is, as of May 2026, largely absent. The country's general information security and cybersecurity legislation — including the Federal Act on Information Security (ISG) and the revised ordinances underpinning it — focuses primarily on the security of critical infrastructure and federal IT systems, not on the cybersecurity properties of products placed on the market. Critical infrastructure in this context means the sectors whose disruption would have severe consequences for society or the economy: energy networks (electricity, gas, oil), water supply and wastewater, transport (rail, road, air, ports), financial services and payment infrastructure, health systems, and federal and cantonal government IT. The ISG obliges

operators in these sectors to implement information security measures and report significant incidents, but it does not regulate what cybersecurity properties a product must have before it is sold.

The one significant recent development is the mandatory incident reporting obligation for critical infrastructure operators, which came into force on 1 April 2025 under the revised Information Security Act. This requires operators of critical infrastructure — energy, transport, finance, health — to report cyberattacks to the National Cyber Security Centre (NCSC) within 24 hours of detection. In this narrow respect, Switzerland has developed a parallel to one element of the CRA's reporting obligations. But the obligation falls on infrastructure operators, not product manufacturers, and covers incidents affecting Swiss systems rather than vulnerabilities in exported products.

The Federal Council took its first concrete step toward product-specific cybersecurity legislation on 20 August 2025, when it mandated the Federal Department of Defence, Civil Protection and Sport (DDPS), in collaboration with the Federal Department of the Environment, Transport, Energy and Communications (DETEC) and the State Secretariat for Economic Affairs (SECO), to prepare a draft bill for consultation. The draft is expected to be submitted by fall 2026. The Council's stated objective is that the new legislation will set out cybersecurity requirements for the development and commercialisation of products with digital components, establish rules for market surveillance, and lay the groundwork for restricting the import and sale of insecure devices.

Alignment with the CRA

The Federal Council has explicitly acknowledged the CRA as the key reference for the forthcoming Swiss bill. The ambition is a framework that is compatible with EU standards and reduces dual-compliance burdens for Swiss exporters while establishing a credible domestic baseline. However, several points of likely divergence are already apparent from the political context surrounding the bill's mandate.

- Switzerland is unlikely to replicate the CRA's full conformity assessment architecture immediately. The EU system depends on a network of notified bodies, harmonised standards developed by CEN/CENELEC/ETSI, and the EUCC Common Criteria certification scheme. Building an equivalent Swiss infrastructure from scratch would take years. The more probable outcome is mutual recognition of EU assessments for Swiss market purposes, at least in the transitional period.
- The bill is expected to focus initially on the most clearly harmful products — insecure IoT devices, network equipment with hardcoded credentials — rather than attempting to replicate the CRA's full product taxonomy from the outset.
- The bill's mandate specifically references the need to avoid creating new barriers to the Swiss internal market, suggesting a preference for EU-adjacent rather than fully EU-equivalent standards, consistent with Switzerland's general approach to regulatory alignment.

The net result is that Swiss digital product manufacturers face a near-term period of compliance asymmetry: full CRA obligations for EU-market products, almost no equivalent domestic obligation, and a domestic framework that is at an early drafting stage. The business case for designing to CRA standards universally — rather than maintaining separate EU and

Swiss compliance paths — is compelling, particularly for manufacturers whose product lines are not easily differentiated by geography.

3. The United Kingdom: A Head Start with Important Gaps

3.1 The PSTI Act: A Narrower Parallel

The UK's Product Security and Telecommunications Infrastructure Act 2022 and the accompanying Security Requirements Regulations 2023 (together, 'PSTI') came into force on 29 April 2024 — approximately seven months before the CRA entered into force. In one narrow sense, the UK moved faster: it had binding consumer-device security law on the books before the EU. But context matters. The UK developed PSTI independently after Brexit, drawing on work that predated its EU departure — it did not start from a blank page. The EU, by contrast, was building a horizontal cross-sector regulation covering the entire single market of 27 member states, a structurally more complex legislative task. The UK's pre-existing experience with the Radio Equipment Directive (RED) when it was still in the EU also informed PSTI's design; the same ETSI EN 303 645 standard underlies both. So the chronological head start reflects different scope and institutional starting points as much as speed. PSTI imposes three core requirements on manufacturers, importers, and distributors of consumer connectable products: a ban on universal default passwords (each device must have a unique password or prompt the user to set one); a publicly accessible vulnerability disclosure policy; and a defined and published minimum security update period.

The conceptual overlap between PSTI and the CRA is real. Both prohibit default credentials, both mandate vulnerability disclosure processes, and both require manufacturers to communicate security update timelines to users. For companies already compliant with PSTI, these overlapping obligations represent a foundation rather than a starting point for CRA compliance. However, the scope and depth of the two regimes diverge materially in ways that matter for exporters.

Where the CRA Goes Further than PSTI

- Scope. PSTI applies to consumer connectable products — devices capable of connecting to the internet or a local network, intended for consumer use. The CRA covers all products with digital elements, including software products, enterprise hardware, and industrial systems. A network management application, an enterprise firewall, or a software-defined radio product would fall under the CRA but not PSTI in its current form.
- SBOM requirement. The CRA mandates a Software Bill of Materials (SBOM) for every in-scope product. An SBOM is a machine-readable, structured inventory of every software component in a product — every open-source library, third-party module, in-house component, and dependency — together with version numbers and known vulnerability status. It is the software equivalent of an ingredient list on a food product. When a new vulnerability is discovered in a widely-used library (a Log4Shell-type event), an SBOM allows a manufacturer or regulator to instantly identify which products are affected. PSTI has no equivalent requirement. SBOM production is a significant operational undertaking for manufacturers with complex software supply chains — many of whom have never systematically mapped their own component dependencies — and represents one of the more substantive gaps between the two regimes.
- CE marking and technical documentation. CRA-compliant products must bear the CE marking and be accompanied by a formal declaration of conformity and a comprehensive

technical file. PSTI requires a statement of compliance but does not involve CE marking or the same documentation architecture.

- Third-party conformity assessment. The CRA requires mandatory third-party assessment for Important (Class II) and Critical products. PSTI has no equivalent third-party assessment pathway.
- Incident reporting. From September 2026, CRA manufacturers must report actively exploited vulnerabilities to ENISA. PSTI does not contain equivalent mandatory incident reporting obligations for manufacturers, though the UK NCSC operates voluntary reporting schemes.

The penalty structures differ too. PSTI penalties can reach £10 million or 4% of global turnover, whichever is higher — actually more severe on the turnover metric than the CRA's ceiling of €15 million or 2.5% of global turnover. But penalty severity is less important for compliance planning than the breadth and specificity of the obligations themselves.

NO MUTUAL RECOGNITION

The European Scrutiny Committee in the House of Commons noted explicitly that the EU has not indicated any intention to recognise UK conformity assessments under PSTI as valid for CRA compliance purposes. UK manufacturers of in-scope products cannot rely on PSTI compliance as a proxy for EU market access after December 2027. They must comply separately with the CRA's conformity assessment requirements.

3.2 The Cyber Security and Resilience Bill: A Different Instrument

The UK Cyber Security and Resilience (Network and Information Systems) Bill was introduced to Parliament on 12 November 2025 and is progressing through the House of Commons, with Royal Assent expected in late 2026. It is an important development in the UK's cyber legislative landscape — but it is not a product security law, and it should not be conflated with a CRA equivalent.

The Bill amends the UK's existing Network and Information Systems (NIS) Regulations 2018 to bring them closer in spirit to the EU's NIS2 Directive. Its primary effect is to expand the scope of regulated entities — adding managed service providers, data centres, and additional supply chain actors — and to tighten incident reporting obligations and enforcement powers. It addresses the security posture of organisations operating critical services; it does not address the cybersecurity properties of products those organisations manufacture or sell.

The Bill's introduction was partly motivated by high-profile UK cyber incidents in 2025, including attacks affecting major retailers and manufacturers, which exposed limitations in the existing NIS framework. Its focus on ransomware reporting and supply chain risk is timely. But for companies trying to understand their UK-market obligations relative to the CRA, the Bill is largely orthogonal — meaning it operates in a different dimension entirely, addressing a different set of actors (infrastructure operators) with a different set of obligations (organisational security posture), rather than overlapping with or substituting for the CRA's product-manufacturer requirements. It answers a different question: not “how secure must a product be” but “how secure must an organisation's operations be.” A software company manufacturing products for sale in the UK market faces no CRA-equivalent domestic obligation for those products under either PSTI or the Resilience Bill. Given this fragmented

landscape, a clear practical hierarchy emerges for UK businesses. If you sell or plan to sell into the EU, CRA compliance is non-negotiable and should be your primary design target — begin with SBOM generation, secure-by-design assessment, and appointing an EU authorised representative. For UK domestic sales of consumer connectable products, PSTI compliance is the current legal floor. For UK domestic sales of enterprise software, industrial hardware, or non-connectable products, there is currently no product cybersecurity legal obligation beyond general product liability law — but designing to CRA standards now avoids costly retrofitting when domestic requirements tighten. If your organisation also operates critical services (as a managed service provider, data centre, or similar), the Cyber Security and Resilience Bill adds a separate layer of organisational security obligations. Product security (CRA/PSTI) and organisational security (CS&R Bill) are distinct programmes requiring distinct governance structures, but they share common engineering foundations.

4. Comparative Overview

The table below summarises the current regulatory position across the three relevant jurisdictions (EU, Switzerland, and Great Britain) as of May 2026. Several implementing acts under the CRA remain in development, and both Switzerland and the UK are at early stages of domestic reform. The table reflects published legislation, enacted laws, and credibly anticipated positions based on draft bills and official statements.

Requirement	EU CRA	Switzerland	Great Britain
Legally binding domestically	Yes (from Dec 2027)	Draft bill, fall 2026	PSTI (limited scope)
Secure-by-design mandate	Yes — all PDEs	Not yet (bill pending)	Consumer IoT only
Vulnerability reporting to authority	ENISA (from Sep 2026)	NCSC (critical infra, Apr 2025)	NCSC (voluntary / PSTI)
Software Bill of Materials (SBOM)	Required	Not yet required	Not required
CE marking required	Yes (from Dec 2027)	Not applicable	UKCA marking (separate)
Third-party conformity assessment	For Important / Critical	Not yet established	No equivalent requirement
Lifecycle security updates	Mandatory support period	Not yet mandated	Required under PSTI
Fines / penalties	Up to €15M or 2.5% turnover	TBD (bill pending)	Up to £10M or 4% turnover

The table illustrates a landscape in which the CRA is the most comprehensive and legally certain of the three columns, and in which both Switzerland and Great Britain are catching up to its requirements from different starting points. The direction of travel — toward greater alignment with CRA-equivalent standards — is consistent across both non-EU jurisdictions, but the timelines and completeness differ considerably.

5. Practical Implications for Businesses

5.1 Swiss Manufacturers and Software Developers

Swiss companies with EU market exposure face the most immediate and concrete compliance requirement. The September 2026 vulnerability reporting obligations are already within the current planning horizon — organisations need to establish ENISA-compatible reporting processes and appoint authorised EU representatives if they have not done so. For the December 2027 deadline, the full scope of CRA obligations — secure-by-design assessment, SBOM production, CE marking, technical documentation — need to be embedded in product development processes.

For domestic-only products, there is currently no legal obligation equivalent to the CRA. However, the Federal Council's August 2025 mandate to prepare a bill, with consultation expected by fall 2026, signals that domestic product cybersecurity requirements are coming. Companies building compliance programmes now should design them to be CRA-compatible, not merely compliant with the narrower domestic bill that eventually emerges. The cost of retrofitting CRA-grade security processes to products originally designed to a lower standard is substantially higher than building them in from the outset.

5.2 UK Companies Exporting to the EU

UK businesses placing digital products on the EU market must comply fully with the CRA — PSTI compliance does not substitute, and no mutual recognition arrangement exists. The practical gap for most UK manufacturers lies in SBOM production, third-party conformity assessment for Important/Critical products, and ENISA-compatible vulnerability reporting processes. These are not trivial undertakings and require investment in tooling, process change, and potentially in legal representation within the EU.

For domestic UK sales, PSTI remains the relevant regime for consumer connectable products, with the Cyber Security and Resilience Bill adding obligations for certain infrastructure operators. The gap between what PSTI requires and what the CRA requires is significant enough that UK businesses should treat them as distinct compliance programmes rather than a single harmonised effort — though there is substantial overlap in the underlying engineering practices that satisfy both.

5.3 Does CRA Compliance Cover Domestic Law? The Key Question for Swiss and UK Businesses

The key question for any Swiss or UK business with EU market exposure is: if we comply fully with the CRA, does that cover our domestic legal obligations in Switzerland or the UK as well? The short answer is no, not entirely — but the gap is smaller than it might appear, and it runs in a predictable direction. CRA compliance means you satisfy the requirements for placing products on the EU market. It does not automatically discharge your domestic obligations in Switzerland or the UK, because those are separate legal instruments with some requirements the CRA does not address.

For Switzerland: as of May 2026, there is almost no domestic product cybersecurity law to comply with, so the question is largely theoretical for now. Once the forthcoming Swiss bill enters force (expected 2027), it will likely be less demanding than the CRA in several areas — notably conformity assessment architecture and third-party assessment requirements. A company fully CRA-compliant will, in most respects, exceed whatever the Swiss bill eventually requires, since the bill is explicitly designed as a lighter-touch alignment with the CRA. The one area where separate Swiss steps will still be required is any domestic market surveillance or registration process that the Swiss authorities establish — analogous to the EU authorised representative requirement but for the Swiss market.

For the UK: the answer is more nuanced. CRA compliance does not satisfy PSTI, and PSTI compliance does not satisfy the CRA. They are independent legal instruments. For consumer connectable products, both must be complied with separately — different statements of compliance, different vulnerability disclosure processes structured to each regime's requirements, and different notification contacts (ENISA plus national CSIRT for CRA; the Office for Product Safety and Standards for PSTI). The SBOM, CE marking, third-party conformity assessment, and authorised representative requirements under the CRA have no UK equivalents at present — so there is no domestic compliance overhead for those specific elements. But for the three PSTI obligations (default password ban, vulnerability disclosure policy, defined update period), these must be demonstrably met against the PSTI Regulations, even where your product already carries CRA-compliant equivalents.

The practical recommendation is to use CRA compliance as the engineering foundation: if your product satisfies CRA Annex I requirements, you are very likely also satisfying the technical substance of PSTI. The additional work is administrative — producing a PSTI statement of compliance, structuring your vulnerability disclosure policy to reference both ENISA and the UK authority, and ensuring your update period disclosures meet the PSTI format. This is a documentation exercise, not a product redesign. For the Swiss market, plan for a separate market surveillance registration process once the Swiss bill is enacted. Neither domestic framework requires you to undo CRA-compliant engineering; they require you to layer jurisdiction-specific administrative steps on top of it.

6. Conclusions

The EU's Cyber Resilience Act is not merely an EU regulation. Through its market-access mechanism, it functions as a de facto standard for digital product security for any company wishing to participate in the European single market — applicable regardless of where that company is headquartered. The US and China operate under no equivalent horizontal obligation; calling the CRA a “global standard” would overstate its reach. It is better understood as the entry price for the EU market — one that many companies choose to adopt universally because the economics of maintaining separate EU and non-EU product security postures rarely make sense. The experience of Switzerland and the United Kingdom illustrates this dynamic clearly.

Switzerland enters the CRA era with the weakest domestic product cybersecurity framework of any major European trading economy. Its companies face full CRA obligations for EU-market products while operating in a domestic environment that has, until August 2025, lacked even a mandate to draft equivalent legislation. The forthcoming Swiss bill — explicitly modelled on the CRA — will close this gap, but it will arrive after the CRA's own compliance deadlines and is likely to be less prescriptive in certain areas.

The United Kingdom has moved faster on consumer IoT security than Switzerland but remains behind the CRA on scope, depth, and the specific compliance architecture — SBOM requirements, third-party assessment, CE marking — that the CRA demands. The Cyber Security and Resilience Bill addresses a different dimension of cybersecurity entirely: organisational security posture for critical infrastructure operators, not product security for manufacturers. UK businesses need to manage both tracks as distinct compliance programmes.

For businesses on both sides of these regulatory borders, the practical message is consistent: the CRA sets the standard, September 2026 reporting obligations are already within the current planning horizon, and domestic legislation in both Switzerland and the UK is converging toward CRA-equivalent requirements. Building to CRA standards is the lowest-risk strategy — not because it satisfies all domestic obligations automatically, but because it minimises the engineering work required to meet them and reduces compliance to jurisdiction-specific administrative steps rather than product redesign.

References and Further Reading

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), Official Journal of the EU, 20 November 2024.

European Commission, CRA Implementation Timeline and Delegated Acts, digital-strategy.ec.europa.eu, December 2025 — ongoing.

Swiss Federal Council Press Release — Federal Council to Strengthen Cyber Resilience of Digital Products, NCSC/DETEC/SECO, 20 August 2025.

Swiss Federal Act on Information Security (ISG) — Revised Ordinance on Critical Infrastructure Incident Reporting, in force 1 April 2025.

UK Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023, in force 29 April 2024.

UK Cyber Security and Resilience (Network and Information Systems) Bill, introduced to Parliament 12 November 2025. Committee Stage completed February 2026.

UK Department for Science, Innovation and Technology, Product Security: Guidance for Businesses on PSTI Obligations and Relationship to the EU CRA, updated January 2026.

European Commission, Implementing Regulation (EU) 2025/2392 — Classification of Important and Critical Products under the CRA, 1 December 2025.

European Commission, Draft Guidance on CRA Implementation — consultation March–April 2026.

Homburger AG, EU Cyber Resilience Act's Impact on Swiss Companies, November 2024.