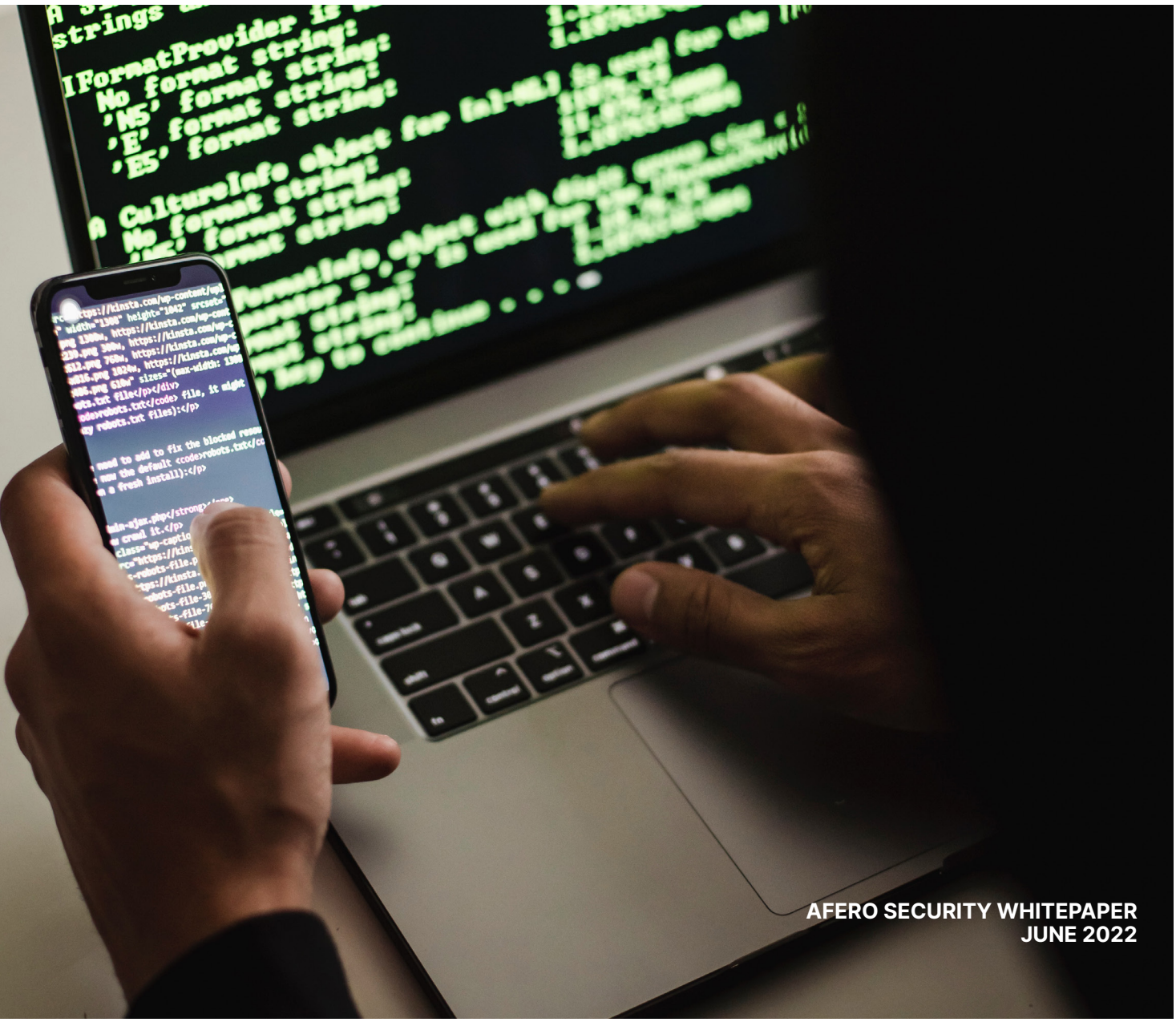
Born Secure

reputation-proof IoT innovation from product conception to market penetration

how a secure connected device + cloud platform requires hardened security at every layer of the IoT ecosystem

afero



AFERO SECURITY WHITEPAPER
JUNE 2022

Executive Summary

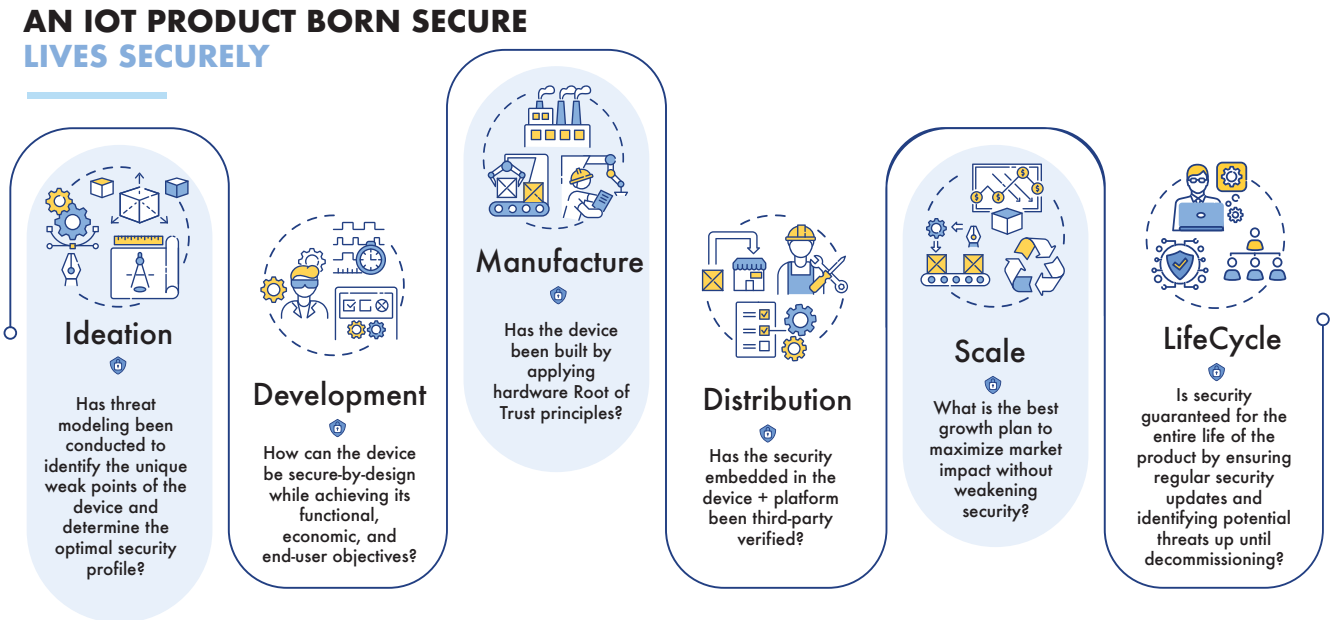
The business imperative for launching a line of IoT products is impossible to ignore – but security concerns often threaten a company's well-laid plans to innovate. While smart devices have been mainstream for more than a decade, the security behind these devices has not demanded the urgency it deserves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

Eseye's **2021 State of IoT Adoption survey** of business leaders in the US and UK pointed out that 36% of companies had reduced their investment plans for IoT in 2021, and 33% have canceled their IoT programs entirely. Similarly, a March 2022 **report** from Meticulous Research expects restrained market growth for the next decade. And in the last quarter of 2021, investment in IoT innovation, as evidenced by the number of patent applications filed, continued a **downward trend** that began in 2020 and has yet to reverse itself.

While there are numerous reasons for the pullback – including the pandemic, chip shortages, and geopolitical disturbances – security concerns top the list. **91%** percent of companies cite security uncertainty – such as the risk of cyberattacks as well as challenges with onboarding and certifying IoT devices – as hindering 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.



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, for instance, that security deficiencies primarily compromise low cost, low criticality products – "but it's just a light bulb!" anyone? 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 enter via the weakest link and navigate laterally throughout the network to reach the 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 if they want 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 .

Sincerely,

Joe Britt
CEO, Afero

Our white paper consists of three parts, each exploring vital security questions in the IoT space today.

part one

The Internet-of-Things (IoT): does the potential outweigh the risk?

- Intensity and scope of IoT ambition depends on a company's unique objectives
- IoT gold rush! Maybe not so fast?

part two

Threat assessment: IoT's near-infinite spread is also its greatest vulnerability

- Reputation catastrophe: been-hacked is the biggest taboo
- The regulatory environment for securing IoT devices is still nascent
- Weapons of mass disruption?

part three

A secure approach to product innovation considers every layer of the IoT value chain

- A fully integrated design strategy unifies the IoT hardware, software, and cloud services under a single managed security umbrella
- How can a company benefit by applying these principles while pursuing its latest IoT product line?

PART one

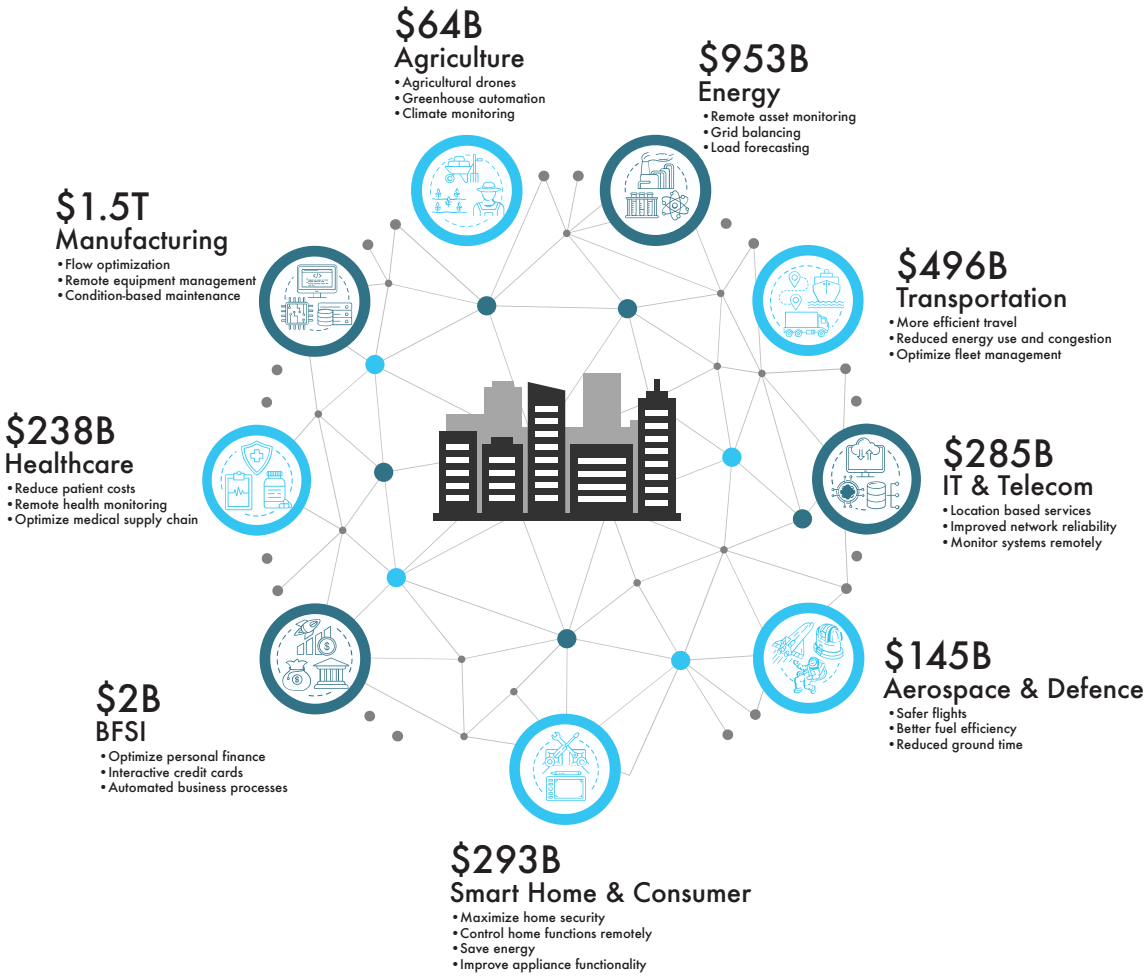
“The Internet of Things (IoT) devoid of comprehensive security management is tantamount to the Internet of Threats.”

STEPHANE NAPPO
Global Chief Information Security Officer, Group SEB

The Internet-of-Things: does the potential outweigh the risk?

You've probably seen the headline numbers: **55.7 billion** connected IoT devices globally by 2026 and **$4.4 trillion** in market value by the end of the decade. But absent from those oft-cited (and oft-revised) figures are the drivers that underlie them; a company needs industry-specific context to evaluate what IoT can enable it to achieve and how those capabilities underpin its future viability.

VALUE OF IOT BY MARKET SECTOR, 2030



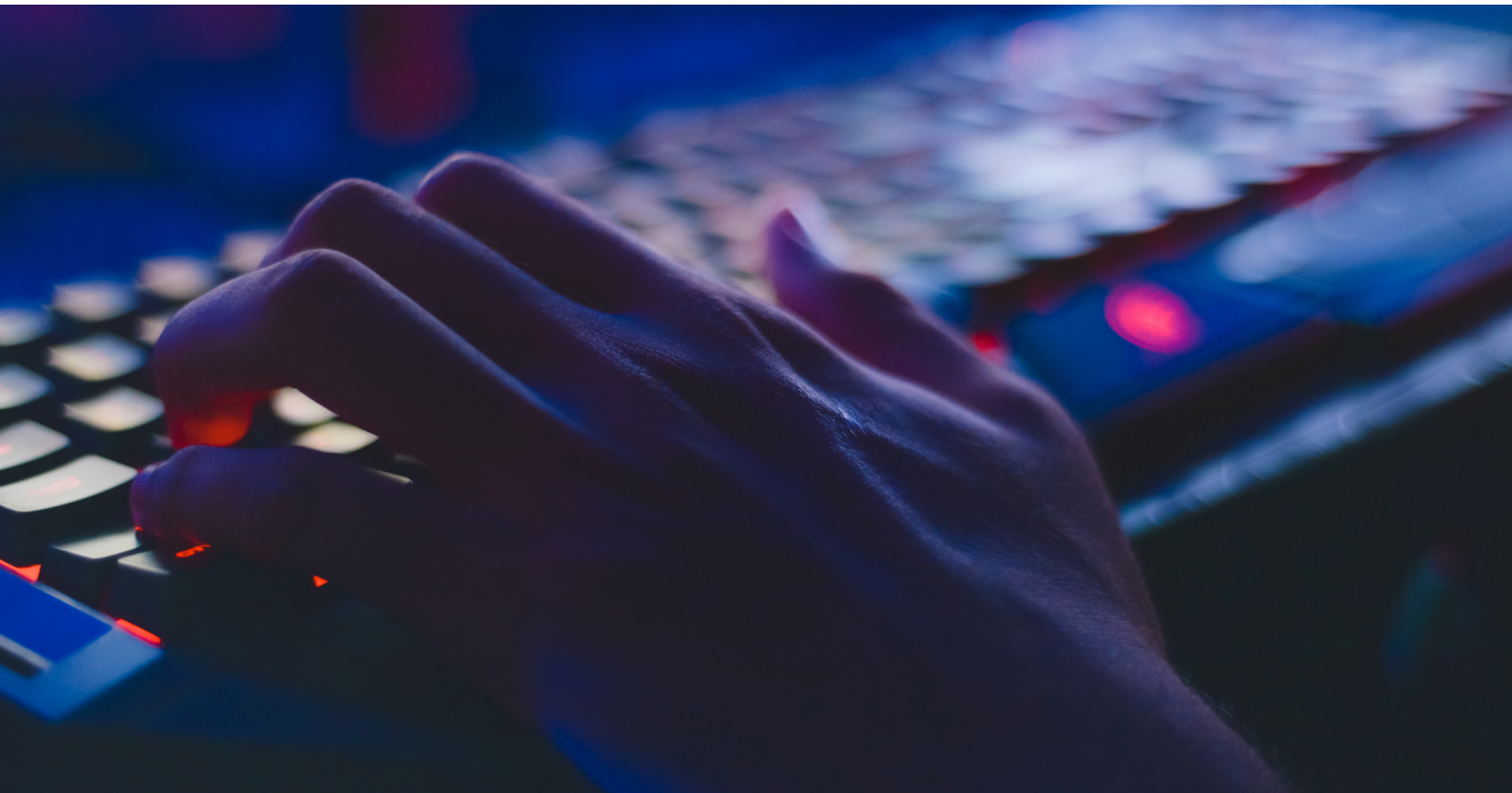
Virtually every company will acknowledge that innovation is essential to competing in today's technologically advanced economy, but that does not mean they all rush out to integrate the latest buzzy tech trend into their flagship products. For some, innovation means improving processes rather than transforming 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.

IoT enables companies to grow profit, enter new markets, and pursue new business lines. Whether it's evolving a well-known product to function in a modern context or introducing the world to an entirely new capability, the immense value potential and competitive necessity of IoT is impossible to ignore.

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, for example, has had four console versions since 1994, each of which offers better functionality and graphics than the last. Toyota has released eleven generations of its bestselling Corolla since 1966, with each generation having improved gas mileage, electronic capabilities, and interiors.



The motive for a business to hop on the IoT bandwagon many times 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 for these reasons – from remote temperature monitoring for vaccines to connected inhalers and heart rate monitors – IoT saves lives.

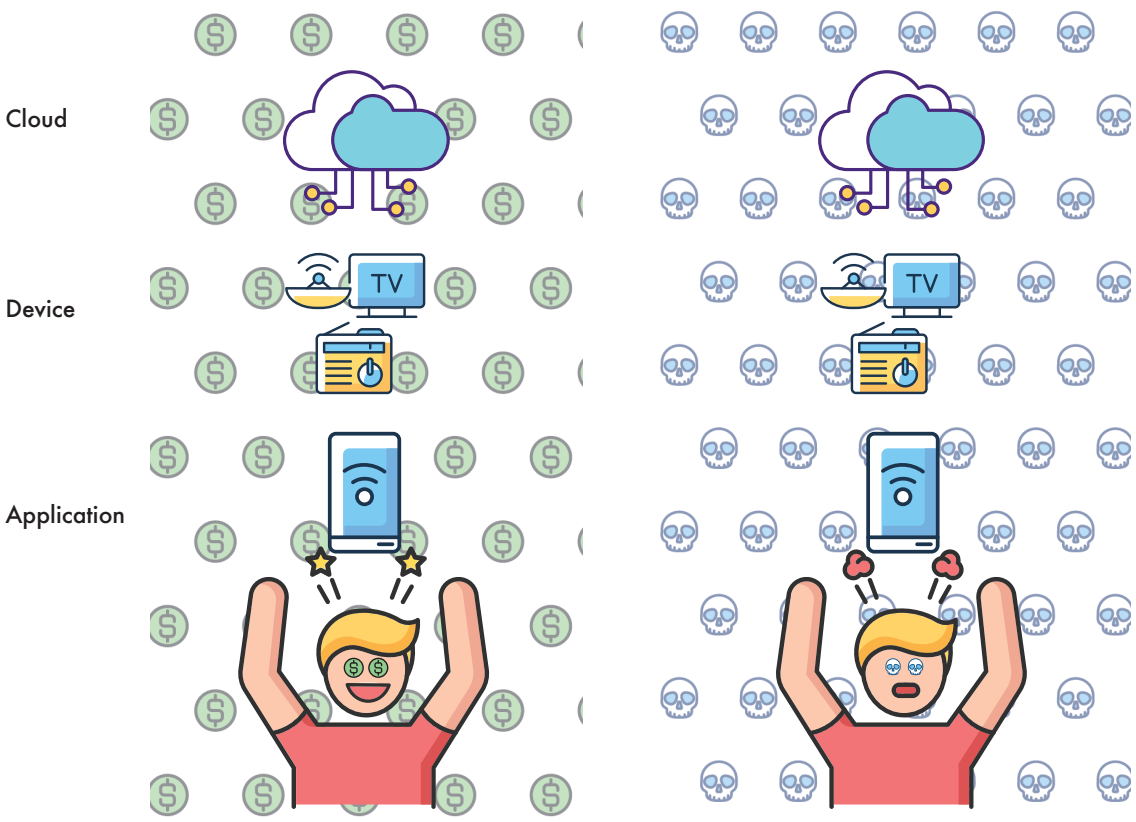
And in manufacturing – estimated to be the biggest market for IoT devices in the coming years – companies are using predictive maintenance, robots, and AI logistics to slash production times and boost efficiency.

While IoT devices qualify as such because of their ability to collect data via sensors, much of IoT innovation happens in the analytics layer – where machine learning and artificial intelligence provide real-time insights for enhanced decision making. In these cases, IoT advancements are the core enabler of a new product beyond just an upgrade of an existing one.

IoT gold rush! Maybe not so fast?

But if all of this IoT market potential exists, how come we notice a concerning shift in business appetite to innovate in the space?

Each layer of the IoT ecosystem presents a new attack surface – and security solutions must address the picture in its entirety.




All Devices
HOME
OFF
living room
ON
Bedroom
ON
Hall
Speaker
Intercom
Heater
Broadcast
Thermostat
Bedroom
Webcams
Control
Scenes
Automation
Settings

PART two

“Hacking the location data on a car is merely an invasion of privacy, whereas hacking the control system of a car is a threat to a life.”

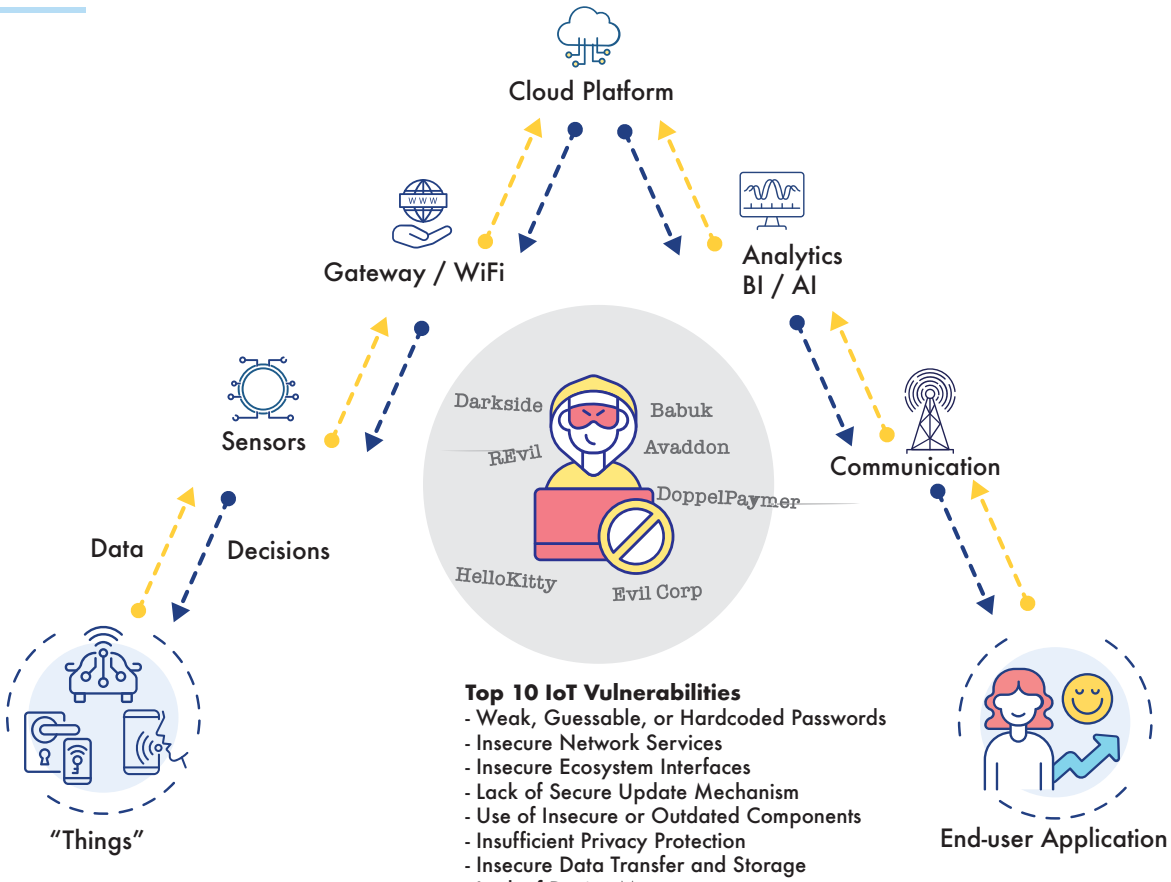
WORLD ECONOMIC FORUM

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 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.

IOT ECOSYSTEM



Top 10 IoT Vulnerabilities
- 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

source: Open Web Application Security Project (OWASP)

Data powers IoT and produces zettabyte of it – more data produced means more data to be compromised.

Perhaps most foundationally, 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 – but can be used to manipulate real-world objects and interrupt our lives in unprecedented ways. It's unpleasant to think about, but the prospect of your car being remotely **hijacked** or your local drinking water supply being **poisoned** are real possibilities when IoT security is weak.

IoT is "things", sensors, applications, communications protocols, and the cloud working in coordination to improve our lives via deep insight and intelligent action. But for 55 billion internet-connected devices to take root, society must have faith in the security of critical systems and the stewardship of their data.

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, sex toys, and the shutting down of an entire city's stoplights. While some of these famous cases involved researchers looking to test product vulnerability to improve security in deployment, others were carried out on live systems by bad actors with malicious intent proving a vulnerability can be hiding just about anywhere.

But what exactly motivates the adversaries? According to **Sectrio Threat Research Labs**, the prized assets hackers seek are business code and customer data that can be monetized and sold on the Dark Web. Another monetary pursuit is disruption, such as locking the data flow of a critical system and demanding a ransom to unlock it. In 2021, nearly half of known attacks on supply chains originated from advanced persistent threat (APT) actors – nation-states or state-sponsored – where espionage plays a key role. On the other hand, independent hackers tend to have more personal motives including revenge and settling scores.

Software, hardware, and firmware of dubious origin evades easy detection

Beyond attacks on deployed systems, there are critical gaps in the IoT product manufacturing process. Adversaries can implant malicious code or counterfeit hardware in the factory setting, thus compromising the device before it even leaves the assembly line, unbeknownst to the company, manufacturing partner, retailer, and most importantly – the end-user. This strategic compromise occurs during software

development and product design, where third-party software and hardware elements are integrated covertly. If a company discovers a weak link in their IoT product once it is already to market, it becomes an arduous task to identify how many devices from their vendors and manufacturing partners may have this same weakness.

Compounding this is the fact that companies managing a fleet of IoT products often lack the inventory expertise needed to properly keep tabs on all active devices connected to the network. This makes identifying and monitoring vulnerable devices especially challenging.

Our deep integration and dependence on a globally distributed supply chain, where manufacturers source IoT parts and components from geographically dispersed suppliers, only magnify these threats.

Reputation catastrophe: been-hacked is the biggest taboo

Organizations are on record revealing how much money security breaches have already cost them. **Hacks** on the US Office of Personnel Management in 2015 cost them $500 million, Equifax in 2017 $700 million, and Epsilon in 2011 a whopping $4 billion! And those are just the direct economic costs measured in shutdowns, business interruption, and remediation.

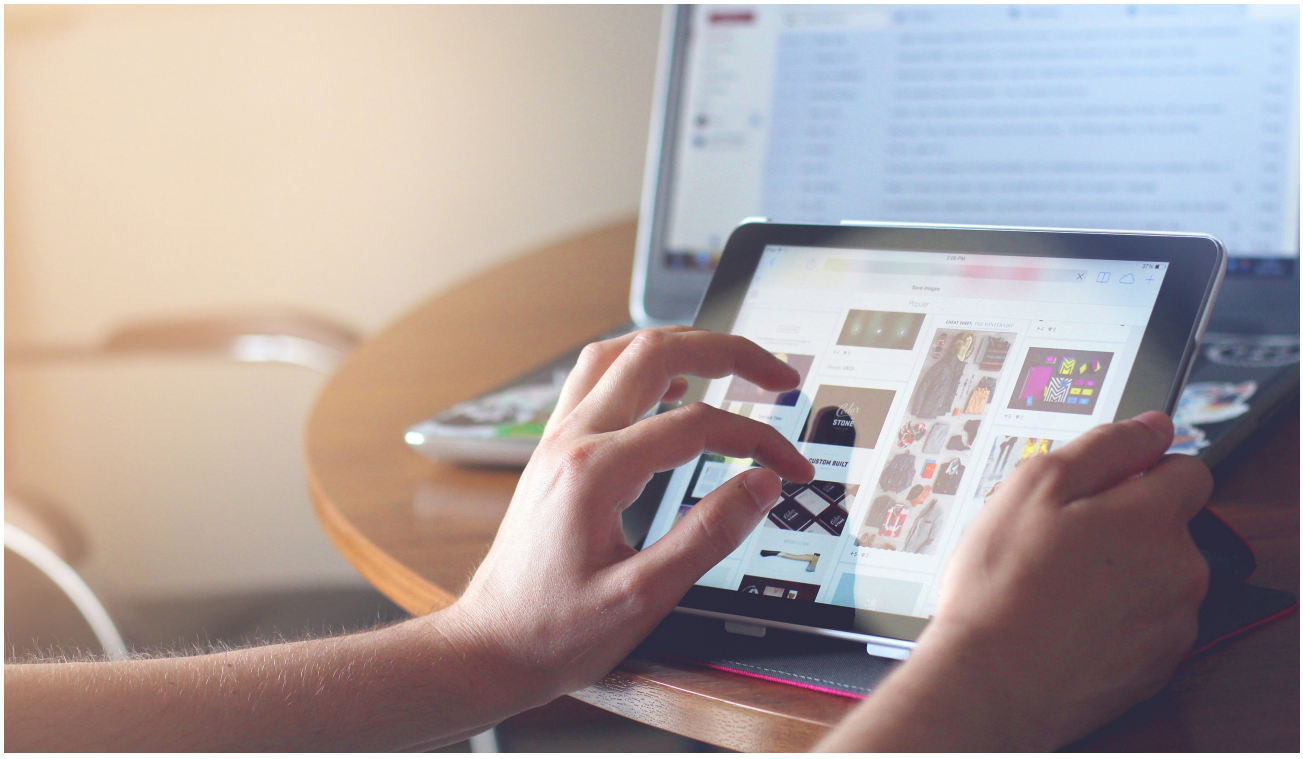
Perhaps more lasting is the cost to reputation when consumers learn a company has been hacked and sever business ties. The damage a hacking event causes to a reputation depends on how much exposure it gets. Hack narratives with national security, human safety, and cutting off essential services as their focal point garner the most attention. It also depends on whether the hack hits a private or public sector institution. People have high expectations from a government entity regarding their data but can boycott a specific company more readily than the former.

In any case, the public does not take data breaches lightly, and **87%** part ways with a company in the aftermath. Surveys have also found that while Millennials had more faith in businesses upon becoming independent consumers, high-profile security breaches have eroded that trust.

A Forbes Insight **report** found that 46% of organizations had suffered reputational damage from a data breach. A **Reputation Risk in the Cyber Age report** from Aon and Pentland Analytics found that some companies lost over 25% of their stock value in the year after a major attack. For small businesses, it gets even worse – **60%** go bankrupt within six months of suffering a data breach or cyber-attack. And if an attack has not hit them yet, they should be on alert – more than **80%** of firms have been victims of hacks.

But when it comes to a more subjective measure like reputation, can the consequences ever be fully quantified? Reputation is essential to give a company life for generations to come. Legendary brands outlast whatever their initial product was by expanding into new business verticals. Take Johnson & Johnson, which started with baby powder in 1894. Yet, by 2022, reins as the top innovator in IoT healthcare as measured by the number of **patents** filed.

The question of reputational damage highlights the Catch-22 companies face. Cost-cutting protects their bottom line in the short term, yet lax security is perhaps the biggest threat to that same bottom line should their worst hackmares materialize.



The regulatory environment for securing IoT devices is still nascent

Well-known and blue-chip companies face higher stakes when entering an emerging segment such as IoT. While start-up renegades often lead the charge on tech innovations and take risks for big payouts, established players jump in only after the viability of something has been proven – via an acquisition or else creating a new product internally. Think cryptocurrencies, which major institutions have only entered ten years after their invention, or the shale boom, pioneered mainly by independents rather than the big oil companies.

The same trends are happening in IoT, which is just coming out of its Wild West era. Despite the massive security risks, there is no globally uniform regulatory framework for IoT at a government level with respect to consumer protection – something that matters to prominent brands. While a wide-impact security breach could happen anywhere, anytime, the onus of IoT security is largely upon the shoulders of individual companies and consumers. And should a more sophisticated regulatory framework arise in the coming years, it will likely shift even more responsibility to companies in the form of tighter compliance rules, fines, and penalties.

PART

three

“As long as companies continue to look at security as a ‘feature’ rather than as a fundamental operating characteristic, they will be unable to cooperate to build proper security infrastructure.”

JENNIFER ZICKERMAN
Entrepreneur (via Pew Research Center)

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. Dark Cubed's latest **The State of IoT Security report** discovered that despite increased awareness among the public, there have not been adequate efforts on the part of retailers to allow only the securest of devices to hit the shelves and that the situation is not improving. Their investigation of consumer IoT products discovered that the earliest stages of the IoT value chain – product development and manufacturing – are rife with security gaps exploited by largely China-connected groups, and that the true origin of IoT product components on store shelves is being intentionally obscured.

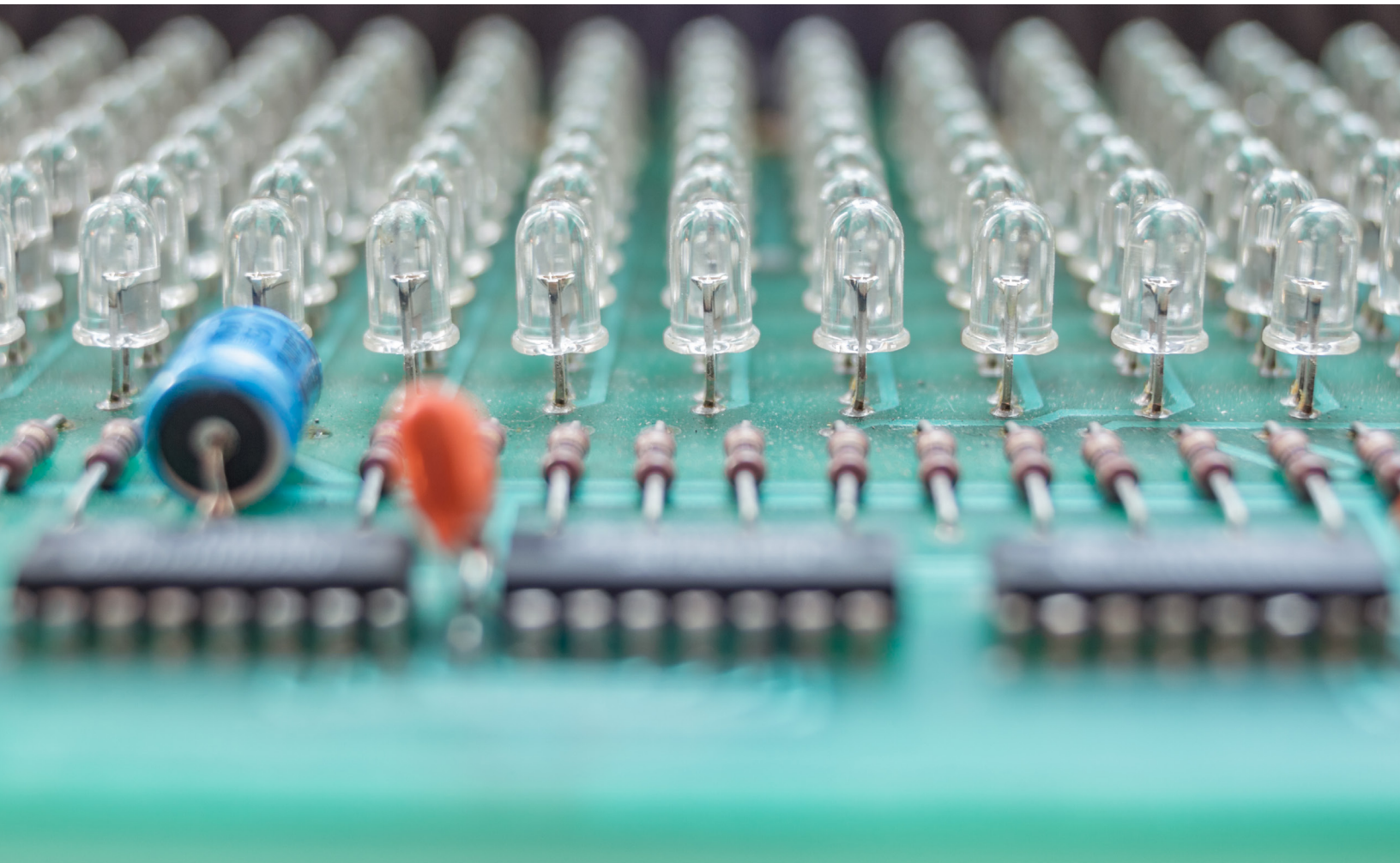
Companies assume the costs and complexity of having a secure device undermine profitability. Manufacturing partners seek to minimize touch times and find that integrating intricate security components extends production cycles. Consumers have traditionally been driven by price more than security when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

As security moves to the forefront, the consumer mindset shifts. According to PSA Certified's **2022 Security Report**, **83%** of today's consumers are now factoring in the security profile of a device when considering a new purchase, and 72% are willing to pay a premium to guarantee protection. 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 an afterthought. Achieving that goes beyond simply attaching an IoT security solution at some point between manufacturing the product and releasing it into the market.

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 + platform that will keep malicious actors at bay.

A fully integrated design strategy unifies the IoT hardware, software, and cloud services under a single managed security umbrella



The complexity of the IoT ecosystem makes putting 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 – a big ask. Too big. This is quite a shift from how we deal with products like laptops and smartphones, where end-users have some role in securing the device.

A deeply interwoven approach (see figure below) solves this problem but is not without critics, as such a tightly woven protocol reduces the flexibility of security options. Buying a product with security inbuilt restricts our ability to install another security option on the device; or have different security options between the device, the cloud platform, and the mobile application. But considering the consequences of a breach and the deep end-user knowledge required to prevent one, the public must be willing to exchange a certain level of configurability for security.

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, where direct interaction with the manufacturer is unnecessary for the long-term functioning of the device. 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.

It is more reasonable for consumers to ally with trustworthy third-party stamps of security approval – reassuring them that a device and associated platform are secure by design but not requiring them to secure it themselves. Many consumer products have components secondary to the headline brand, yet these constituent components are well known. An HP laptop has a sticker indicating an Intel CPU, a Kellog's packaged food may be labeled Non-GMO, and a Chase bank card has a VISA logo denoting the payment processor when a customer swipes.

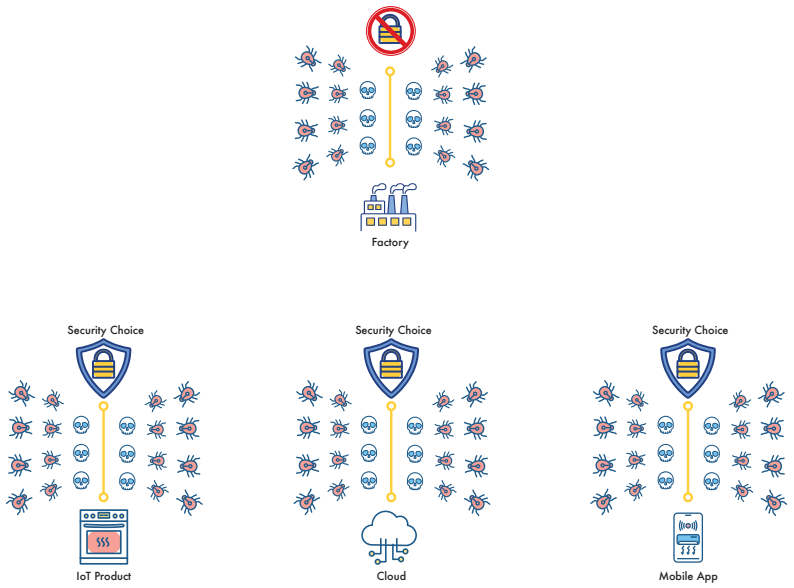
Consumers discover further information about their products via these labels on products, so it is likely the same will develop with IoT device security. A trusted third-party regulatory body to evaluate and certify devices and platforms will be instrumental in formalizing this trend. And

"Most IoT devices that lack security by design simply pass the security responsibility to the consumer, thus, treating the customers as techno-crash test dummies."

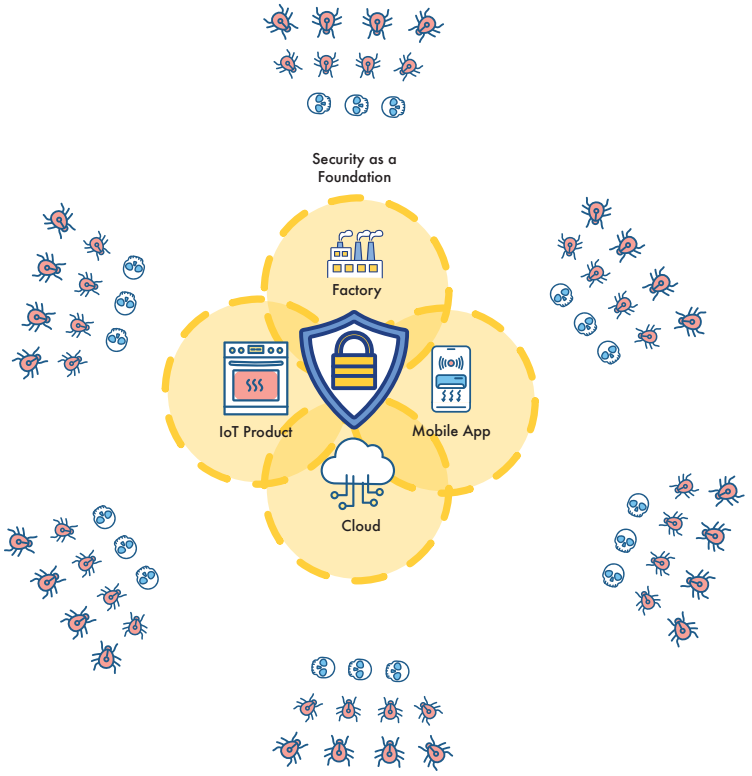
JAMES SCOTT
Senior Fellow, Institute for Critical Infrastructure Technology

A NEW PARADIGM FOR SECURE IOT PRODUCT DEVELOPMENT

CURRENT = VULNERABLE



FUTURE = IMPENETRABLE



for companies, it means choosing security solutions that meet rigid third-party requirements.

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 while pursuing its latest IoT product line?

A secure-by-design and tightly integrated IoT platform-as-a-service allows a company to release a secure connected product into the 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.

Some recommend that certain products have different security levels and that you should assign varying risk profiles. Considering the threat landscape and reputational risk, security providers are moving closer to a reality that there is no room for low-level security protocols.

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

Of course, cost will continue to be a flashpoint. Creating a highly secure IoT product requires more planning, expertise, and financial resources than producing a less secure version. While security is quickly moving into the must-have rather than would-be-nice category, product developers will be taking a closer look at how highly secure can coexist with healthy profit margins.

To achieve profitable outcomes, companies must carefully evaluate security solution providers on the market and find one that can provide a scalable off-the-shelf solution. It must be a close fit with the product in question.

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 the time of project inception, and underestimating what it takes to secure a device and overestimating internal resources is one of the most substantial mistakes a company can make.

About Afero

Afero is the ultimate sensor-to-cloud #IoT platform. Manufacturers report 3x faster time to market, 10x more attach rates, and 99% fewer escalations. Engineers love the robustness of the Afero service that allows them to re-use 90% of their work from project to project. End-users appreciate how easy it is to get their device connected and how reliable and responsive their device operates.

afero.io