Born Secure

Reputation-proof IoT innovation from product conception to market penetration

Executive Summary

The business imperative for launching a line of IoT products is impossible to ignore – but security concerns often threaten a company's well-laid plans to innovate. While smart devices have been mainstream for more than a decade, the security behind these devices has not demanded the urgency it deserves until more recently. The inherent risks of a hyperconnected world make this lack of urgency difficult to fathom, but the trend of neglecting security in the development of web-enabled "things" has several interlinked motives.

Eseye's 2024 State of IoT Adoption Report, drawing on responses from 1,200 senior decision-makers in the US and UK, tells a story of strong momentum paired with persistent friction. 80% of organizations plan to expand their IoT deployments within the next 18 months, and 74% expect to increase investment over the next two years. Yet despite that confidence, execution remains a challenge. Security risks have surpassed connectivity as the top concern, with 50% of businesses reporting an IoT-related security breach in the 12 months prior to the survey.

While persistent execution challenges stem from many sources, including supply chain pressures and geopolitical disturbances, security concerns consistently top the list. The risk of cyberattacks and the complexity of onboarding and certifying IoT devices at scale remain the most commonly cited barriers to progress.

Yet, the same reports have found that nearly all companies consider investment in IoT a long-term priority and critical for their success, even if they have decided to sideline or curtail certain projects. The message is clear: if companies can surmount security concerns, they will be better positioned and more confident to pursue their strategic IoT roadmaps to the fullest.

In this white paper, we put both the business potential and security threat of pursuing an IoT product line into perspective. We also explore the security roadmap that will propel the next generation of secure-as-can-be IoT devices into the market.

An IoT product born secure lives securely. Key lifecycle questions to consider:

- Ideation: Has threat modeling been conducted to identify the device's unique weak points and determine the optimal security profile?
- Development: How can the device be secure-by-design while achieving its functional, economic, and end-user objectives?
- Manufacture: Has the device been built by applying hardware Root of Trust principles?
- Distribution: Has the security embedded in the device + platform been third-party verified?

- Scale: What is the best growth plan to maximize market impact without weakening security?
- Lifecycle: Is security guaranteed for the entire life of the product by ensuring regular security updates and identifying potential threats up until decommissioning?

Many companies prioritize being cost-competitive over security-competitive – a decision based on consumer price elasticity, manufacturing haste, naivety, sheer indifference, or perhaps even a reckless disregard of security risks.

However, cost concerns only tell part of the story. Many might assume that security deficiencies primarily compromise low-cost, low-criticality products – "but it's just a light bulb!" There are two issues with that line of thinking:

First, security faults and hackability have jeopardized even the most life-critical, strictly regulated applications. Perhaps the most frightening example is implantable cardiac devices with a weakly encrypted communication channel between the transmitter and implant, allowing bad actors to control the pacer shocks of unsuspecting heart patients.

Second, assuming there exists an innocuous entry point into a connected system is oxymoronic. In an IoT ecosystem, a malicious actor's best bet is to exploit the weakest link and navigate laterally across the network to reach sensitive and prized assets.

In light of these facts, we believe that even elementary IoT-enabled products need to be developed with the utmost security stewardship and hygiene to fend off attacks. Product developers will need to adopt a deeply integrated security approach to achieve this objective. This starts at the earliest stage in the IoT value chain, by ensuring that all hardware and software components used in the manufacturing process are born secure – a complex task considering the diversity and geographic dispersion of component suppliers.

***Joe Britt** CEO, Afero*

Part One. The Internet-of-Things: Does the Potential Outweigh the Risk?

The scale of IoT opportunity is no longer a matter of debate — billions of connected devices are already deployed across every industry, with projections pointing toward tens of billions more by the end of the decade. But headline numbers only tell part of the story; a company needs industry-specific context to evaluate what IoT can enable it to achieve and how those capabilities underpin its future viability.

Virtually every company will acknowledge that innovation is essential to competing in today's technologically advanced economy, but that does not mean they all rush out to integrate the latest buzzy tech trend into their flagship products. For some, innovation means improving processes rather than transforming merchandise. For others, there is an elevated risk of breaking the status quo and alienating loyal customers who may expect their trusted staples to stay the same.

But as consumers become convinced of the day-to-day benefits that IoT offers, they drive a demand that forces companies to adapt traditional products to align with contemporary connectivity trends.

Intensity and scope of IoT ambition depends on a company's unique objectives

Iteratively modernizing a trusted product rather than starting from scratch is nothing new. PlayStation has had five console versions since its introduction in 1994, each offering better functionality and graphics than the last. Toyota has released eleven generations of its bestselling Corolla since 1966, with each generation improving gas mileage, electronic capabilities, and interior quality.

The motive for a business to pursue IoT falls along these same lines: adaptation, modification, and enhancement to keep the brand relevant in a new era. On the other hand, product developers can apply IoT in ways that impact our lives by providing previously unattainable functionality and feedback. The healthcare sector is already deeply invested in IoT, from remote temperature monitoring for vaccines to connected inhalers and heart rate monitors. In manufacturing, estimated to be the biggest market for IoT devices in the coming years, companies are using predictive maintenance, robots, and AI logistics to slash production times and boost efficiency.

Part Two. Threat Assessment: IoT's Near-Infinite Spread is Also Its Greatest Vulnerability

While the media often conflates attacks on enterprise IT and IoT as being part of a shared class of vulnerability, the truth is that IoT systems, and thus attacks, are more complex. The proliferation of billions of devices creates an overabundance of porous attack surfaces. As noted in the introduction, all it takes to harm an entire IoT network is a single weak point of entry.

Top 10 IoT Vulnerabilities (OWASP)

- Weak, Guessable, or Hardcoded Passwords

- Insecure Network Services
- Insecure Ecosystem Interfaces
- Lack of Secure Update Mechanism
- Use of Insecure or Outdated Components
- Insufficient Privacy Protection
- Insecure Data Transfer and Storage
- Lack of Device Management
- Insecure Default Settings
- Lack of Physical Hardening

Data powers IoT and produces zettabytes of it; more data produced means more data eligible to be compromised. Perhaps most fundamentally, IoT creates a link between the physical and digital worlds. An ever more pressing security puzzle arises, where hacks are about more than just disrupting systems. They can manipulate real-world objects and interrupt our lives in unprecedented ways. The prospect of your car being hijacked remotely, hospital infusion pumps commandeered by ransomware, or a city's water supply being chemically altered are no longer hypothetical — all have occurred when IoT security was left unaddressed.

Weapons of Mass Disruption?

The competition for the craziest IoT device compromise continues indefinitely. Spying dolls, infiltrated casino fish tank thermometers, hacked baby monitors, and remotely programmed apartment thermostats set to below freezing — not to mention voting machines, cars, and the shutting down of an entire city's stoplights. More recently, attackers have used an unsecured webcam to deploy ransomware across a corporate network, and a botnet of compromised smart TVs became the largest of its kind ever recorded. While some of these cases involved researchers probing for vulnerabilities to improve security, others were carried out on live systems by bad actors with malicious intent — proving a vulnerability can be hiding just about anywhere.

Reputation Catastrophe: Been-Hacked is the Biggest Taboo

The financial toll of a security breach is well-documented and growing. According to IBM's annual Cost of a Data Breach Report, the global average cost of a breach reached $4.88 million in 2024, which is a record high and the largest year-over-year increase since the pandemic. 70% of breached organizations reported significant or very significant disruption to their operations, and for most, recovery took more than 100 days. And those are just the direct costs measured in shutdowns, business interruption, and remediation.

Perhaps more lasting is the reputational cost when consumers learn a company has been breached. The public does not take data breaches lightly. Customers leave, stock prices fall, and for smaller businesses, the consequences can be fatal. The pattern repeats with every high-profile incident: trust, once lost, is rarely fully recovered.

A New Era of IoT Regulation

The regulatory environment for IoT security has shifted dramatically. The EU Cyber Resilience Act, which entered into force in December 2024, establishes mandatory cybersecurity requirements for all connected products sold in the EU. The UK's Product Security and Telecommunications Infrastructure (PSTI) Act, which came into force in April 2024, mandates minimum security standards for consumer connectable products. In the US, the FCC formally established the Cyber Trust Mark, a voluntary IoT labeling program, in 2024. The regulatory shift that industry observers long anticipated has arrived, bringing with it mandatory compliance requirements and real penalties for non-compliance. For companies that have already embraced a secure-by-design approach, this is validation. For those who haven't, it is a deadline.

Part Three. A Secure Approach to Product Innovation Considers Every Layer of the IoT Value Chain

Relative to the gravity of the threats, the prioritization of security in IoT devices has been disturbingly lax. Companies assume the costs and complexity of having a secure device undermine profitability. Manufacturing partners seek to minimize touch times and find that integrating intricate security components extends production cycles. Consumers have traditionally been driven by price more than security when purchasing an IoT-enabled product.

As security moves to the forefront, the consumer mindset shifts. Research consistently shows that the majority of consumers now factor in the security profile of a device when considering a new purchase, and most are willing to pay a premium to guarantee protection. According to PSA Certified's 2023 Security Report, 65% of consumers look for security credentials when buying connected products, and 69% are willing to pay more for built-in security. As a result, security is now a key driver of commercial value.

For companies, facing this reality head-on means adopting a security approach that builds confidence at each point along the IoT value chain. Security must be integral to product conception and by-design – meaning built into all stages of product development rather than implemented as an afterthought.

A Fully Integrated Design Strategy Unifies the IoT Hardware, Software, and Cloud Services Under a Single Managed Security Umbrella

An IoT initiative that is born secure begins by ensuring that all hardware and software components embedded in the device during manufacturing are of known and secure origin. When product developers address security at every layer of the IoT value chain, they create an impermeable device-and-platform stack that keeps malicious actors at bay.

The complexity of the IoT ecosystem makes placing the security onus on the end user impractical. Even for consumers who care about security in connected devices, relying on them to take all the correct implementation steps assumes they have at least a basic knowledge of IoT security, which is a big ask.

An IoT device built today could remain installed in our homes, businesses, cities, and infrastructure for decades to come. Managing the security lifecycle of IoT products is unique compared to most consumer goods. Because an IoT product lifespan relies on regular software updates and password changes, companies must be able to continue to service large device fleets indefinitely and at scale.

Approaching a new smart product line from a holistic and lifecycle perspective is essential. It only takes one vulnerable point in the network to wreak havoc. Pursuing a security solution that unites the device, the cloud platform, and the mobile app under a common security umbrella is the most secure, and thus the only viable, option.

How Can a Company Benefit by Applying These Principles?

A secure-by-design, tightly integrated IoT platform-as-a-service enables a company to release a secure, connected product to market and manage its lifecycle at scale. When the company that built a family of products continues to secure it during the deployment phase, it streamlines customer interaction and enhances customer service outcomes. It means the careful application of security best practices without compromising user experience.

We have observed that when you protect end-user data and the security solution does not interfere with ease of use, customer call rates and return rates drop by several orders of magnitude compared to less secure smart products.

While it may not be intuitive that the design of a smart refrigerator requires as much security forethought as a military application, the fact is that all devices in the next IoT era should be as secure as possible.

To achieve profitable outcomes, companies must carefully evaluate security solution providers in the market and find one that offers a scalable, off-the-shelf solution. When companies believe they can pursue robust IoT security solutions in-house, they quickly find that the time and labor inputs required to create a truly secure device in today's threat landscape are prohibitive. The decision to build or buy arises at project inception, and underestimating what it takes to secure a device and overestimating internal resources are among the most substantial mistakes a company can make.