

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Security in the Air: Understanding IoT Vendor Practices and the Economics of Over-the-Air Updates

Huancheng Hu and Christian Doerr, *Hasso Plattner Institute, University of Potsdam*

https://www.usenix.org/conference/usenixsecurity26/presentation/hu-huancheng

This paper is included in the Proceedings of the 35th USENIX Security Symposium.

August 12–14, 2026 • Baltimore, MD, USA

ISBN 978-1-939133-58-8

Open access to the Proceedings of the 35th USENIX Security Symposium is sponsored by



جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

ARTIFACT EVALUATED
USENIX
AVAILABLE

Security in the Air: Understanding IoT Vendor Practices and the Economics of Over-the-Air Updates

Huancheng Hu
Hasso Plattner Institute, University of Potsdam
huancheng.hu@hpi.de

Christian Doerr
Hasso Plattner Institute, University of Potsdam
christian.doerr@hpi.de

Abstract

Over-the-air (OTA) firmware updates are essential for maintaining IoT device security. However, vendors frequently reduce update frequency and discontinue support before devices reach end of life. Prior work has focused on protocol design and deployment measurements, but has not explained why vendors struggle to sustain long-term update support. Through interviews with 30 IoT vendors and a survey of over 100 practitioners, we examine OTA practices from the vendor perspective. We find that OTA failures stem from fragmented responsibility across multi-tier supply chains, economic constraints that determine support duration independent of security needs, and structural mismatches between component lifecycles and deployment periods. These organizational and economic factors create systematic barriers to security maintenance that technical solutions alone cannot address. Our findings reveal why current approaches to IoT security are insufficient and suggest policy interventions for sustainable update practices.

1 Introduction

Over-the-air (OTA) firmware updates have become a foundational requirement for modern Internet-of-Things (IoT) systems. Once an optional post-deployment feature, OTA support is now increasingly mandated by regulatory frameworks and market access requirements. Recent regulations, including the European Union Cyber Resilience Act (CRA) and delegated acts under the Radio Equipment Directive, require IoT products to provide timely security updates throughout a defined support period, with similar expectations emerging through security labeling and procurement policies in other regions.

While economic pressure on security is well understood in general [1], IoT OTA firmware updates are shaped by structural conditions absent from traditional software: fragmented multi-party supply chains, white-label firmware reuse with shared signing keys, device lifetimes that outlast upstream support, and hardware constraints that can make patching infeasible. Despite its importance, sustaining OTA firmware update services remains challenging in practice, particularly for small and medium-sized enterprises (SMEs), white-label manufacturers, and low-margin IoT vendors [17]. Unlike large companies, these actors must deliver OTA firmware updates under strict cost constraints while depending on upstream chipsets, SDKs, and cloud platforms they do not control. To manage this risk, vendors often adopt conservative or ad hoc practices that are largely invisible to users and regulators yet directly shape the long-term security posture of deployed IoT ecosystems.

Related research on IoT firmware updates and OTA mechanisms spans designs of secure or scalable update protocols, empirical measurements of update behavior and analyses of update practices. On the mechanism side, a range of research has explored integrity and scalability challenges in OTA delivery [4, 18, 26, 29, 34]. Large-scale measurement studies have shown that most deployed IoT devices run outdated firmware, revealing significant gaps between available patches and actual field deployment [6]. Complementary work characterizes IoT software update practices at scale, documenting pervasive fragmentation and inconsistent update behavior across vendors [2], and [15] analyzes the mismatch between real support periods and user or regulatory expectations. Although these works advance understanding of update deployment, vulnerability prevalence, and secure or efficient OTA mechanisms, they largely treat OTA as a technical or protocol problem and do not explicate why OTA support degrades over product lifecycles or how upstream supply-chain structure and economic constraints shape long-term update sustainability.

In this paper, we show through in-depth interviews and surveys with IoT vendors across consumer, industrial, and white-label markets that OTA failures stem not from lack of security knowledge, but from misaligned incentives and fragmented responsibility within the supply chain. Upstream dependencies on SDKs, chipset firmware, and cloud platforms create hidden costs and accountability gaps that undermine long-term update sustainability.

We structure our investigation around five research ques-

tions that examine vendor perceptions, operational practices, supply chain responsibility allocation, economic factors, and technical constraints. **RQ1:** How do IoT vendors perceive OTA's purpose, and what factors shape their attitudes toward OTA security? **RQ2:** What OTA practices are deployed, including white-label firmware sharing, third-party cloud platform usage, and resource allocation strategies? **RQ3:** How is responsibility allocated across the supply chain (chip vendors, SDK providers, cloud platforms), and how do upstream dependencies affect security maintenance? **RQ4:** What are the costs of providing OTA capability, how do vendors calculate security support duration, and what hidden costs emerge post-deployment? **RQ5:** What hardware, toolchain, and deployment environment constraints prevent vendors from maintaining reliable OTA systems over product lifetimes? We makes the following contributions:

- We present an empirical study of OTA practices based on interviews with 30 IoT vendors and a validated survey of over 100 practitioners across consumer, industrial, and white-label markets.
- We analyze OTA updates through a supply chain lens, showing how fragmented responsibility across chip vendors, SDK providers, and cloud platforms creates accountability gaps and delays incident response.
- We characterize how white-label firmware sharing and centralized signing infrastructure cause vulnerabilities to propagate across brand boundaries without public visibility.
- We identify the economic factors shaping OTA sustainability, including how vendors calculate support duration and how hidden costs emerge years after product launch.
- We document structural constraints, including toolchain expiration and hardware limitations, that render devices unpatchable independent of vendor resources or regulatory mandates.

2 Background

This section provides necessary background on OTA firmware updates in IoT systems. We first describe the technical mechanisms and constraints of OTA updates (§2.1), then characterize the supply chain actors whose interactions shape OTA delivery and maintenance in practice (§2.2).

2.1 Over-the-Air Updates in IoT Devices

OTA firmware updates are the primary mechanism by which IoT devices are modified after deployment. An OTA update allows a device to receive a new firmware image through its network interface and install it locally, without requiring physical access to the hardware. Because IoT devices are often

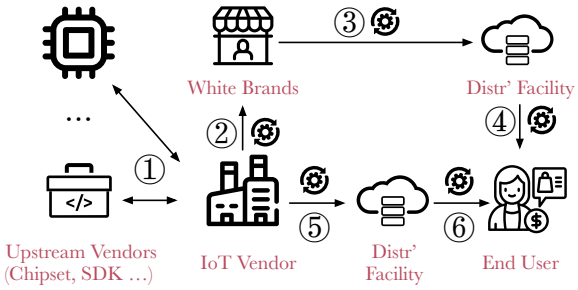


Figure 1: The OTA update supply chain in IoT ecosystems. ① IoT vendors develop OTA patches collaborating with upstream chipset and SDK providers. Two distribution paths exist: *Via resellers:* ② Patches delivered to white-label OEM resellers, ③ and ④ resellers upload to distribution facilities (cloud servers/CDN), then pushed to end users. *Direct distribution:* ⑤ IoT vendors upload patches directly to distribution facilities, ⑥ pushed to end users.

deployed at scale and in locations that are difficult or costly to access, OTA updates are widely used for bug fixes, security patching, and functional changes throughout a device's operational lifetime [19].

At a high level, an OTA update consists of three steps: distribution of an update image, verification of the received image, and installation on the device. The update image is typically retrieved from a remote server using an application-layer protocol, while verification is performed on-device using cryptographic integrity and authenticity checks. Installation replaces or activates the new firmware, often followed by a reboot. To reduce the risk of device failure, many OTA designs include rollback or recovery mechanisms that allow a device to return to a previous firmware version if installation fails [19].

OTA update mechanisms are constrained by the characteristics of embedded IoT platforms. Devices often have limited storage, memory, and power budgets, which restrict the size of update images and the complexity of update logic. Network connectivity may be intermittent or low bandwidth, further influencing update design. As a result, OTA systems frequently rely on staged deployment, compact update representations, and explicit update state tracking to ensure reliability across large device fleets [25].

Standardized architectures and protocols formalize these mechanisms. The IETF firmware update architecture defines a common model in which update metadata, firmware images, and transport are separated, allowing different network protocols to be used with the same update logic [19]. Device management protocols such as Lightweight M2M specify concrete procedures for firmware download, validation, installation, and status reporting, providing a reference implementation of OTA updates in operational IoT systems [25].

2.2 OTA Update Supply Chain and Stakeholder Roles

OTA firmware updates in IoT ecosystems span multiple independent actors that produce, integrate, and distribute update artifacts to fielded devices as shown in Figure 1. These actors exert economic and technical influence over the update pipeline, and their interactions shape the operational characteristics of OTA delivery.

Semiconductor and chipset vendors design and manufacture the hardware platforms that underlie IoT endpoints. These vendors supply silicon, reference firmware stacks, and development kits that define the baseline capabilities of devices, including cryptographic primitives and boot architectures used in update verification [12]. Device manufacturers and original equipment manufacturers (OEMs) integrate these hardware platforms with application software, construct firmware images, and define update schedules and versioning schemes. OEMs are responsible for producing and signing firmware artifacts that are suitable for their particular hardware configurations.

Cloud service providers and dedicated IoT platform vendors operate the infrastructure that hosts firmware artifacts and metadata, schedules update rollouts, and mediates communications with deployed endpoints. These platforms provide device lifecycle management features such as inventory tracking, OTA orchestration, and group targeting, supporting scalable update distribution for large device fleets [16].

In addition to OEMs and cloud platforms, software middleware and integration partners supply SDKs (Software Development Kits), update client libraries, and deployment tooling that enable OTA functionality within a product ecosystem. These middleware components abstract network protocols and repository interfaces, enabling OEMs to leverage third-party services for update distribution while retaining control over versioning and policy configuration.

3 Related Work

Prior research has extensively documented that firmware update and OTA mechanisms constitute a major attack surface in embedded and IoT systems. Large-scale firmware analyses reveal pervasive security weaknesses, including improper cryptographic use, missing authenticity checks, and flawed update logic across vendors and product categories [3, 32]. Update-specific studies further show that vulnerabilities are systematically introduced at multiple stages of the update pipeline, from package generation to installation, and that these flaws frequently lead to real-world exploits and CVEs [32]. At the same time, standards-based designs demonstrate that secure firmware updates are technically feasible even on highly resource-constrained devices, undermining claims that hardware limitations alone preclude secure OTA deployment [33].

A complementary line of work focuses on update deployment and patch latency. Measurement studies across Internet-facing services, mobile ecosystems, and IoT firmware consistently find substantial delays between patch availability and effective deployment [5, 10, 13, 22]. Collectively, this literature does not yet explain how internal constraints and incentives shape update behavior.

Software supply chain security research provides further context for understanding OTA risk. Empirical analyses and incident reports show that update channels and build pipelines are attractive targets for attackers, as demonstrated by numerous real-world compromises [28, 31]. Studies of package ecosystems reveal recurring attack patterns rooted in dependency trust, build integrity, and multi-party coordination failures [24]. While these works primarily focus on general-purpose software ecosystems, their insights directly apply to OTA pipelines that span chip vendors, SDK providers, cloud platforms, and device manufacturers.

Research in security economics establishes that misaligned incentives and externalities lead to systematic underinvestment in security [1, 7]. Recent work applies these insights to IoT, studying incentive structures and barriers from the perspectives of consumers and ISPs [23, 27], examining security economics in IoT standardization and proposing update labels as an incentive mechanism [20, 21], and surveying technical approaches for updating IoT devices [9]. These works address downstream actors, standardization, or technical mechanisms, but do not investigate how vendor-internal supply chain dependencies, white-label arrangements, and lifecycle economics shape OTA firmware update practices.

These measurement studies provide essential empirical foundations for understanding OTA security challenges. Building on their documentation of patch delays [10] and pervasive deployment of outdated firmware [3], we examine the vendor-side organizational and economic factors that cause update support to degrade over product lifecycles. Similarly, while research on SME security practices establishes that economic pressure and organizational constraints limit security investments [11, 30], we extend this line of inquiry by investigating how these pressures specifically manifest in OTA sustainability within multi-party IoT supply chains. User studies reveal important mismatches between consumer expectations for long-term support and actual vendor practices [8, 15]; we complement this work by characterizing the structural and economic barriers vendors face in meeting those expectations. Supply chain security research establishes that multi-party coordination creates vulnerabilities [24, 31], primarily examining general-purpose software ecosystems. We apply and extend these insights to IoT OTA delivery, investigating how responsibility fragmentation across the supply chain shapes long-term update sustainability from the vendor perspective.

4 Study Design

We employed a two-phase mixed-methods approach to investigate OTA firmware update practices among IoT vendors. We focus specifically on updates delivered remotely via network connectivity; other mechanisms such as USB flashing or JTAG programming are outside scope because they require physical access and do not scale to large deployed fleets. Phase 1 establishes the empirical foundation by quantifying update frequency disparities through firmware release analysis. Phase 2 then investigates why these disparities exist using complementary methods: semi-structured interviews provide rich contextual insights into vendor challenges, while a large-scale survey quantifies how widespread these patterns are across the broader vendor population.

4.1 Phase 1: Firmware Update Frequency Analysis

We collected firmware release metadata from publicly available sources to quantify how update patterns differ across vendor types and resource levels. This establishes the empirical basis for investigating vendor-side barriers in Phase 2.

4.1.1 Data Collection

We collected firmware release timestamps from vendor support websites, official firmware download repositories, and product documentation pages. For each device model, we recorded all publicly available firmware release dates, including both major and minor versions; we did not distinguish patch-level from feature releases, as vendor release-note conventions vary too widely for consistent classification. We included only publicly listed firmware; updates distributed exclusively through companion apps or gated behind device ownership were not captured, which we acknowledge as a limitation.

We focused on IoT devices with Internet connectivity and security implications: smart home devices, IP cameras, wearables, industrial sensors, and connected appliances. Smart home devices and IP cameras capture high-volume consumer endpoints with extensive white-label firmware reuse; wearables capture deeply resource-constrained hardware that stresses patching feasibility; industrial sensors capture regulated environments with the longest deployment lifetimes; connected appliances capture long-lived devices where vendor support routinely lapses before end-of-life. Together these categories span consumer through industrial IoT, capturing the range of supply chain structures relevant to our research questions. In the results, we group them into three product types: Consumer IoT, Enterprise, and Industrial IoT.

Vendor selection followed a two-tier strategy designed from the outset. For large vendors, we included all Fortune 500 companies with publicly listed IoT product lines and downloadable firmware, yielding 15 vendors. For SMEs, we selected category leaders identified through market research reports (Berg Insight, Frost & Sullivan, European smart-home market-share data), choosing the top-ranked SMEs within each product category. From each selected vendor, we included all device models with publicly available firmware downloads. Because these are category-leading SMEs, the observed update gap relative to Fortune 500 vendors likely understates the difference for average SMEs. Our dataset includes 523 device models from 117 vendors. Table 1 summarizes our dataset composition.

Table 1: Phase 1 Dataset Composition

Vendor Category	Vendors	Device Models
Fortune 500	15	266
SME	102	257
Total	117	523

4.1.2 Results

We measure update disparity as the difference in annual firmware release frequency between vendor categories. Figure 2 presents the distribution of annual update frequencies by vendor category. Fortune 500 vendors exhibit significantly higher update frequencies than small and medium enterprise (SME) vendors (Mann-Whitney U test, $p < 0.001$, effect size $r = 0.73$). The Fortune 500 distribution has median 3.5 updates/year (IQR 2–6), with most products concentrated in the 1–10 updates/year range. Notably, 80% of Fortune 500 products receive at least 2 updates per year, and 46% receive 4 or more. While outliers exist at both extremes, the distribution clearly skews toward regular update cadences. SME vendors show a fundamentally different pattern: 93% of products receiving 1 or fewer updates annually. Only 6% of SME products reach 2 or more updates per year, suggesting that frequent update cycles remain out of reach for most smaller vendors. Fortune 500 products receive 12$\times$ more updates than SME products on average. Update frequency reflects a vendor's capacity to deliver patches on security-relevant timescales: a vendor that rarely releases firmware structurally cannot respond to vulnerabilities promptly regardless of intent. To confirm that the observed cadence corresponds to actual security work and not only feature releases, we examined the security content of releases directly. Table 2 reports the share of releases that mention a security fix or reference a CVE, broken down by company size and product type. Roughly half of all updates mention security fixes, and CVE references appear more frequently in SME and industrial releases, confirming that firmware updates are a meaningful, though not exclusive, vehicle for security patching. We note that update frequency and security-related release-note mentions serve as proxies for security-maintenance capacity rather than direct measures

Table 2: Percentage of firmware updates addressing security issues, based on release note analysis.

	% security fix	% w/ CVE	Coverage
By company size			
Large	48.8%	4.1%	2002–2026
SME	58.1%	28.9%	2008–2026
By product type			
Consumer IoT	52.9%	0.7%	2002–2026
Enterprise	48.4%	4.5%	2013–2026
Industrial IoT	58.1%	28.9%	2008–2026

Table 3: Percentage of devices still receiving firmware updates by product age.

Product type	0–1y	1–3y	3–5y	5+y
Consumer IoT	100%	62.0%	18.9%	1.6%
Enterprise	100%	95.6%	78.7%	55.9%
Industrial IoT	100%	97.1%	89.5%	63.5%

of vulnerability reduction, patch latency, or realized security outcomes.

The concentration of SME vendors at $\leq$1 update/year means many lack the operational capability to respond to emerging threats on security-relevant timescales. Large vendors have established update infrastructure and processes that enable regular cadences, while smaller vendors face barriers that prevent even annual updates. Beyond frequency, OTA support also degrades over product lifecycles. Table 3 shows the percentage of devices still receiving firmware updates at each age interval. Consumer IoT shows the sharpest decline: only 18.9% of devices receive updates between three and five years, dropping to 1.6% beyond five years. Enterprise and industrial products degrade more gradually but still lose over 40% of coverage beyond five years.

This pattern motivated Phase 2's investigation into vendor-side barriers: understanding why IoT vendors struggle requires examining the economic, technical, and organizational constraints they face.

4.2 Research Questions

Phase 1 revealed substantial disparities in firmware update frequency across vendor categories, with resource-rich enterprises maintaining significantly higher update cadences than SME vendors. This disparity is not explained by technical feasibility, as standards demonstrate that secure OTA mechanisms work even on resource-constrained devices and the technical literature extensively documents secure update protocols. This gap motivated us to investigate whether organizational, economic, or structural factors differentially affect vendors based on their resources and position in the supply chain.

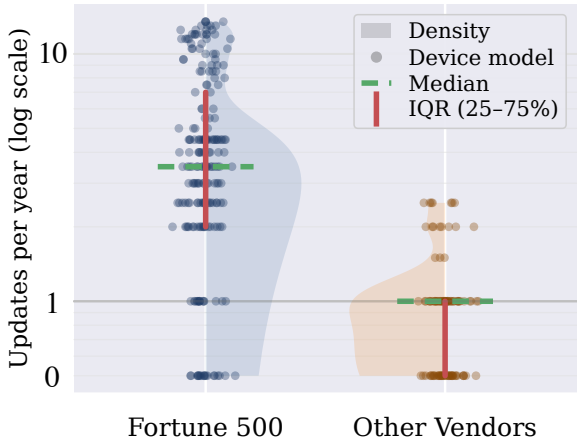


Figure 2: Annual firmware update frequency by vendor category. Each point represents one device model. Fortune 500 vendors concentrate in the 4–10 updates/year range (blue), while SME vendors cluster at $\leq$1 update/year (orange). Violin plots show density distributions; bars indicate median and IQR.

To investigate these factors, Phase 2 builds on both our Phase 1 findings and prior research. We observed substantial update frequency disparities between vendor types in Phase 1. Measurement studies document similar patterns of outdated firmware deployment [3, 10], motivating our examination of vendor perceptions and operational practices. Phase 1 revealed resource-based performance gaps across vendor sizes. Research on SME security constraints shows economic factors limit security investments [11, 30], guiding our investigation of OTA cost structures and lifecycle economics. The variation in update sustainability we observed aligns with supply chain security work identifying coordination failures [24, 31], directing focus toward responsibility fragmentation and upstream dependencies. These motivations correspond to the five research questions (RQ1–RQ5) introduced in Section 1.

4.3 Phase 2: Vendor Investigation

We investigate these research questions through a mixed-methods approach combining semi-structured interviews (N=30) with a large-scale structured survey (N=102). Interviews provide rich contextual insights into vendor challenges and decision-making processes, allowing us to explore the nuanced barriers and organizational factors that shape OTA practices. The survey quantifies how widespread these patterns are across the broader vendor population and tests whether findings from interviews generalize beyond our interview sample. Table 4 summarizes participant demographics across both methods, demonstrating coverage of vendor types, company

Table 4: Phase 2 Participant Demographics: Overview

Dimension	Category	Interviews	Survey	Dimension	Category	Interviews	Survey
Company Size	1–50 employees	2(6.7%)	5(4.9%)	**Product Scale**	1–50 SKUs	12(40.0%)	20(19.6%)
	51–500 employees	25(83.3%)	56(54.9%)		51–150 SKUs	15(50.0%)	72(70.5%)
	500+ employees	3(10.0%)	41(40.2%)		150+ SKUs	3(10.0%)	10(9.8%)
Product Category	Consumer Electronics	11(36.7%)	64(62.7%)	**Annual Revenue**	<$1M	1(3.3%)	5(5.0%)
	Smart Home	8(26.7%)	68(66.7%)		$1M–$10M	17(56.7%)	35(34.3%)
	Industrial/IIoT	6(20.0%)	19(19.0%)		$10M–$50M	12(40.0%)	62(61.0%)
	Wearables/Health	5(16.7%)	58(56.9%)				
Target Market	Asia	24(80.0%)	56(54.9%)	**Participant Role**	CTO/Engineering Lead	13(43.3%)	38(37.6%)
	Europe	23(76.7%)	52(51.0%)		Product Manager	6(20.0%)	25(24.6%)
	North America	12(40.0%)	47(46.1%)		Firmware Engineer	10(33.3%)	34(33.3%)
	Middle East	5(16.7%)	15(14.9%)		Founder/CEO	1(3.3%)	5(4.9%)
	Others	2(6.7%)	23(22.5%)				

Note: Interviews N=30, Survey N=102. SKU = stock keeping unit. Format shows count (percentage). Multi-select categories (Product Category, Target Market) may sum to over 100%.

scales, product categories, and operational contexts.

4.3.1 Semi-Structured Interviews

Recruitment. We recruited participants to ensure coverage of the organizational, economic, and supply chain dimensions central to our investigation. We targeted variation across four key dimensions: company size to capture resource differences affecting OTA sustainability, product categories to represent diverse supply chain structures, geographic markets to reflect varying regulatory contexts, and organizational roles to obtain perspectives from decision-makers, technical implementers, and product strategists. We recruited through professional networks, screening for direct OTA decision-making involvement and hands-on implementation experience. Participants received 20 EUR equivalent compensation for their time. We conducted 30 interviews, continuing until achieving thematic saturation across all research questions. Table 4 demonstrates comprehensive coverage across these dimensions.

Protocol. Interviews were conducted via video call, lasted 45–60 minutes, and were audio-recorded with participant consent. We used a semi-structured protocol organized around our five research questions (Section 4.2). Each interview began with warm-up questions about the participant's role and product portfolio to build rapport and establish context. We then systematically explored each research question, using open-ended prompts to elicit detailed narratives about vendor experiences rather than yes/no responses.

The semi-structured format allowed us to maintain consistency across interviews while adapting to each vendor's unique context. When participants raised unexpected topics or tensions, we probed deeper with follow-up questions to understand the underlying mechanisms. We explicitly asked for concrete examples and specific incidents to ground abstract claims in real-world experience. To minimize social desirability bias, we framed questions around industry challenges rather than individual failures, and emphasized that we sought to understand systemic barriers rather than evaluate individual practices. For sensitive topics like cost constraints or supply chain dependencies, we began with broader industry-level questions before asking about the participant's own situation. We concluded each interview by asking participants what they wished researchers or policymakers better understood about OTA challenges, often surfacing additional insights not covered by our structured questions. The interview guide, survey instrument, and qualitative codebook are available in the supplementary materials on OSF. We transcribed all interviews verbatim. Two researchers independently coded the transcripts following an inductive open-coding process with multiple coding passes over the full transcript set. We started with open coding to generate candidate codes, then grouped codes into themes aligned with the research questions. We reviewed the codebook and a sample of coded excerpts at each round, and revisited earlier transcripts after the codebook stabilized to ensure consistency. Disagreements were resolved by returning to the source transcripts.

4.3.2 Large-Scale IoT Vendor Survey

Instrument Development. We developed a structured survey to validate and quantify the patterns identified in interviews. The 29-question instrument covered six areas: company demographics and product characteristics, OTA delivery practices and update frequency, cost structures (lifecycle costs, per-device costs, margin impact, and specific factors that erode profitability), supply chain dependencies (reliance on chip/SDK vendors, patch lead times), security measures deployed, and deployment failure rates. Two ranking questions measured the relative importance of OTA motivations and constraints, revealing which factors dominated vendor

decision-making. We pilot tested the instrument with 20 IoT vendors, refining questions with high non-response or ambiguous wording. The final survey used multiple-choice, multiple-select, ranking, and numerical estimate formats, with 10–15 minute estimated completion time.

Distribution and Quality Control. We distributed the survey through Qualtrics, WJX, and Google Forms over a 4-week period in December 2025, using multiple channels: IoT industry mailing lists, trade association newsletters, and targeted advertising on business networking platforms. No monetary reward was offered for participation. We received 135 responses passing initial screening.

Quality control measures, following established survey transparency guidelines [14], identified low-quality responses through pre-screening questions to verify IoT domain involvement, embedded attention checks, completion time thresholds (flagging responses under 6 minutes), and pattern analysis for straight-lining and logical inconsistencies. After applying quality filters, we retained 102 responses for analysis (24% exclusion rate, consistent with technical professional surveys). Comparison of early versus late respondents showed no significant demographic differences, suggesting limited non-response bias. Because target market is a multi-select field, the sample covers all major regions with substantial representation: 55% of survey respondents serve Asian markets, 51% European, and 46% North American, with most vendors operating across multiple regions simultaneously (Table 4).

5 Results

We present findings from 30 vendor interviews and 102 survey responses, organized around our five research questions: vendor perceptions of OTA updates (RQ1), deployed operational practices (RQ2), supply chain responsibility allocation (RQ3), economic factors shaping sustainability (RQ4), and technical constraints limiting reliability (RQ5). Where survey data quantifies patterns observed in interviews, we integrate these findings within the corresponding research question.

5.1 RQ1: IoT Vendors' Perceptions and Attitudes

When asked why OTA capability matters, vendors rarely framed answers in terms of attackers, compromise, or integrity guarantees. Instead, almost all interviewees focused on post-shipment control: the ability to modify deployed devices when physical access is no longer practical. Vendors view shipment as the point at which uncertainty begins. They expect bugs, environmental mismatches, and new requirements to surface after deployment. OTA capability enables vendors to retain control over products once they leave the factory:

> *"For IoT products, OTA is the product's second life. After devices are shipped, fixes, optimizations, and feature additions all rely on OTA." – V21*

Survey data confirms this prioritization across the industry. When asked to rank reasons for providing OTA updates, respondents placed product improvements and reducing support costs above security. Only 18% of all survey respondents ranked security as their primary OTA motivation; the majority (61%) ranked it third or lower among five options. When vendors described OTA as "critical," their explanations focused on avoiding irreversible post-shipment failures, not proactive security strategy.

Vendors' understanding of OTA updates emerges from experience rather than anticipation. A majority of interviewees described a shift in attitude following incidents that caused direct loss: abnormal OTA behavior, device safety issues, or publicly disclosed vulnerabilities. Some learned by observing competitors' failures:

> *"There was a hardcoded password vulnerability in a smart camera product. More than 100,000 devices had to be recalled, and the direct loss exceeded 2.5 million USD. Only after that did we truly realize the role of OTA in product security." – V12*

Among interviewees who had not experienced security-related incidents, none ranked security as their top OTA priority. Security becomes the dominant justification for OTA only when failures produce visible consequences: recalls, compensation, or reputational damage.

While vendors frame OTA updates in terms of internal product control, regulatory requirements introduce external pressure that shapes investment decisions differently. Most interviewees described compliance requirements as moving targets that evolve over time and vary across markets. Unlike the reactive pattern observed for security incidents, compliance pressure operates preemptively: vendors invest in OTA capability before regulations take effect rather than waiting for enforcement actions.

> *"For overseas markets, requirements are not static. Even if you pass certification today, the rules may change next year. OTA is the only way to make sure products already in the field can still comply." – V7*

This preemptive investment is visible in resource allocation patterns. Figure 3 compares resource allocation across SME and large companies from the survey. Both groups allocate substantial resources to OTA: 18% for SME companies and 15% for large companies. The difference in compliance allocation is striking: large companies allocate 25% to compliance compared to only 6% for SME companies, reflecting the certification burden of multi-market operations. SME companies concentrate resources on hardware development at 30% and feature development at 22%, consistent with a growth-phase focus on product differentiation. Large companies distribute resources more evenly across categories, with compliance matching hardware at 25% each. The finding that

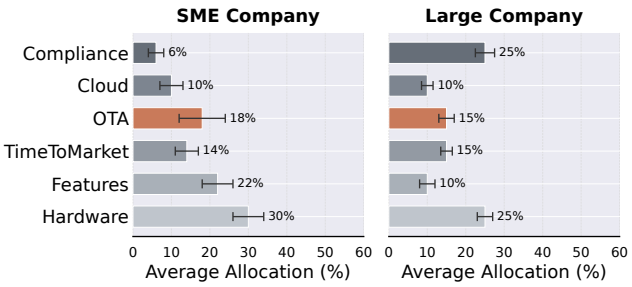


Figure 3: Resource allocation patterns for SME and large companies across hardware, features, time-to-market, OTA, cloud, and compliance expenditures. SME companies prioritize hardware and features while large companies allocate substantially more to compliance.

SME companies maintain the highest proportional OTA allocation despite constrained resources suggests that regulatory requirements for market access compel investment even when resources are scarce.

FINDING 1

OTA is perceived as lifecycle control, not security infrastructure, yet regulatory pressure drives preemptive investment. Vendors frame OTA as post-shipment product control, with security views emerging only reactively after incidents. However, compliance requirements compel preemptive OTA investment even among resource-constrained vendors.

5.2 RQ2: Deployed OTA Practices Across Products

In IoT manufacturing, many devices are produced by one company and sold under another company's brand. These white-label and OEM arrangements mean that vendors serving such markets reported multiple branded products commonly sharing the same firmware core, OTA backend, and cryptographic signing keys. A single codebase ships under multiple brand names, with differences limited to logos and configuration files. This sharing often extends to security infrastructure: several vendors reported centralizing signing under a single offline key because maintaining separate keys per brand would require dedicated key management teams they lack:

> *"Different brands use the same core firmware. The differences are mostly logo, UI, or configuration. The signing and update mechanism is shared... We do not have a professional key management team. Managing separate keys would increase the risk of mistakes or loss." – V11*

Because multiple brands share the same firmware and signing key, a vulnerability in the shared codebase affects all brands simultaneously, even if those brands are unaware of each other. Vendors do not maintain complete mappings from firmware components to downstream products, so when issues emerge, they discover the affected scope incrementally through brand-specific complaints rather than through infrastructure-level visibility:

> *"One brand reported a problem first. Later we found other brands using the same firmware had the same issue, just not reported yet. We do not have a list of all brands affected by a specific internal module. When something happens, we investigate step by step." – V6*

FINDING 2

Shared infrastructure couples security across brand boundaries without downstream visibility. Vendors reuse firmware and signing keys across white-label products, causing single updates to span multiple brands. Downstream brands and end users are unaware of this sharing, and cross-brand issues are detected through brand-specific complaints rather than infrastructure-level tracking, leading to delayed identification of affected scope.

Figure 4 shows that update practices diverge sharply by business model. Self-brand vendors, those that design, manufacture, and sell products under their own brand name, concentrate at regular intervals: 52.5% update quarterly or more frequently, and 32.9% update quarterly. OEM vendors cluster at the reactive end: 20.0% update only when issues arise, 11.0% rarely update, and 31.0% fall into this reactive category overall. Only 27.4% of self-brand vendors are similarly reactive. This divergence likely reflects both incentive differences (OEM vendors bear less direct reputational risk from security incidents) and the infrastructure sharing described above (shared firmware means each update affects more devices, raising the stakes and testing burden for each release).

The update frequency divergence is not about different firmware but about who decides when to release. Self-brand vendors control their own release schedule and bear direct reputational risk from unpatched devices, so they push updates proactively. OEM vendors produce shared firmware that ships under customer brands, but release timing depends on customer requests or reported issues, reducing the urgency to initiate updates independently. As V3 explained: *"Some clients keep firmware ownership and we just push what they send us. Others outsource the whole OTA to us. Either way, we don't decide when a release goes out."* The effort required for each release reinforces this reactive pattern: survey data shows that almost half of respondents require up to a month to prepare a typical update, while the other half require more than that, with 40% reporting 20 to 60 person-days per release.

What consumes this time? The dominant workload is not writing the patch itself but validating it against failure modes that only appear under real deployment conditions:

> *"The most time-consuming part is testing. We must simulate disconnection, power loss, insufficient memory, and other extreme conditions to check whether the device bricks. This*

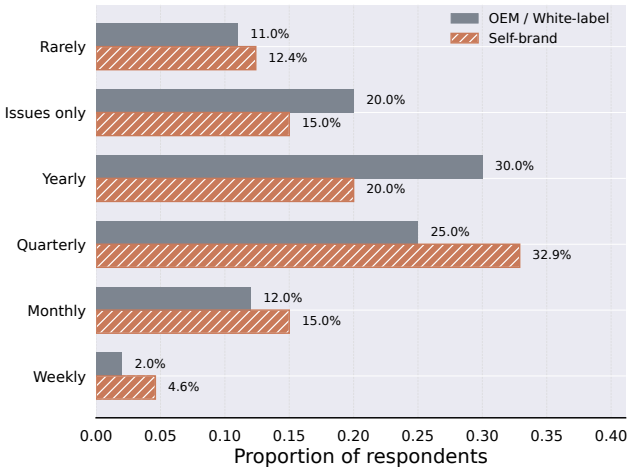


Figure 4: OTA update frequency diverges by business model (survey data, N=102). Self-brand vendors concentrate at regular intervals (quarterly to monthly), while OEM vendors cluster at the reactive end (rarely update or update only when issues arise).

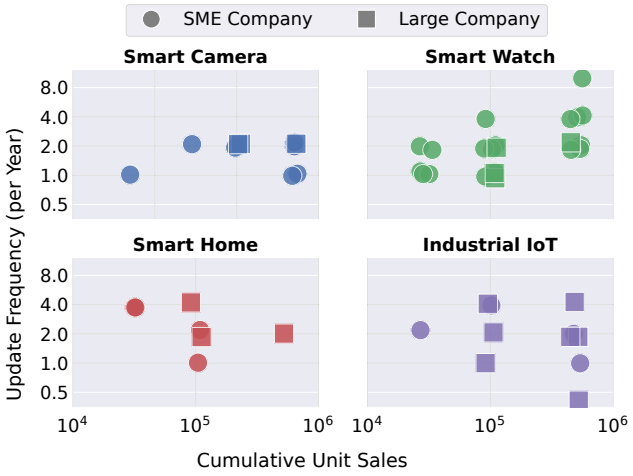


Figure 5: Update frequency versus sales volume for four product categories, comparing SME and large company vendors. Across all product types, SME vendors maintain lower update frequencies than large companies regardless of sales volume.

takes more time than development itself." – V28

Version fragmentation compounds this testing burden. Unlike mobile apps where platforms enforce updates, IoT devices in the field run many different firmware versions simultaneously. Vendors cannot assume users have updated; an update must work correctly whether the device is on V1.0, V2.0, or any intermediate version:

> *"Old users are on V1.0, new users are on V2.0, and another group is on a V1.5 bug version. We must ensure all groups receive update packages that work correctly. Maintaining this compatibility matrix is extremely painful." – V22*

Beyond development and testing, OTA imposes ongoing operational costs from backend monitoring, failure handling, and infrastructure maintenance that vendors often underestimate at product launch. As V12 noted: *"Bandwidth, support calls, version management. None of it shows up early, but it piles up over time."* We analyze these cost dynamics in detail in Section 5.4. These resource requirements translate into capacity limits that constrain how frequently vendors can issue security updates. Figure 5 plots update frequency against sales volume across four product categories, comparing SME and large company vendors. The four-panel comparison reveals a consistent pattern. As shown in the figure, across all product types, SME vendors maintain lower update frequencies than large companies, and this gap persists regardless of sales volume. Even at higher sales volumes, SME vendors do not achieve the update rates of large companies. This pattern suggests that the fixed costs of OTA infrastructure (testing environments, version management, dedicated personnel) require organizational scale that SME vendors cannot achieve through revenue growth alone. V7 illustrated the underlying economics: *"An entry-level smart plug earns us $0.70 per unit, but 5 years of OTA storage, operations, and compliance costs $1.10. We lose money on every one."* For security, this means SME vendors lack the capacity to respond to multiple vulnerabilities per year, even when they have the financial resources from product sales. However, the limited update frequencies observed for SME vendors leave minimal room for proactive security updates beyond the compliance minimum.

FINDING 3

OTA workload scales with deployment diversity, not patch size. The dominant burden comes from validating updates across product variants, fielded firmware versions, and failure-prone environments. SME vendors maintain lower update frequencies that higher sales cannot overcome, limiting their ability to respond to security vulnerabilities even when financially viable.

5.3 RQ3: Responsibility Allocation Across the OTA Supply Chain

OTA update capability depends on coordination among multiple independent entities, each controlling distinct layers of the technology stack. Survey data reveals this fragmentation is universal: 94% of respondents reported depending on at least three external parties for OTA functionality, with a median of five distinct organizations involved. No single organization possesses complete visibility into or authority over the full OTA pipeline. The typical distribution spans chip vendors controlling flash partitioning and drivers, communication module vendors handling network protocols, device manufacturers leading firmware development and testing, cloud platforms

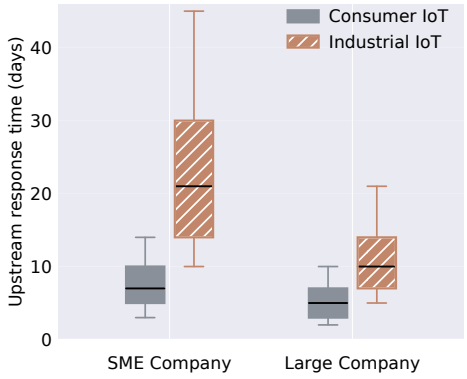


Figure 6: Upstream vendor response times by company size and product type. SME companies face substantially longer response delays than large companies, with Industrial IoT experiencing the worst delays (median 21 days for SMEs vs. 10 days for large companies).

managing distribution and monitoring, and customers or integrators deciding whether to upgrade.

Device manufacturers position themselves as coordinators, yet their actual control remains limited to integration and release decisions. While manufacturers bear market accountability for security failures, they lack technical authority over foundational components. This creates a fundamental mismatch: 87% of surveyed vendors reported being held responsible for security outcomes dependent on components they do not control. When OTA updates fail, this fragmented structure creates immediate ambiguity regarding responsibility. Vendors universally reported a consistent pattern: mutual blame, joint log-based investigation, and negotiated attribution based on log analysis:

> *"Once upgrade failure rate was abnormally high. Chip vendor said it was our app logic problem. App team said chip driver was unstable. Final resolution: whoever's territory, their responsibility. When truly unclear, we all meet together, pull logs line by line until we find the culprit." – V10*

The phrase "pull logs line by line" reveals that attribution operates through retrospective log analysis rather than pre-established accountability boundaries. Survey data confirms this is systemic: 91% of respondents reported no pre-established security incident response procedures spanning supply chain partners. As V6 noted: *"Whoever's module broke, they lead the fix. We only wrote that rule into the contract after the finger-pointing happened."* Attribution mechanisms focus on fault determination for cost allocation rather than rapid coordinated response. When asked about typical investigation duration, 68% reported requiring three or more days to identify root causes when issues involve upstream components. For security vulnerabilities, these diagnostic windows represent exposure periods during which affected devices remain unpatched while engineering resources target incorrect components.

Chip vendors occupy a critical position because they control foundational security capabilities: bootloader integrity, secure boot implementation, flash partitioning for rollback, and driver availability. Without chip vendor support for dual-bank firmware storage, devices cannot implement safe update mechanisms; without vendor-supplied cryptographic accelerators, devices may lack resources for signature verification. This technical dependency becomes a security problem when chip support lifecycles (typically 2 to 5 years) prove shorter than device deployment periods (5 to 10 years). Survey respondents identified chip vendors as the most difficult supply chain partner: 78% ranked chip vendors as their primary coordination bottleneck, compared to 12% for cloud platforms and 10% for SDK providers.

> *"Most difficult to coordinate is chip vendor. Their business scope is broad, they interface with many customers. Response speed to single customer's OTA update needs is slow. Sometimes we need SDK version adapted to new components. Often wait one to two weeks." – V5*

When chip vendors discontinue support entirely, the impact on security maintenance is severe. Survey data shows 62% of respondents have experienced chip support termination during active product lifecycles. Among these vendors, 71% reported cost increases of three times or more for subsequent security patches, while 23% reported losing patching capability entirely due to inability to reproduce build environments or reverse-engineer proprietary drivers:

> *"The chip vendor dropped SDK support while we still had 500k devices in the field. Reverse-adapting cost us $400k and 20 engineers for three months." – V7*

SDK providers create a different dependency problem. They supply pre-packaged modules (cryptographic operations, network communication, update verification) as compiled libraries without source code access. Survey data shows 83% of respondents integrate third-party SDKs for security-critical functions, yet only 31% have any visibility into SDK source code. This information asymmetry means manufacturers depend on SDK security properties they cannot independently verify. When security flaws exist within SDKs, they surface only through downstream symptoms. Manufacturers initially misattribute problems to their own code, spending investigation time on the wrong components while actual vulnerabilities persist. Once an SDK defect is correctly identified, remediation requires SDK provider cooperation. Respondents reported a median SDK response time of one to two weeks, with the remaining vendors experiencing delays exceeding one month.

Cloud platforms add a third layer of dependency. Survey data shows 67% of respondents experienced at least one OTA disruption caused by unannounced platform changes in the past two years. When platforms modify APIs without notice, the effects propagate immediately to all dependent devices. Beyond API stability, platform pricing structures create incen-

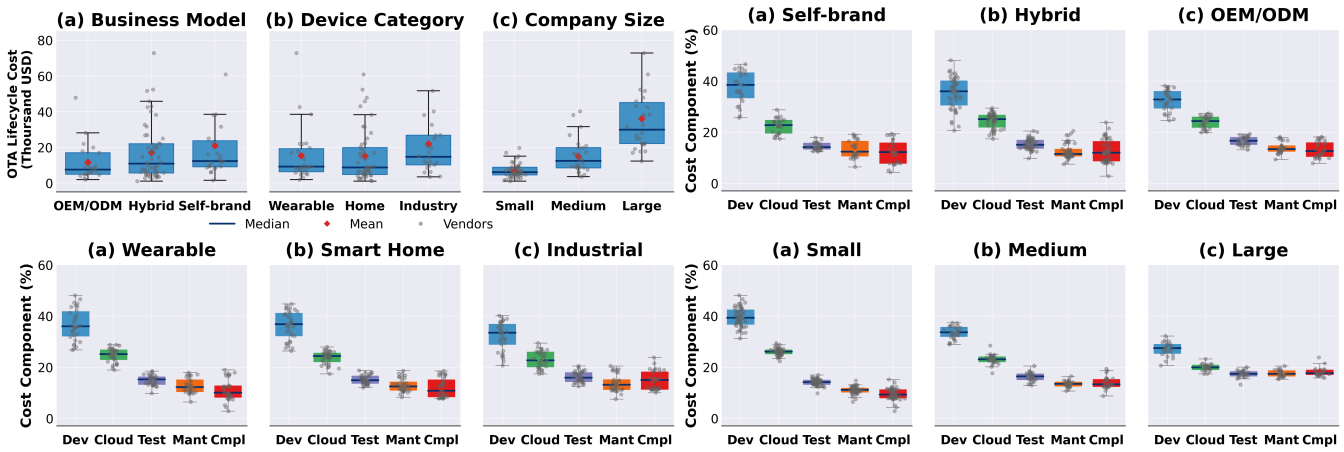


Figure 7: OTA lifecycle costs and cost composition across 102 vendors. Top row shows total costs by business model, device category, and company size. Bottom row shows cost composition breakdown for each dimension. Development dominates small vendor budgets while large vendors allocate more evenly across maintenance and compliance.

tives to batch or delay security patches: 54% of respondents reported that per-device update costs influence their patch deployment frequency.

Figure 6 quantifies these upstream dependencies across our survey population. SME companies face substantially longer response times than large companies across both industrial and consumer IoT product types. For Industrial IoT, SMEs experience median response times of 21 days compared to 10 days for large companies. Consumer IoT shows a similar pattern: SME medians of 7 days versus 5 days for large companies. This disparity may reflect upstream vendors prioritizing larger customers, or the greater internal engineering capacity of large companies to prepare requests and integrate responses faster. Regardless of cause, SMEs experience extended vulnerability windows during which security patches cannot be delivered.

The economic structure of these dependencies creates systematic cost transfer to device manufacturers. Upstream partners capture revenue at service initiation (chip sales, SDK licensing, platform subscriptions) while imposing ongoing costs through discontinuation, interface changes, or pricing adjustments that materialize years after product launch. Survey data confirms this pattern: 81% of respondents reported experiencing unexpected upstream-imposed costs after product launch, and 69% indicated these costs exceeded initial OTA budget projections. As V2 summarized: *"None of these upstream changes are under our control, but the bill always lands on us."* Device manufacturers cannot recover these costs through pricing adjustments for already-sold devices, forcing them to absorb the costs from existing margins or curtail security support when margins prove insufficient.

FINDING 4

Fragmented responsibility creates diagnostic delays and escalating costs. The OTA stack spans chip vendors, SDK providers, cloud platforms, and device manufacturers with no single entity possessing complete visibility. Most vendors lack pre-established incident response procedures across partners, requiring multi-day cause investigation.

5.4 RQ4: OTA Costs and Lifecycle Decisions

To understand the economic factors behind OTA maintenance decisions, we collected cost data from 102 vendors. Figure 7 decomposes OTA expenditure into five categories (development, cloud infrastructure, testing, maintenance, compliance) across company size, business model, and device category. The cost panels explain the update-frequency gaps reported in Section 5.2: small vendors allocate 40% of their OTA budget to development versus 27% at large vendors, leaving only 20% combined for maintenance and compliance against 36% at large vendors, roughly half the proportional spend on ongoing patch delivery and regulatory adherence.

Business model and device category shift costs along different axes. OEM/ODM vendors carry the highest median lifecycle costs from serving multiple regulatory environments across customer brands (13% compliance share versus 12% for self-brand vendors in single environments), while maintenance remains a 12–13% baseline burden regardless of business model. Across device categories, Industrial IoT carries the highest combined testing-and-compliance share at 30% to meet safety certifications and longer support expectations, leaving less budget for maintenance; consumer wearables concentrate 39% on development and only 9% on compliance in lightly regulated markets.

While these expenditures reflect current spending, vendors

reported that costs grew substantially beyond initial expectations. 76% of respondents reported that actual maintenance costs exceeded their original budget projections once products were in the field. Version fragmentation emerged as the primary unanticipated cost: as products mature, maintaining compatibility across deployed firmware versions creates engineering burden that vendors did not anticipate at launch. Upstream supply chain changes impose costs after products ship, as chip discontinuation forces firmware redevelopment and platform changes cause OTA disruptions. For 41% of respondents, government or enterprise contracts required support for the full operational lifetime of deployed devices, which in these sectors often extends well beyond the vendor's original product support horizon, turning what were scoped as short-term customizations into ongoing maintenance commitments. Because device pricing is fixed at sale, none of these costs can be recovered through the installed base.

FINDING 5

OTA cost composition varies systematically across company size, business model, and device category. Small vendors concentrate budgets on development, leaving maintenance and compliance underresourced. OEM vendors face high lifecycle costs from multi-customer compliance overhead. Industrial IoT products carry the largest testing and compliance burdens. Hidden costs from version fragmentation, supply chain changes, and contractual obligations consistently exceed initial projections.

These cost pressures also shape how long vendors maintain devices. 82% of respondents indicated that margin-to-maintenance ratios drive support period decisions:

> *"Our formula: support years equals sale price minus hardware cost, divided by annual OTA cost. High-end products get multi-year updates. Low-end products, after two years we recommend buying new ones." – V2*

These calculations contain no room for deployment lifetime or user safety. 58% of respondents confirmed that product price tier determines update frequency, with budget products receiving updates at half the rate of premium products or less. Figure 8 aggregates the cost and profit data reported by respondents across nine product categories, plotting five-year OTA costs as a percentage of per-unit profit. Smart plugs face OTA costs consuming 111% of unit profit, making security maintenance economically unsustainable. Smart bulbs and sensors fall in a marginal zone at 66% and 65%, where vendors reported curtailing security activities to preserve margins. Higher-margin products such as smart cameras, locks, and industrial gateways achieve viable economics below the 50% threshold. The products with the lowest per-unit margins are therefore the ones where vendors cannot sustain security maintenance.

The EU Cyber Resilience Act introduces minimum support periods with a five-year floor, creating a direct collision with these economics. 89% of respondents expressed concern about meeting five-year requirements for their current portfolios:

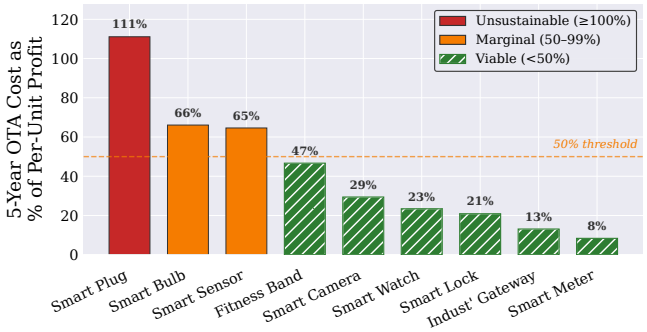


Figure 8: Five-year OTA costs as percentage of per-unit profit across nine product categories, based on cost and profit figures reported by survey and interview respondents. Low-margin products like smart plugs face unsustainable economics where OTA costs exceed unit profit. Smart bulbs and sensors fall in the marginal zone. Higher-margin products achieve viable economics below the 50% threshold.

> *"Current pricing cannot cover five years for low-profit products. If regulations force five-year updates, we will most likely abandon the low-end market." – V4*

When asked about responses to mandates exceeding economic constraints, vendors identified market exit at 45%, price increases at 38%, and category abandonment at 31%. Only 12% described absorbing cost differences as viable, and these were exclusively large enterprises. 73% of small vendors already reduce update frequency for low-margin products, and among OEM manufacturers, 52% indicated that white-label margins leave no room for extended maintenance. The regulatory mandate thus risks driving vendors from budget market segments rather than improving security maintenance across the IoT landscape.

FINDING 6

Support duration emerges from economic calculation with no security consideration. Margin-based formulas determine how long devices receive updates and at what frequency. Low-margin products face economically unsustainable OTA costs, and regulatory mandates requiring extended support may trigger market exit rather than improved security practices.

5.5 RQ5: Constraints Blocking Reliable OTA

Sections 5.3 and 5.4 documented how fragmented supply chains and cost structures shape OTA decisions. While Section 4.2 established that standardized OTA mechanisms are feasible for mainstream IoT devices, this section isolates legacy and sub-threshold devices (e.g., resource-constrained wearables) where technical constraints limit OTA reliability

across three stages: what devices can receive updates at all, whether vendors can produce patches, and whether patches reach devices in the field.

On resource-constrained devices, hardware limitations create threshold effects where devices below certain resource boundaries lack the capacity to run security mechanisms at all. Multiple vendors across smart city and wearable segments reported that memory and storage act as hard boundaries below which OTA security mechanisms become technically impossible. One smart city vendor described legacy streetlight controllers with only 4MB flash that could not run basic encryption, forcing the vendor to abandon security verification entirely. A wearables vendor reported that chips with only a few kilobytes of memory cannot run encryption algorithms, cannot store two firmware images for dual-bank rollback, and therefore cannot perform safe OTA updates at all. These are not cases of degraded security but of complete omission. The constraint compounds over time: devices that ship below the resource threshold lack the verification infrastructure that future updates would need to install, meaning they cannot be retrofitted with security mechanisms through the very OTA process that would deliver them.

For devices that are technically capable of receiving updates, patch production is constrained by the toolchain discontinuations described in Section 5.3. Of the vendors who experienced such discontinuation, 47% reported that it occurred while devices were still under warranty or contractual support obligations. Some vendors worked around discontinuation through reverse engineering, but this required months of effort for a single patch, making it unsustainable as routine practice. Others reported complete failure to reconstruct build environments, leaving no path to compile a security patch at all. This constraint is not limited to legacy products: 34% of vendors with products launched in the past three years reported already experiencing at least one upstream discontinuation affecting their ability to deliver patches. Combined with the version fragmentation documented in Section 5.2, patch production faces compounding constraints. Even when vendors successfully produce and test a patch, delivering it to devices faces its own barriers. 67% of respondents experienced OTA delivery failures from network or platform factors in the past year. Incomplete downloads from network interruption were the most common cause, reported by 58% of respondents, followed by app store review delays blocking companion app updates at 41% and carrier-specific behaviors interfering with device-cloud communication at 37%.

> *"Android app store review is more troublesome than Apple due to multiple channels, which have their own review rules. Third-party stores add further requirements. Synchronizing cross-platform launches requires dedicated personnel monitoring multiple channels." – V8*

54% of respondents maintain dedicated personnel for platform coordination, overhead that scales with market reach rather than device count. Physical deployment conditions further reduce delivery reliability. Vendors reported temperature-induced verification failures in extreme climates, where flash read-write anomalies at low temperatures caused CRC checks to fail, making it impossible to distinguish corrupted updates from environmentally induced errors. Power infrastructure variability in regions with frequent outages forced vendors to implement battery-threshold policies that delay updates until sufficient charge is available. In underground and industrial deployments with intermittent connectivity, one vendor reported OTA success rates as low as 60%. Across the full survey population, respondents reported average OTA success rates of 87%, meaning 13% of devices fail to receive any given update on the first attempt. For security patches requiring rapid deployment, this failure rate translates into extended vulnerability windows for a significant fraction of the installed base.

FINDING 7

Technical constraints limit OTA reliability across hardware capability, patch production and delivery. Resource-constrained devices lack the capacity for security verification and cannot be retrofitted through OTA. Even when patches can be produced, infrastructure and environmental heterogeneity can cause a significant fraction of devices to miss any given update, extending vulnerability windows.

6 Discussion

Our findings reveal how supply chain fragmentation, white-label firmware reuse, and lifecycle economics cause IoT OTA security to degrade in practice. We discuss how these findings connect to prior work, their societal implications, their consequences for regulatory approaches, and limitations of our study.

6.1 OTA Security as a Supply Chain Problem

Prior supply chain security research focuses on adversarial compromise of update channels [24, 31]. Our findings reveal a different problem: even without attackers, the structure of IoT supply chains produces insecure outcomes. No single actor can address OTA security unilaterally because none possesses both the technical authority and economic incentive to do so. The economic structure reinforces this fragmentation through temporal separation between revenue capture and cost imposition. Upstream partners capture revenue at service initiation including chip sales, SDK licensing, platform subscriptions, while costs from support discontinuation or interface changes materialize years later and fall on device manufacturers. Manufacturers cannot recover these costs from already-sold devices, forcing them to absorb losses from margins or curtail support. Upstream partners face no direct

consequences for decisions that undermine downstream security maintenance, creating systematic underinvestment in long-term maintainability across the supply chain. The result is that security degrades not from negligence at any single point, but from a structure in which no actor's incentives align with the long-term maintenance the ecosystem requires.

6.2 Societal Impact

This supply chain dynamic has a direct societal consequence: IoT security degrades along socioeconomic lines. The lowest-margin products, smart plugs, bulbs, and sensors, are the most widely deployed yet economically unsustainable to maintain. These are also the devices most accessible to price-sensitive consumers who cannot replace them when support ends. Unlike traditional software, where one operating system update covers all users regardless of device price, IoT vendors' margin-based formulas translate price differences directly into security differences. Prior work documents that users assume devices will receive long-term support [8], but our data shows this assumption fails most severely for the lowest-cost devices that dominate residential deployments. As these devices increasingly mediate physical safety through smart locks, smoke detectors, and medical monitors, this economic stratification of security maintenance carries consequences beyond data privacy.

6.3 Implications for Regulation

Our findings reveal a tension in how regulation shapes OTA investment. Section 5.1 showed that compliance requirements are among the most effective drivers of OTA investment: vendors invest preemptively to maintain market access, even under tight resource constraints. Yet Section 5.4 showed that when compliance costs exceed what product margins can sustain, vendors respond with market exit or category abandonment rather than improved security. This suggests a calibration problem: regulation must be strong enough to compel investment but structured to avoid pushing low-margin product categories, which are often the most widely deployed, out of the market entirely.

The EU CRA mandates security updates for expected product lifetime with a five-year floor, targeting device manufacturers as the responsible party. Our findings suggest this approach may not address the supply chain dynamics we observed. Manufacturers bear compliance obligations but lack authority over partner support lifecycles, SDK maintenance commitments, or distribution platform stability. When facing mandates exceeding economic constraints, vendors in our survey reported planning market exit, price increases, or category abandonment rather than absorbing costs. Prior work has documented mismatches between consumer expectations for long-term support and actual vendor practices [8, 15]. Our findings help explain why this mismatch persists: vendors cannot guarantee long-term support when upstream dependencies have shorter lifecycles. Regulations targeting manufacturers create compliance obligations that manufacturers may be unable to meet given their position in the supply chain. Requirements for chip vendors to maintain driver support for defined periods, mandates for SDK providers to offer source escrow, and distribution platforms stability requirements could address some barriers our findings identify.

6.4 Limitations

Our study relies on self-reported data from vendors, which we triangulate by comparing survey responses against independent interview accounts and by analyzing relative differences across vendor categories rather than absolute values. Vendors who participated may be more familiar with OTA practices than the broader population, which if anything makes our findings conservative, as less engaged vendors likely face similar or greater challenges. Our data reflects a single point in time, though the structural factors we identify, such as toolchain lifecycle mismatches and supply chain coordination requirements, are embedded in how IoT ecosystems are organized and are unlikely to change on short timescales. We focus on the device manufacturer perspective because manufacturers occupy the integration point where upstream dependencies and downstream support obligations converge, providing the most direct view into why OTA support degrades over time; however, we do not observe internal processes of chip vendors, SDK providers, or cloud platforms, whose views on responsibility and coordination may differ. Phase 1 SME vendors were selected as category leaders, so the observed update gap may understate the problem for average SMEs, and product type may confound vendor-size comparisons. Phase 1 relies on publicly posted firmware releases, which may undercount vendors who distribute updates exclusively through OTA without publishing firmware files. Interview and survey participants skew toward mid-size companies; very small companies are underrepresented and may face different constraints.

7 Conclusion

Through interviews with 30 vendors and a survey of over 100 practitioners, we show that IoT OTA update delivery failures caused from fragmented supply chain responsibility, inadequate technical solutions, and structural lifecycle mismatches rather than just economic constraints. No single actor in the supply chain possesses both the technical authority and economic incentive to ensure long-term security maintenance. Margin-based formulas determine support duration with no security variables, and low-margin products face OTA costs that exceed per-unit profit. These organizational barriers cannot be overcome by protocol improvements alone, and effective regulation must extend beyond device manufacturers to upstream supply chain actors.

Ethical Considerations

Our research investigates vendor practices and organizational challenges in IoT over-the-air update delivery through interviews with 30 vendors and surveys of 100+ practitioners. This work raises several ethical considerations regarding participant protection, responsible disclosure, and societal impact.

Protecting Vendor Participants. Vendors who agreed to discuss their OTA practices faced professional risks in sharing information about security limitations, cost pressures, and operational constraints. Many expressed concerns about regulatory exposure or competitive disadvantage. We obtained institutional ethics approval and secured informed consent emphasizing voluntary participation and confidentiality. All vendors are anonymized using categorical identifiers (e.g., "Small-OEM", "Component Supplier") that prevent identification while preserving analytically relevant distinctions. We excluded specific product names, version numbers, and implementation details that could expose individual companies. Interview transcripts containing sensitive business information are stored on encrypted institutional servers with restricted access.

Several vendors disclosed inadequate security practices or expired support commitments during interviews. We committed not to report these to regulatory authorities, as doing so would violate research confidentiality and chill future cooperation. Our goal is understanding systemic patterns, not enforcement. However, we encouraged vendors to address critical issues and provided resources for improving practices where appropriate.

Responsible Disclosure of Industry Practices. Our findings reveal widespread challenges in sustaining long-term OTA support, including fragmented supply chain responsibilities and economic pressures that shorten support lifecycles. While transparency serves the public interest, we carefully considered how presenting these findings might impact consumer security. We avoid detailed technical disclosures that could enable exploitation of specific products. When describing vendor constraints, we distinguish between structural challenges requiring policy intervention and cases of negligence. Our recommendations focus on constructive pathways forward rather than simply documenting failures.

Balancing Stakeholder Interests. IoT security involves competing interests: consumers deserve secure devices with long-term support, vendors face economic constraints and technical challenges, and policymakers need evidence for regulation. Our analysis explicitly addresses these tensions rather than privileging any single perspective. We present vendor constraints honestly while maintaining that security requirements remain necessary, and propose policy mechanisms that provide support alongside accountability.

Implications for Vulnerable Populations. Inadequate OTA update practices disproportionately affect users who cannot afford frequent device replacement or lack technical expertise to assess security posture. Our work highlights how economic pressures on vendors translate to security risks for end users. We emphasize this distributive justice concern in our recommendations, advocating for extended support periods and clearer disclosures that benefit all users, particularly those most vulnerable to insecure IoT devices.

Open Science

To enable verification while protecting participant confidentiality, we provide interview and survey question lists, a qualitative codebook with code definitions and representative quotes, the Phase 1 vendor, device, and firmware list, and anonymized consented survey responses. Survey response distributions are included in Appendix A. The interview and survey question lists, qualitative codebook, vendor/device/firmware list, and anonymized survey responses are available as supplementary materials on Zenodo at https://zenodo.org/records/20544041. The interview question list details all questions used during vendor interviews, organized by research question. The survey question list presents the survey questionnaire. The qualitative codebook documents all codes derived from thematic analysis, including definitions and representative anonymized interview quotes.

References

[1] Ross Anderson. Why information security is hard – an economic perspective. In *Seventeenth Annual Computer Security Applications Conference (ACSAC 01)*, pages 358–365. IEEE, 2001.

[2] Conner Bradley and David Barrera. Towards characterizing IoT software update practices. In *Foundations and Practice of Security (FPS 2022), Lecture Notes in Computer Science, Volume 13877*. Springer, 2023.

[3] Andrei Costin, Jonas Zaddach, Aurélien Francillon, and Davide Balzarotti. A large-scale analysis of the security of embedded firmwares. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 95–110, San Diego, CA, 2014. USENIX Association.

[4] Andrea De Simone, Giovanna Turvani, and Fabrizio Riente. Incremental firmware update over-the-air for low-power IoT devices over LoRaWAN. *arXiv preprint arXiv:2505.13764*, 2025.

[5] Zakir Durumeric, James Kasten, David Adrian, J. Alex Halderman, Michael Bailey, Frank Li, Nicholas Weaver, Johanna Amann, Jethro Beekman, Mathias Payer, and Vern Paxson. The matter of heartbleed. In *Proceedings of the 2014 ACM Internet Measurement Conference (IMC 14)*, pages 475–488, Vancouver, BC, Canada, 2014. ACM.

[6] Frank Ebbers. A large-scale analysis of IoT firmware version distribution in the wild. *IEEE Transactions on Software Engineering*, 49(2):816–830, 2023.

[7] Fariborz Farahmand, Mikhail J. Atallah, and Eugene H. Spafford. Incentive alignment and risk perception: An information security application. *IEEE Transactions on Engineering Management*, 60(2):238–246, 2013.

[8] Julie Haney, Yasemin Acar, and Susanne Furman. "It's the company, the government, you and I": User perceptions of responsibility for smart home privacy and security. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 411–428. USENIX Association, 2021.

[9] José L. Hernández-Ramos, Gianmarco Baldini, Sara N. Matheu, and Antonio Skarmeta. Updating IoT devices: Challenges and potential approaches. In *2020 Global Internet of Things Summit (GIoTS)*, pages 1–5. IEEE, 2020.

[10] Qinsheng Hou, Wenrui Diao, Yanhao Wang, Xiaofeng Liu, Song Liu, Lingyun Ying, Shanqing Guo, Yuanzhi Li, Meining Nie, and Haixin Duan. Large-scale security measurements on the android firmware ecosystem. In *Proceedings of the 44th International Conference on Software Engineering (ICSE 22)*, pages 1257–1268. ACM, 2022.

[11] Nicolas Huaman, Bennet von Skarczinski, Christian Stransky, Dominik Wermke, Yasemin Acar, Arne Dreißigacker, and Sascha Fahl. A large-scale interview study on information security in and attacks against small and medium-sized enterprises. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 1235–1252. USENIX Association, 2021.

[12] S. El Jaouhari and E. Bouvet. Secure firmware over-the-air updates for IoT: Survey, challenges, and discussions. *Internet of Things*, 18:100508, 2022.

[13] Kailani R. Jones, Ting-Fang Yen, Sathya Chandran Sundaramurthy, and Alexandru G. Bardas. Deploying android security updates: An extensive study involving manufacturers, carriers, and end users. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS 20)*, pages 551–567, Virtual Event, 2020. ACM.

[14] Jan H. Klemmer, Juliane Schmüser, Fabian Fischer, Jacques Suray, Jan-Ulrich Holtgrave, Simon Lenau, Byron M. Lowens, Florian Schaub, and Sascha Fahl. How transparent is usable privacy and security research? A meta-study on current research transparency practices. In *34th USENIX Security Symposium (USENIX Security 25)*. USENIX Association, 2025.

[15] Lorenz Kustosch, Carlos Gáñan, Mattis van 't Schip, Michel van Eeten, and Simon Parkin. Regulating smart device support periods: User expectations and the european cyber resilience act. In *Proceedings of the 34th USENIX Security Symposium*, 2025.

[16] Knud Lasse Lueth. What happened to the 620+ IoT platforms, and what is ahead, 2025.

[17] Prianka Mandal and Adwait Nadkarni. "We Can't Change it Overnight": Understanding industry perspectives on IoT product security compliance and certification. In *2025 IEEE Symposium on Security and Privacy (SP 25)*, pages 2341–2359. IEEE, 2025.

[18] Ioannis Mavromatis, Aleksandar Stanoev, et al. Reliable IoT firmware updates: A large-scale mesh network performance investigation. *arXiv preprint arXiv:2203.04682*, 2022.

[19] Brendan Moran, Hannes Tschofenig, David Brown, and Milosch Meriac. A firmware update architecture for internet of things. Technical Report RFC 9019, Internet Engineering Task Force (IETF), April 2021. IETF RFC on firmware update terminology and architecture.

[20] Philipp Morgner and Zinaida Benenson. Exploring security economics in IoT standardization efforts. In *NDSS Workshop on Decentralized IoT Security and Standards (DISS)*, 2018.

[21] Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling, and Zinaida Benenson. Security update labels: Establishing economic incentives for security patching of IoT consumer products. In *2020 IEEE Symposium on Security and Privacy (SP 20)*, pages 429–446. IEEE, 2020.

[22] Antonio Nappa, Richard Johnson, Leyla Bilge, Juan Caballero, and Tudor Dumitras. The attack of the clones: A study of the impact of shared code on vulnerability patching. In *2015 IEEE Symposium on Security and Privacy (SP 15)*, pages 692–708. IEEE, 2015.

[23] Joo Ng. Rethinking the cybersecurity of consumer internet of things (IoT): How to incentivise companies to produce cyber-secure consumer IoT products. Technical Report RHUL–ISG–2019–2, Information Security Group, Royal Holloway University of London, 2019.

[24] Marc Ohm, Henrik Plate, Arnold Sykosch, and Michael Meier. Backstabber's knife collection: A review of open source software supply chain attacks. In *Proceedings of the 17th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 20)*, pages 23–43. Springer, 2020.

[25] Open Mobile Alliance. OMA Lightweight M2M (LwM2M) technical specification. https://omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m/, 2025. Standard protocol for IoT device management including firmware updates.

[26] Ali Shoker, Fernando Alves, and Paulo Esteves-Verissimo. ScalOTA: Scalable secure over-the-air software updates for vehicles. *arXiv preprint arXiv:2307.02032*, 2023.

[27] Nissy Sombatruang, Tristan Caulfield, Ingolf Becker, Akira Fujita, Takahiro Kasama, Koji Nakao, and Daisuke Inoue. Internet service providers' and individuals' attitudes, barriers, and incentives to secure IoT. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 1541–1558. USENIX Association, 2023.

[28] Santiago Torres-Arias, Hammad Afzali, Trishank Karthik Kuppusamy, Reza Curtmola, and Justin Cappos. in-toto: Providing farm-to-table guarantees for bits and bytes. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1393–1410, Santa Clara, CA, 2019. USENIX Association.

[29] Luca Verderame, Antonio Ruggia, and Alessio Merlo. PARIOT: Anti-repackaging for IoT firmware integrity. *Journal of Network and Computer Applications*, 217:103699, 2023.

[30] Charles Weir, Ben Hermann, and Sascha Fahl. From needs to actions to secure apps? the effect of requirements and developer practices on app security. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 289–305. USENIX Association, 2020.

[31] Laurie Williams, Giacomo Benedetti, Sivana Hamer, Ranindya Paramitha, Imranur Rahman, Mahzabin Tamanna, Greg Tystahl, Nusrat Zahan, Patrick Morrison, Yasemin Acar, Michel Cukier, Christian Kästner, Alexandros Kapravelos, Dominik Wermke, and William Enck. Research directions in software supply chain security. *ACM Transactions on Software Engineering and Methodology*, 34(5):Article 146, 2025.

[32] Yuhao Wu, Jinwen Wang, Yujie Wang, Shixuan Zhai, Zihan Li, Yi He, Kun Sun, Qi Li, and Ning Zhang. Your firmware has arrived: A study of firmware update vulnerabilities. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 5627–5644, Philadelphia, PA, 2024. USENIX Association.

[33] Koen Zandberg, Kaspar Schleiser, Francisco Acosta, Hannes Tschofenig, and Emmanuel Baccelli. Secure firmware updates for constrained IoT devices using open standards: A reality check. *IEEE Access*, 7:71907–71920, 2019.

[34] Qian Zhang, Yi He, Yue Xiao, Xiaoli Zhang, and Chunhua Song. OTA-Key: Over-the-air key management for flexible and reliable IoT device provision. *IEEE Transactions on Network and Service Management*, 2024.

Appendix A Survey Response Distributions

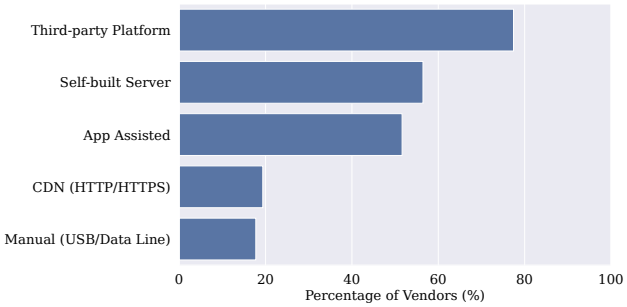


Figure 9: Distribution of OTA delivery methods used by survey respondents.

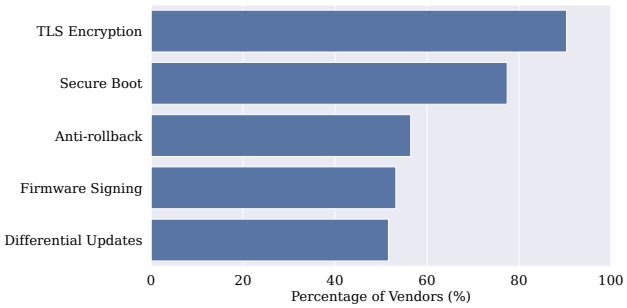


Figure 10: Distribution of security measures implemented in OTA delivery systems.

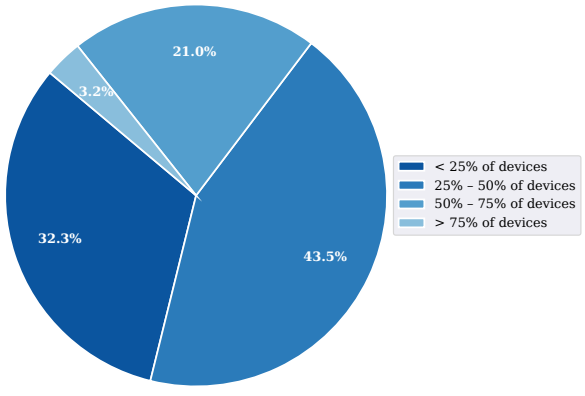


Figure 11: Percentage of deployed devices updated within 90 days.

Perceived Barrier	R1	R2	R3	R4	R5	R6	R7
High Engineering Cost	21	12	10	3	4	5	4
Lack of Manpower	5	7	3	8	11	7	16
Upstream Dependency	12	5	11	11	9	7	6
Testing Burden	4	13	8	9	10	10	5
Bricking Risk	10	12	10	7	9	7	4
Logistics Complexity	1	5	13	10	8	10	13
Low Profit Margin	9	8	7	10	6	9	7

Table 5: Ranking frequency for barriers preventing frequent OTA deployment (R1 = Most Critical, R7 = Least Critical).

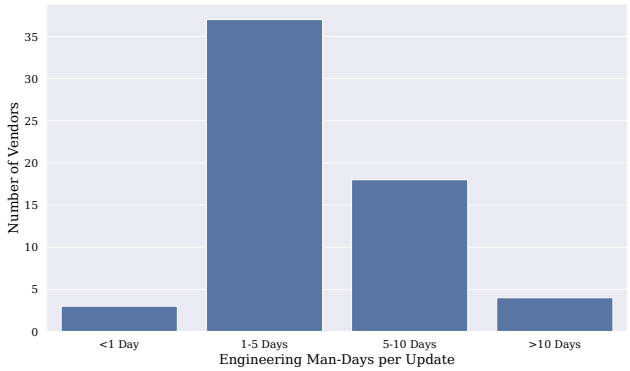


Figure 12: Engineering effort per OTA release across survey respondents.

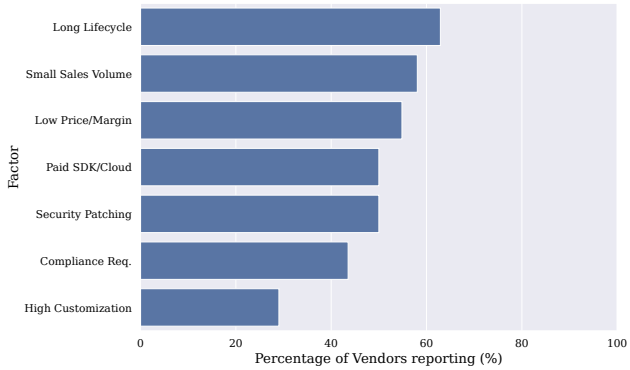


Figure 13: Profit erosion from OTA costs over product lifecycle.