EU Cyber Resilience Act (CRA) for Connected Device OEMs: Compliance to Competitive Edge

Georgia Cooke, Industry Analyst

CONTENTS

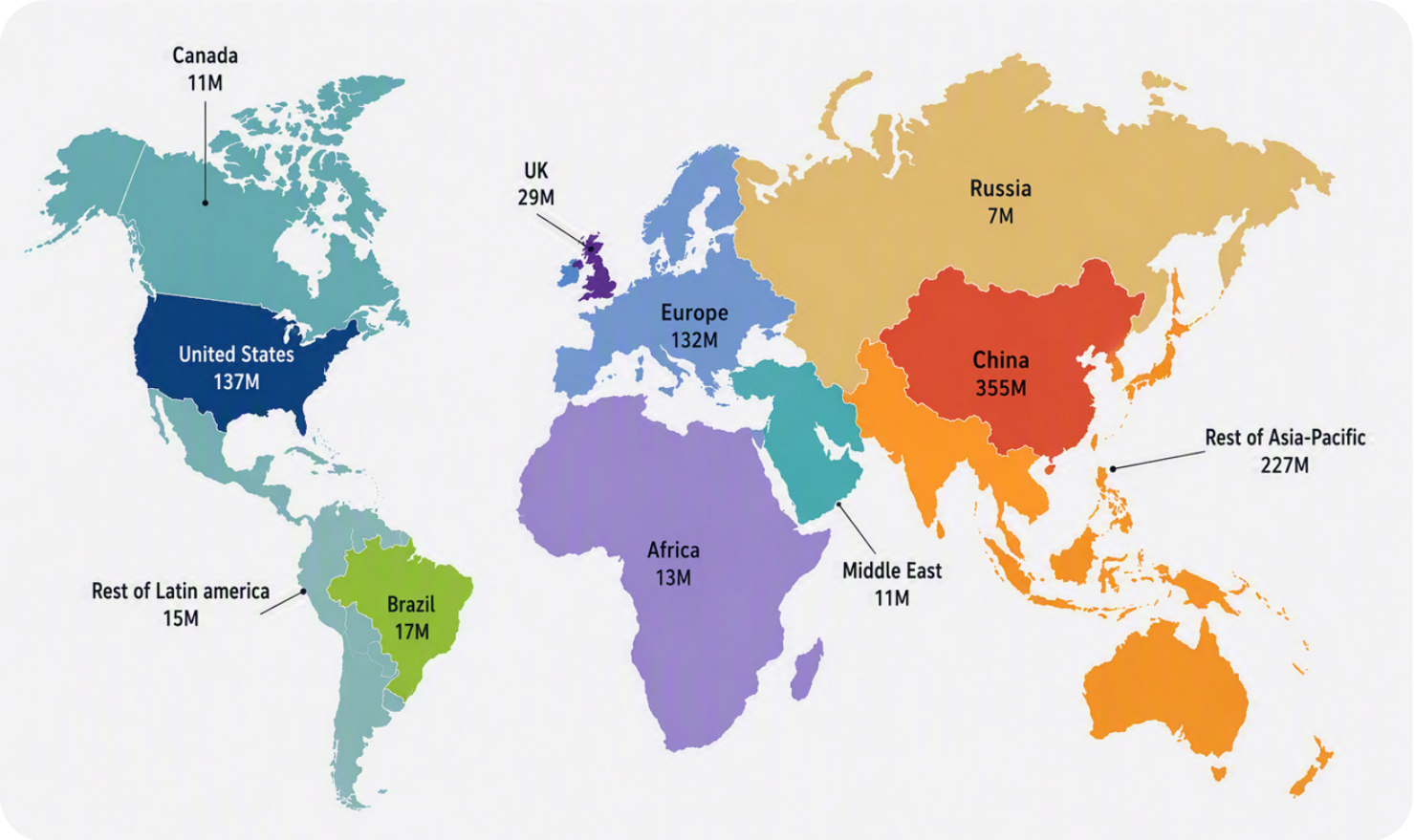
COSTS AND OPPORTUNITIES

The upcoming enforcement of the European Union's (EU) Cyber Resilience Act (CRA) and National Institute of Standards and Technology (NIST) requirements in the U.S. market poses a challenge for Internet of Things (IoT) device Original Equipment Manufacturers (OEMs). This paper explores Remote SIM Provisioning (RSP)-enabled embedded Subscriber Identity Module (eSIM) integration as a solution, outlining the importance of the affected markets, the costs and considerations to make in the compliance journey, how eSIM supports security requirements, and how this approach turns a compliance burden into an opportunity.

THE GATEWAY TO THE LARGEST MARKETS

Although today's IoT market is heavily skewed by region, with China and the rest of Asia-Pacific making up the majority of the available market for hardware shipments, there are several frontiers offering opportunities for expansion.

Chart 1: Cellular IoT Device Shipments by Region, 2027



In 2027, 23.8% of cellular IoT device shipments will be destined for end use in Asia-Pacific, outside of China. This means that the next largest market is close at hand for IoT device manufacturers currently focused on China, with some similarities in market dynamics and requirements, but with countries like India inhibiting long-term roaming, there is a requirement to either support multiple device Stock Keeping Units (SKUs) or provide full RSP in order to access the market cost efficiently.

This challenge is compounded when looking further afield—with such dominant markets at play, reaching global coverage to support the 10.8% of devices not shipped into Asia-Pacific, continental Europe, and the United States becomes infeasible with a multi-SKU approach. By adopting RSP-enabled eSIM, using the new SGP.32 standard to ensure compatibility with a broad range of device types, device OEMs can feasibly target international expansion with significantly reduced logistical complexity, and with far higher resilience to changing local regulations such as anti-roaming initiatives.

The United States and Europe are, by far, the largest single IoT markets outside of Asia-Pacific, but increasing scrutiny on security requirements, and new regulations coming into force in 2027 pose a challenge to device manufacturers. OEMs cannot afford to be locked out of such key opportunities for high sales volumes—especially as these regions typically present the highest achievable sales price per device globally.

For cellular device providers, this means that higher standards are required for detailed auditing, capacity for long-term patching, and timely reporting.

For non-cellular device makers, the question is how to provide an effective trust anchor cost efficiently, and how to effectively implement more robust Over-the-Air (OTA) update capacity. Adoption of embedded cellular capability is, for some, the most cost-effective solution.

THE PRE-CRA WORLD: ALREADY UNDER PRESSURE

Security is, and always has been, a daunting requirement. When design cycles are time-pressured, it is difficult to allocate enough time to deeply embedded security. Security practice has also been traditionally led by "castle-and-moat" approaches that rely on segmentation of high-value assets, but this retains vulnerability to advanced persistent threats that can move through the network to circumvent these protections. Moving to Zero Trust principles has improved this situation considerably, but the evolution has not progressed uniformly, with some lagging behind.

The reputational damage of a breach can be severe, and numerous IoT device makers have fallen foul of class-action lawsuits, regulatory fines, and plummeting stock prices as a result of vulnerabilities in recent years.

Consumers have noticed and so have legislators. Given the proliferation of traffic and storage of consumer data, including sensitive identity information, and the accompanying proliferation of breaches driven by increasingly sophisticated attackers, there is growing pressure on everyone involved in the production of a data-handling device to meet standards and avoid being the weak link in the security chain.

The reputational damage of a breach can be severe, and numerous IoT device makers have fallen foul of class-action lawsuits, regulatory fines, and plummeting stock prices as a result of vulnerabilities in recent years.

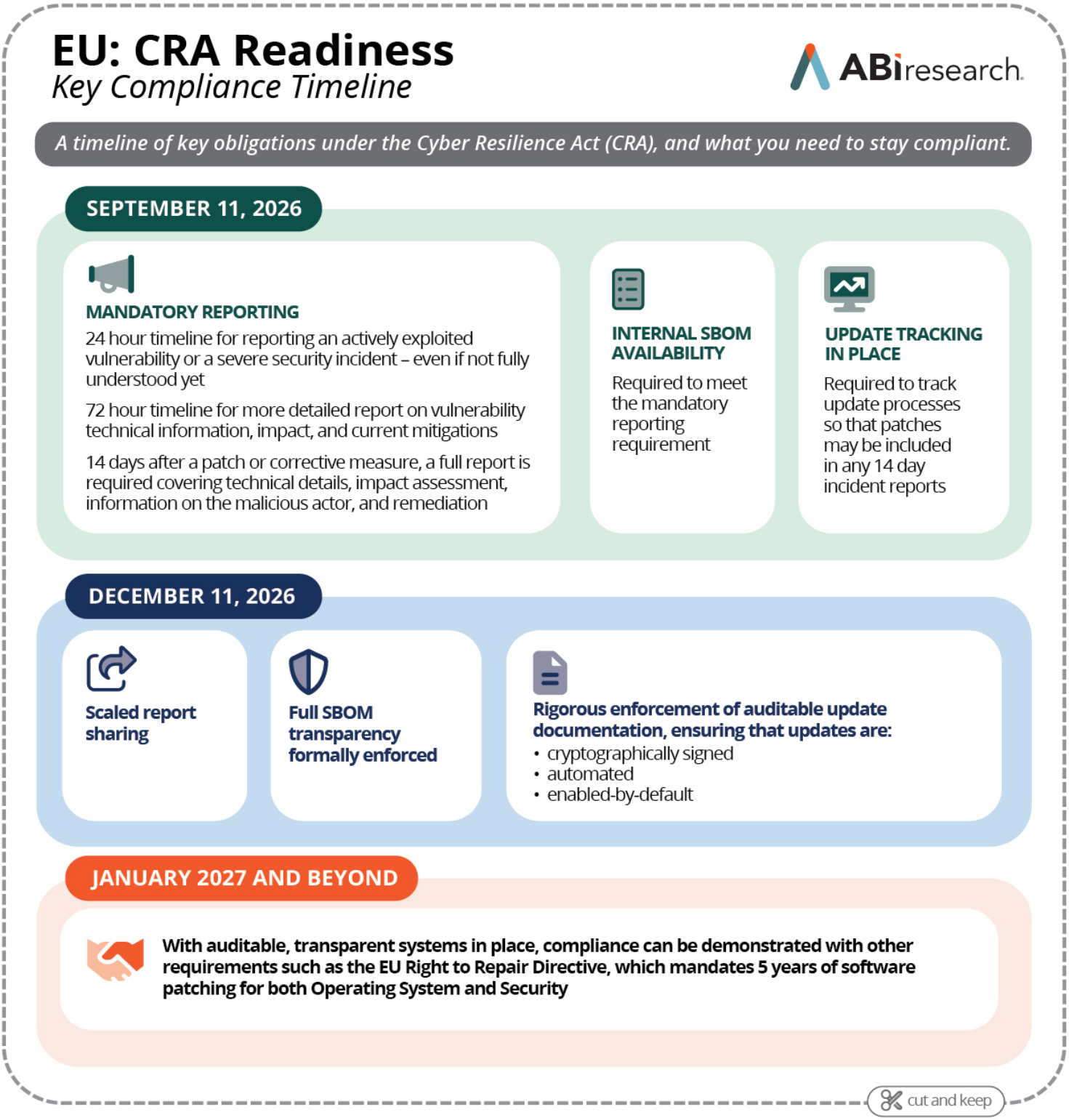
Ensuring compliance with consumer privacy legislation meant to prevent these disasters is highly regional, with the EU's General Data Protection Regulation (GDPR) rules, the United States' various Consumer Privacy Acts, which even vary by state, and China's Personal Information Protection Law (PIPL) posing their own distinct challenges.

Compliance with these regulations is essential to accessing the largest consumer markets in the world. While regulation is becoming more uniform globally, compliance is a key issue affecting ease of international trade, and the regulatory "gateway" is much stricter and more rigorously enforced than it has been in the past, and becoming stricter.

However, security is not solely a compliance issue. Particularly now, with device makers embedding Artificial Intelligence (AI) and proprietary intelligence at the edge, valuable Intellectual Property (IP) is positioned outside the walled gardens of centralized models, and financial damage from a breach is expanded to include the loss of Return on Investment (ROI) on carefully developed AI models, system designs, and processes, as well as potential liability where models or IP have been licensed and inadequately protected.

CRA & NIST: GATHERING URGENCY FOR THE FUTURE OF IoT

There is simply more to protect now, and regulators are responding accordingly. The first hurdle for device manufacturers is around visibility and transparency, with the bulk of the EU's 2024 CRA provisions coming into effect in late 2026. The accompanying graphic summarizes the key requirements.



U.S. regulation differs. NIST develops standards and best practices for security that are technically only required for federal agencies and defense applications, but broader enterprise will treat these recommendations as the "gold standard," and the frameworks are widely available and preferred for commercial applications.

USA: NIST Recommendations

Key Compliance Timeline

ABIresearch

A timeline of key recommendations from the National Institute of Standards and Technology (NIST).

SEPTEMBER 21, 2026

Sunsetting of FIPS 140-2 Legacy Cryptography for federal government or regulated industries

NOVEMBER 10, 2026

CYBERSECURITY MATURITY MODEL CERTIFICATION
In the Department of Defense Supply Chain, Level 2 Compliance will require more third-party assessments

JANUARY 1, 2027

COMMERCIAL NATIONAL SECURITY ALGORITHM SUITE 2.0
Required for National Security Systems (including suppliers), recommended for Department of Defense and Defense Industrial Base – quantum-safe OS and networking hardware using NIST PQ Algorithms, and used as a benchmark in regulated industries such as BFSI and healthcare.

2027

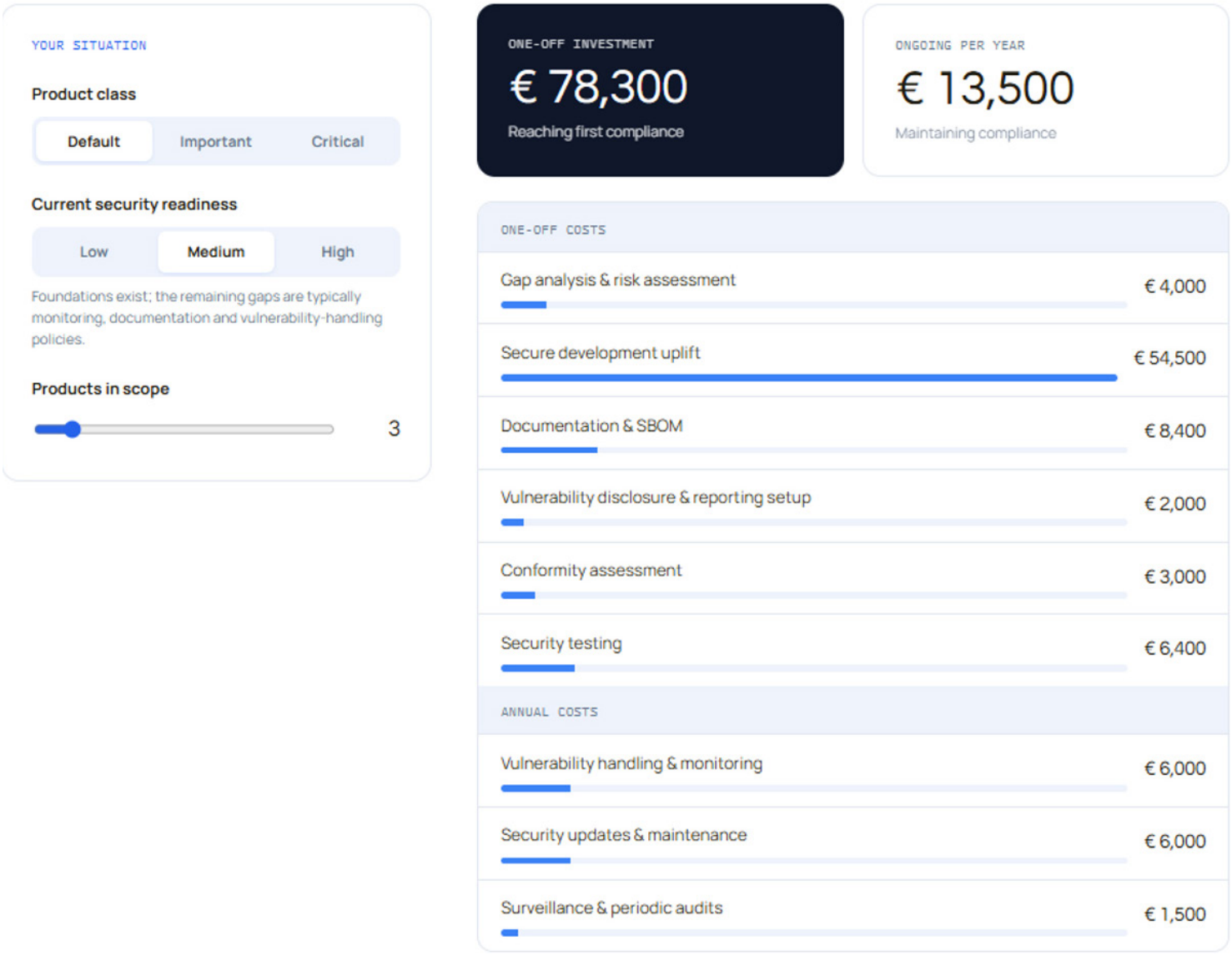
NIST FIPS 206
Use of FALCON quantum-safe algorithm for constrained devices supplied to federal agencies, defense contractors, and regulated industries

cut and keep

UNDERSTANDING THE COST OF CRA COMPLIANCE

Calculating the costs of achieving CRA compliance is a challenge. Security firm i46 provides a cost calculator currently available on The Cyber Resilience Act, giving an initial indication based on three inputs.

Figure 1: A Capture of the Unofficial Cyber Resilience Act Site Run by i46, Providing an Interactive Calculator to Support Initial Estimates

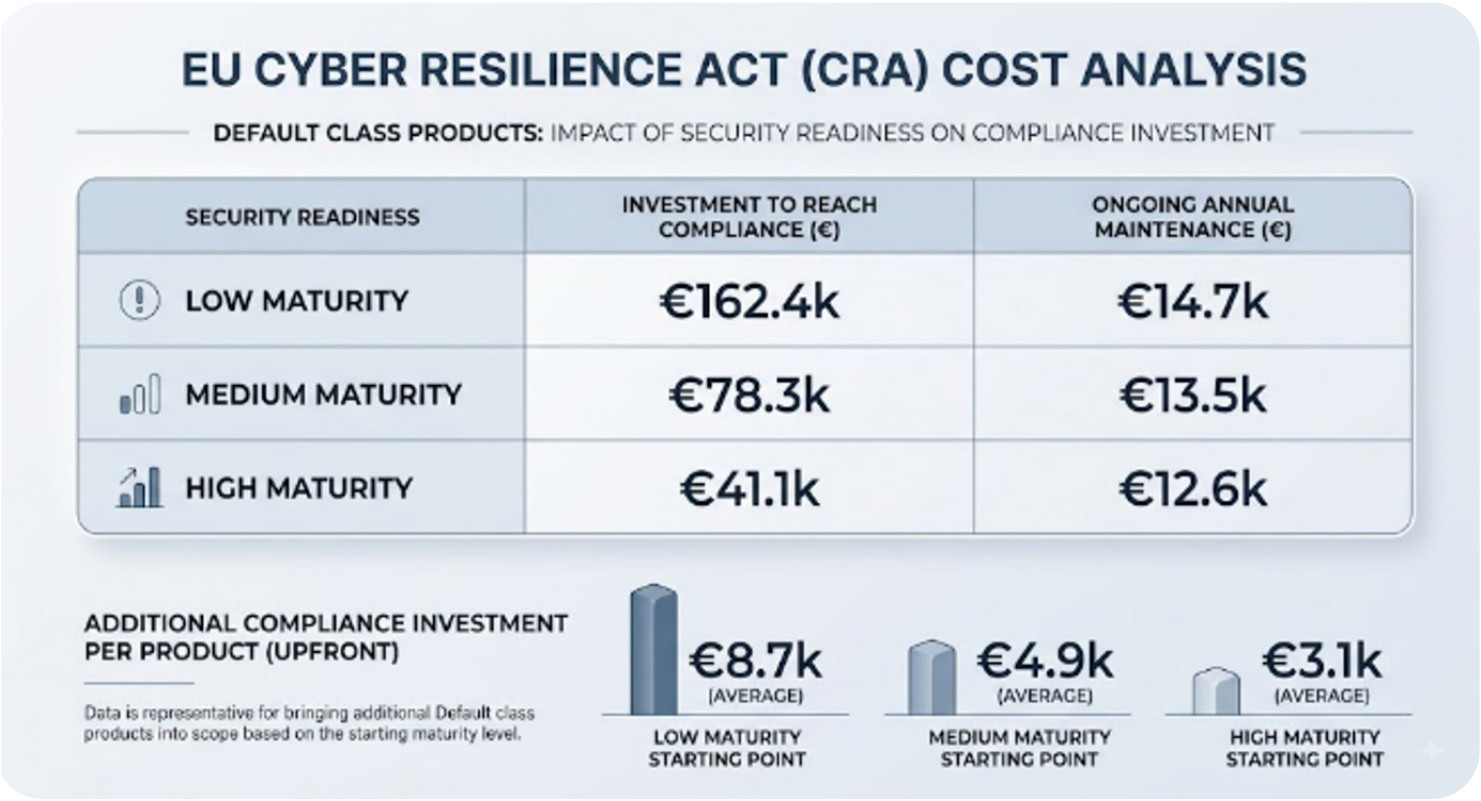


Approximating the cost of reaching compliance relies on three variables:

- **Product class** is split into Default, Important (Class I and II), and Critical, and the vast majority will fall under the default category, requiring self-assessment of compliance.

- **Current security readiness** is a broad assessment of current levels of security infrastructure, ranging from Low, with core controls not yet in place, to Medium where there may be gaps in monitoring, documentation, and vulnerability handling, to High, where security infrastructure is already mature with only official Article 14 reporting and documentation still to formalize.
- **Products in scope,** referring to the number of product designs that need to be made compliant, which includes any intended for EU distribution with a logical or physical data connection, whether direct or indirect.

Current security readiness is the most pertinent variation for most, with costs to make three default class products compliant as follows:



An approximate average of €100,000 for a reasonably mature and scaled vendor is a suitable starting point. Given the margins many IoT device manufacturers operate at, the need to minimize cost is clear, which is why the cost efficiencies of SGP.32 eSIM integration are so attractive.

This investment is an essential measure, with breach of the regulation having direct costs—associated fines are set to run to €15 million or 2.5% of total annual revenue, whichever is higher—and indirect costs in the form of damaged customer trust and, particularly in the growing Edge AI market, potential liability for failure to secure licensed IP.

LEVERAGING ESIM TO SATISFY ESSENTIAL NEW SECURITY EXPECTATIONS

eSIM technology is inherently secured and tested for the highest security assurances for physical and logical security measures, which has served it well in becoming the de facto trust anchor for all things mobile. The new eSIM standard, SGP.32, extends the ability for OEMs to maintain control to send secure profile updates across IoT-class devices. SGP.32 standardized eSIM solutions with GSMA certification allows device OEMs to establish a strong technical foundation. This is crucial for addressing various challenges in an industry pressured to enhance security. Notably, the CRA will be fully enforced by 2027, along with numerous NIST recommendations and similar global cybersecurity regulations.

While the regulation aims to protect end users, the effectiveness of it depends on if attitudes toward security from device OEMs will match. This picture is encouraging—a survey of over 800 IoT practitioners conducted by Mobile World Live in 2026, sponsored by Kigen, reported that 82% of manufacturers surveyed consider IoT security a core business enabler. This is not without reason—75% of all vendor types surveyed were confident that CRA will apply to their products and services as they address the EU market. Recent and upcoming legislation has focused heavily on full transparency and accountability throughout the supply chain, and the message is clear for OEMs: compliance is essential.

FORGING THE PATH TO PROVABLE CRA COMPLIANCE

For "critical" and "important" Business-to-Business (B2B) or Business-to-Consumer (B2C) products with digital elements, manufacturers cannot rely entirely on self-assessment. Notifying bodies independently audit the manufacturer's secure development lifecycle, review documentation, or test the product against CRA essential requirements. If the product passes, the notifying body issues an EU-type examination certificate, which the manufacturer uses to legally affix the CE mark. While the industry transitions to the new operational and conformance shift, there are coordinated efforts underway to reduce the burden of compliance that may be covered by other regulations (such as the EU's Radio Equipment Directive (RED)) and other established security assurances and certification schemes.

eSA ALIGNMENT

For the cellular IoT world, the GSMA's eUICC Security Assurance (eSA) security certification scheme could act as an effective blueprint for CRA compliance. The industry is calling for it to be considered an explicit pathway, but regardless of official equivalency status, there are several key reasons to treat eSA as the foundation for security strategy.

Timelines

- Upcoming legislation is approaching quickly and will soon be strictly enforced. Particularly for industries such as automotive, where design cycles are long and process changes are disruptive and time-consuming, the urgency is only mounting. Using a mature, scaled existing solution is likely to be a necessity to meet the pace required in such industries.
- Though industries with shorter design lifecycles might not be under such severe pressure, the benefits of hitting international markets with compliant solutions early confer a first-mover advantage which should not be underestimated.
- Using eSA means building security on commercially available solutions which are already poised for rapid deployment and painless fast-paced scaling.
- Within eSA testing and assurances, there is possibility for evaluation of the eSIM target hardware and OS for CRA-compliant patching applying to IoT realities such as secure transfer over non-SMS bearer, interrupted downloads and more.

Cost Efficiency

- The eSA certification scheme was officially launched in February 2021, and has had several years to develop, eliminating teething problems and unexpected, costly issues. An ecosystem has matured, providing fill solutions and benefitting from economies of scale. In contrast, novel solutions require significant investment, as well as time, to develop. Cost efficiency is a consideration for all but is particularly pressing in a growing massive IoT & constrained device market where margins can be significantly impacted by unpredictable certification pathway costs.

Universality

- GSMA's standards are influenced by a massive and broad member base, with eSA being designed to provide a general security foundation appropriate for any niche. The focus on shared expectations, interoperable verification systems, and an implementation framework which works for a broad array of vendors is perfectly aligned with the openness and generalized nature of CRA compliance.
- However, no single solution is truly 'one size fits all'. There are other means to achieve OTA functionality. For device types where ongoing cellular connectivity is prohibitively costly or difficult to assign liability for, where power is extremely constrained, or where the device will be located in a zone with no coverage, there is Firmware Over-the-Air (FOTA) over LE (Bluetooth® Low Energy). Cryptographic validation of the payload is completed to verify the security of an update, but for the small subset of using this method, there is a higher exposure to attacks due to the 'relay' involved in update delivery – in contrast to the direct server-to-device connection provided by eSIM.
- In IPAe, the 'IoT Profile Assistant in eUICC' which handles connectivity processes is hosted on the eSIM hardware, while in IPAd, the agent is hosted on the processor of the device. Kigen's suggested solution to the CRA challenge emphasizes the use of IPAe architecture, evaluated in the eSA security testing, to enable rapid deployment with a high degree of hardware agnosticism.
- Some verticals – such as automotive and heavy industry – require more control, and others – such as transport and logistics – see the benefits of direct access to other processor activities such as sensor data, enabling rapid execution of GPS or condition-based connectivity functions. For these applications IPAd might be a better fit.

KIGEN'S APPROACH

Balancing Simplicity and Flexibility

Kigen's eSA-certified solution offers a single, unified connectivity compliance strategy, providing access to international markets with a single implementation. The solution manages security across software, hardware, and enablement tools, and covers both consumer and IoT standards for RSP.

Simplicity is emphasized, with existing SGP.02 devices able to be updated for SGP.32 compliance via "plug-and-play" eSIMs available with Kigen's IoT Profile Assistant for eUICCs (IPAe). This means that future-proof devices can be equipped with robust OTA capabilities—the single most impactful compliance hurdle in the era of CRA compliance, quantum-ready crypto-agility, and long-term support for devices with growing life spans.

Having the practical connectivity requirements and local compliance demands met by a single deployment dramatically shortens the Time to Market (TTM) for any regional target, making eSA-compliant eSIM integration an essential tool for strategic international market capture.

Support for memory- and power-constrained devices provides options to cover a broad range of device types. The MFF4 form factor, measuring just 2 Millimeters (mm) x 2 mm, along with other prevalent and standardized SIM form factors, can be loaded with a profile in around 2 minutes using Kigen's In-Factory Profile Provisioning (IFPP) solution, safeguarding device battery life and integrating easily into existing manufacturing processes. Once in the field, the dynamic polling technique ensures that device check-ins are intelligently managed, eliminating power-hungry repeat-scheduled update checks. Dynamic polling also enables rapid fixes, handling problems as they arise—whether that is a device failure or an urgent security patch.

For manufacturers with the appetite and device capacity for a full-featured SGP.32 solution, making the fullest use of the ability to dynamically redeploy devices with RSP, Kigen's solution offers international compatibility with a single infrastructure deployment and a single manufacturing SKU for devices. Working with global Tier One operators and providing interoperability with around 300 operators ensures flexibility to cross borders seamlessly, instantly streamlining device shipping logistics.

Having the practical connectivity requirements and local compliance demands met by a single deployment dramatically shortens the Time to Market (TTM) for any regional target, making eSA-compliant eSIM integration an essential tool for strategic international market capture.

Adding Value: Leading the Next Wave

Kigen's prominent, active work within the GSMA—one of the most influential industry bodies in the cellular world, contributing to the technical SGP.02, SGP.22, and SGP.32 eSIM standards, and being the first to take an eSIM Operating System (OS) update solution through the eSA certification—means that its solution was developed in lockstep with

industry standards. Kigen's technical experts do not just comply with the standards—they shape them, with Kigen's Head of Standards, Dr Saïd Gharout, chairing the eSIM working group for technical specification for the GSMA and parallel IoT RSP groups in the Trusted Connectivity Alliance (TCA). The mutual influence is reflected in a solution that is tailored for key manufacturer pain points, and an acute awareness of industry-wide technical evolution.

With two clear "waves" on the horizon for device manufacturers—first the urgent integration requirements, and then the challenge of differentiation and rising above the crowd—Kigen's leadership and its position at the cutting edge of development and its deep expertise provide key advantages as a strategic partner.

Scale

Once the first wave is weathered, and new regulatory compliance enters into "ongoing maintenance" status, the problem of scaling a solution must be tackled to ensure that international footholds grow into thriving business. Kigen's solution enables flexible integration of entire fleets, including pre-SGP.32 and constrained-devices, into a single platform. Drawing the entire product line into a single point of control, with one code base, allows for visibility across an entire product portfolio. This unification is a critical first step for innovation, particularly as AI capabilities develop that can dynamically digest, analyze, and influence this single unified pool with a holistic approach. Beginning from this harmonized approach, growth can be accommodated and enabled with less friction, more clarity, and more control.

Security

Security legislation is, by necessity, pitched to a standard that is generally attainable. There is plenty of scope to go beyond the minimal baseline, and with security continually rising up customer priority lists, value-add security features offer a key differentiating factor that will underpin the largest and most valuable project proposals in the coming years.

Strategically leveraging the features of a high quality, secure-by-design eSIM solution empowers device OEMs to position themselves ahead of competition in international markets, providing a solution that provides long-term peace of mind and cements a role as more than simply a device supplier.

The task ahead for manufacturers should not be viewed simply as compliance—ticking off requirements—but as an opportunity. Strategically leveraging the features of a high quality, secure-by-design eSIM solution empowers device OEMs to position themselves ahead of competition in international markets, providing a solution that provides long-term peace of mind and cements a role as more than simply a device supplier.

Eliminating customer pain by taking away the burden and friction of security compliance and connectivity management elevates the role to that of a strategic partner and an essential enabler—one that provides a full, effortless solution instead of a device. In a time of deep uncertainty, and in markets prone to commoditization and impacts from sudden disruption, this repositioning goes well beyond a check-box exercise.

INDUSTRY PERSPECTIVE:
Toward a Cyber-Resilient Future at Scale with EU CRA

Vincent Korstanje, CEO, Kigen

The EU CRA changes the economics of connected products. Security is becoming part of market access, not simply a feature added after the product is designed. Product security is now the market access opportunity and is ever more closely linked to the trust consumers place in your brand. Most products will achieve compliance via CE Marking, but the toughest challenges arise in the critical class of devices that require third-party assessment. We have set out to empower manufacturers in this new security paradigm. With secure eSIM and remote SIM provisioning, it can be embedded directly into the connected product—a foundation for trust that fits on the tip of your finger.

The simple fact is: As the EU Cyber Resilience Act raises expectations for vulnerability reporting, remote updates, secure lifecycle management, and field resilience, and similar requirements emerge across China and North America, manufacturers must build products that can be secured, updated, and trusted throughout their lifetime. This unique product security requirement means that manufacturers of "products with digital elements" now have to place emphasis on security-by-design. The inclusion of eSA-certified eSIM solutions is not a silver bullet, but designing with the right architecture can provide a clearer path to compliance before products are launched.

This shift is a major boost for sectors where connected products must operate securely for years, including automotive, smart metering and grid utilities, point-of-sale terminals, e-bikes, smartwatches, smartphones, industrial IoT, and edge AI. In these markets, eSIM can help manufacturers move from connected devices to trusted global platforms.

As we continue to expand with leading brands that are advancing the global connected product ecosystem, secure eSIM is reshaping global access and driving new growth for IoT and Embedded Intelligence manufacturers in domestic and international markets. The company's growing partnerships with Chinese, European, Indian, ASEAN, and North American manufacturers reflect rising confidence in eSIM as a route to stronger interoperability, lower deployment risk, and enduring global advantage.

Most CRA obligations apply to products now in development and expected to launch in 2027, and there is no time to lose when it comes to compliance readiness. If you are in active development or planning your next product, prudent decisions today will play a part in shaping whether CRA remains a challenge or becomes an opportunity for your business. Together, let's work to build this in the era of intelligent cyber defense and resilience.

ANALYST BIO

Georgia Cooke, Industry Analyst

Georgia Cooke is an Industry Analyst within ABI Research's Digital Security team, conducting research on topics such as 5G security and RISC-V. Georgia works closely with security providers to understand the state of these markets and deliver actionable analysis.

September 2026
157 Columbus Avenue
New York, NY 10023
Tel: +1 516-624-2500
www.abiresearch.com

WE EMPOWER TECHNOLOGY INNOVATION AND STRATEGIC IMPLEMENTATION

ABI Research is uniquely positioned at the intersection of end-market companies and technology solution providers, serving as the bridge that seamlessly connects these two segments by driving successful technology implementations and delivering strategies that are proven to attract and retain customers.