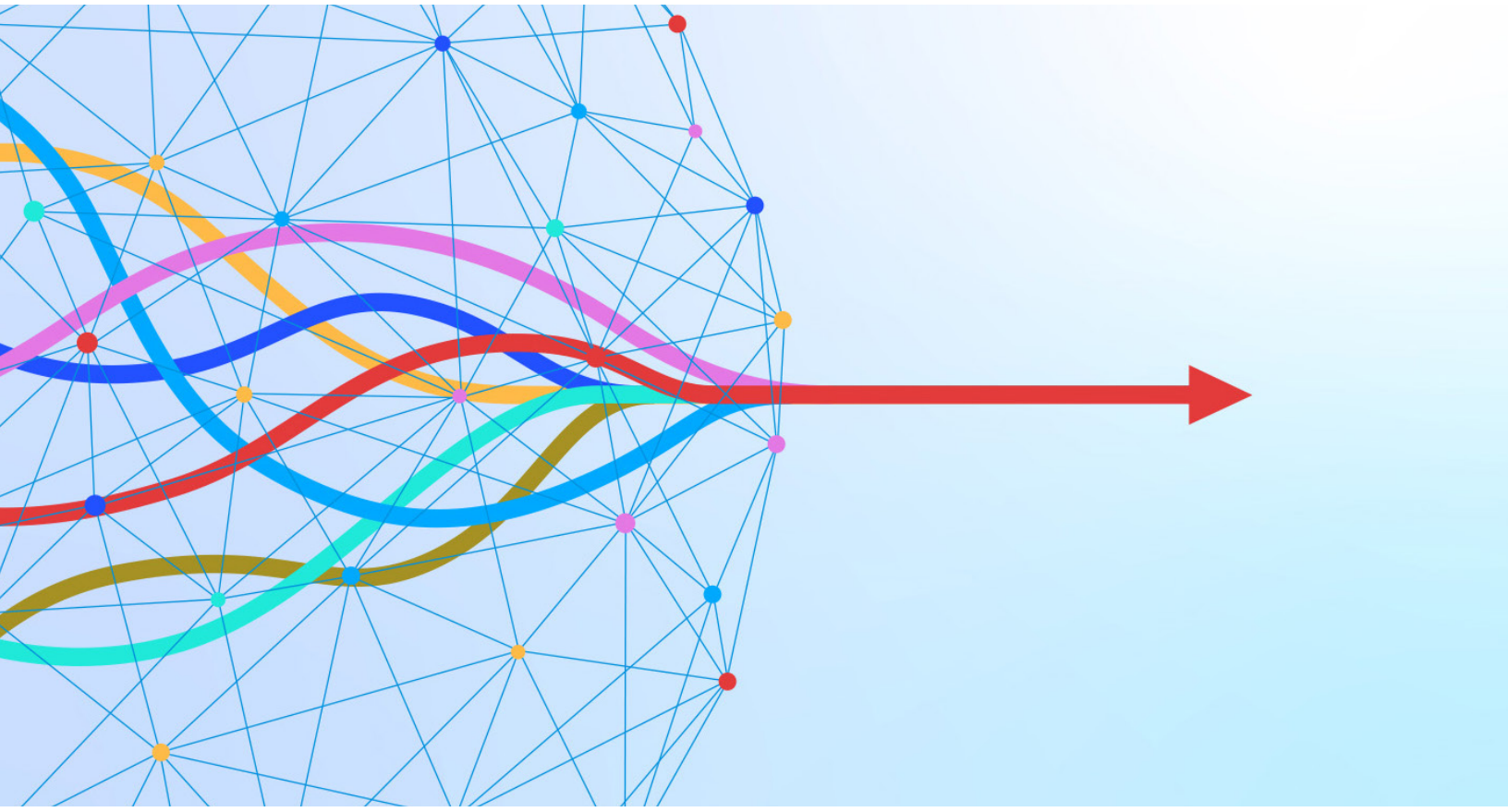
McKinsey & Company

Technology, Media & Telecommunications Practice

Cybersecurity for the IoT: How trust can unlock value

For today's fragmented Internet of Things (IoT) to reach its potential as a fully interconnected ecosystem, the answer may lie in the convergence of cybersecurity and the IoT.

by Jeffrey Caso, Zina Cole, Mark Patel, and Wendy Zhu



April 2023

The Internet of Things (IoT) poses dramatic possibilities for transforming work and everyday life. The IoT, in plain terms, is the intersection of the physical and digital world, with devices of all kinds harnessing the power of interconnectivity to provide seamless experiences for consumers and businesses alike.

At the moment, however, the IoT is at a crossroads. Will it continue to provide incremental value amid siloed clusters, or will it unlock massive value as a fully interconnected IoT ecosystem? That "unlock"—and thus the answer to that question—depends on the transition to a truly integrated IoT network within and across industry verticals.

Core obstacles must be confronted to achieve such a network. Chief among them is cybersecurity risk, which stands in the way of the trust needed to integrate IoT applications and networks. The solution lies in the convergence of the IoT and cybersecurity—the *combination of any technical, functional, or commercial element of the IoT with cybersecurity* to form a new, integrated whole. We shouldn't understate how significant this breakthrough could be for key applications (such as automobiles, healthcare, and smart cities).

This article explores the nature of that convergence, the opportunities it will offer, and the challenges involved in achieving it. Providers of integrated solutions can engage in transformative adaptations to consolidate today's fragmented IoT and cybersecurity ecosystem. With strategies and partnerships aimed at the convergence of the IoT and cybersecurity, industry and consumers alike can realize the remarkable possibilities that lie ahead.[1]

The IoT and cybersecurity landscape

A question commonly asked by technology leaders across the globe: What are the key factors inhibiting wide-scale IoT adoption today? Driven by our hypothesis that the convergence of the IoT and cybersecurity can unlock a massive amount of new value, we explored the IoT landscape to understand better the obstacles to broad IoT adoption and how they might be overcome.[2]

Across industry verticals, applications of the IoT continue to expand, and a shift has occurred from clusters of siloed IoT devices to interconnected IoT environments. This is especially apparent in settings such as factory floors and automotive vehicles. However, the IoT hasn't yet scaled as quickly as expected, and the IoT industry hasn't achieved a genuinely seamless experience in which devices pass into and out of physical environments and are identified, trusted, and managed without a need for separate (and at times manual) authentication steps.

The proliferation of connected devices, along with the advancement of the complexity in IoT use cases (such as autonomous systems and transportation), creates opportunities for multiple players of the value chain. But it also creates the risk of vulnerabilities that could have catastrophic consequences. The risk profiles of many IoT systems are elevated compared with that of enterprise IT, given the IoT's control over physical operations. A seamless IoT experience, therefore, requires a foundation in digital trust, functional convergence of the IoT and cybersecurity, and an early-stage integration of cybersecurity in the architecture design and pilot phase.

Traditional approaches to security in the IoT don't support this secure, seamless experience.

[1] For more, see Michael Chui, Mark Collins, and Mark Patel, "IoT value set to accelerate through 2030: Where and how to capture it," McKinsey, November 9, 2021; "A manufacturer's guide to scaling Industrial IoT," McKinsey, February 5, 2021; "Smart cities: Digital solutions for a more livable future," McKinsey Global Institute, June 5, 2018; and Bharath Aiyer, Jeffrey Caso, and Marc Sorel, "The unsolved opportunities for cybersecurity providers," McKinsey, January 5, 2022.

[2] Unless otherwise specified, the information in this article comes from analysis of public and internal data and of results from the McKinsey B2B Internet of Things (IoT) Survey. During the third quarter of 2022, the survey was in the field and garnered responses from 208 industry executives at major IoT and cybersecurity solution providers (approximately 40 percent of participants) and from key industry buyers at eleven industry verticals (approximately 60 percent of participants). Approximately 70 percent of the participants were from North America, and approximately 30 percent were from the European Union.

IoT buyers report that there is little multilayered security embedded in today's IoT solution designs. This leads to vulnerabilities that in turn require regular over-the-air updates and patches, which can't be reliably implemented. Relative to enterprise IT, solution design in the IoT space lags behind in security assurance, testing, and verification.

We tested our hypothesis around the importance of cybersecurity and IoT convergence with industry leaders and uncovered another important finding. There is a wide mindset gap between IoT buyers and providers regarding expected IoT adoption, digital privacy, and trust concerns, and the delay caused by siloed decision-making leads. Knowing some of these facts should help future technology leaders on both the buyer and provider sides understand the others' mindsets and move toward unlocking the value.

IoT buyers tell us they are less optimistic than IoT solution providers about achieving a seamless experience soon. They are encountering hurdles even during the early stages of IoT implementation. Their main concerns are around interoperability, cybersecurity, and installation complexities.

IoT solution providers heavily underestimate the importance of digital trust in comparison with buyers; only about 30 percent of providers consider digital trust to be critical in IoT solutions, compared with approximately 60 percent of buyers who view it as such. But IoT buyers need more cohesive decision-making structures to address their cybersecurity concerns. Most providers blame siloed decision making between the IoT and cybersecurity groups on the buyer end for delays in IoT adoption—81 percent of providers hold that perspective. Conversely, only 42 percent of buyers believe the decisions are siloed.

From these insights, we conclude that it will take a significant shift in the philosophy of IoT solution design, along with a holistic convergence of IoT and cybersecurity functionalities, to build user confidence in the IoT, speed up its adoption, and drive new value across its verticals—thus creating a fully interconnected IoT environment. These market forces are further supported by increased policy making at both the public and private levels. Technology leaders who grasp the required mindset will be able to influence disruptive change for both consumer and enterprise applications.

When the industry can converge the IoT and cybersecurity, the reward could be enormous. By 2030, the IoT suppliers' market is expected to reach approximately $500 billion in a baseline scenario. In a scenario in which cybersecurity concern is completely managed, executives would increase spend on the IoT by an average of 20 to 40 percent. Moreover, an additional five to ten percentage points of value for IoT suppliers could be unlocked from new and emerging use cases. This implies that the combined total addressable market (TAM) value across industries for IoT suppliers could reach in the range of $625 billion to $750 billion.

What stands in the way? It's highly challenging to manage IoT cybersecurity because the converged solutions need to be either vertical or use case specific and to include a cross-tech stack layer. Success will hinge on various stakeholders acknowledging the challenges, committing to innovation, and agreeing on industrial standards. Testing and validating the solutions also takes time. Additionally, there is an urgent need for industry talent with expertise in both the IoT and cybersecurity, and there is already a global cybersecurity talent shortage. Moreover, embedding IoT skill sets within cybersecurity is an emerging discipline.

However, there are reasons for optimism. Leaders in the IoT and cybersecurity sectors are increasingly aware of the challenges and actively considering solutions. Top cloud providers (such as Amazon Web Services, Google, and Microsoft) have stepped up their approaches to IoT security. Semiconductor players (such as Intel and Qualcomm Technologies), whose products power key IoT devices and networks, now prioritize security in their IoT architectures and hardware. Pure-play IoT technology providers (such as Cisco Systems and

Samsara) recognize the importance of security and offer distinct IoT security offerings. Finally, a few companies (such as BlackBerry and Siemens) sit at the intersection of cybersecurity and the IoT and are well positioned to marry enterprise cybersecurity solutions with IoT platforms.

McKinsey has been surveying companies and decision makers around the world on the topic of the IoT, as well as actively participating in discussions about its potential and challenges, for close to a decade. The firm's experts have sought to understand the transformational value of connecting the physical and digital worlds—the plumbing of which is the IoT. This work has repeatedly led us to the conclusion, shared by many global technology leaders, that enormous value can be realized when broad societal benefit, utility, and productivity are taken into account. We believe that the full potential by 2030 could be between $5.5 trillion and $12.6 trillion.

We have put significant recent effort into understanding today's obstacles and potential solutions for a truly seamless experience that enables the next generation of the IoT. Some of our conclusions are that security and trust have become increasingly prominent inhibitors, yet the solutions that bring together enterprise security and the IoT remain nascent. This has led us to investigate how the answer may lie in the intersection of cybersecurity and the IoT to serve as the driver for IoT adoption. The findings on this question have been significant and, in some cases, surprising.

The IoT future: Seamless industrial and consumer experience

Imagine the seamless Internet of Things experience of the future, merging different industries, technologies, and use cases. A car is more than a means of transportation—it's a vehicle of the broader digital experience. You request a shared car through a portal using touchless facial recognition. The car drives itself to you, with its interior personalized to your preferences. Its communication devices seamlessly integrate your digital accounts. On your morning commute, the car syncs with your wellness tracker to determine which breakfast to order and pick up. You enjoy your meal while your digital assistant alerts the office of your arrival and adjusts your cubicle temperature.

Turning this vision into reality one day requires overcoming several factors currently inhibiting faster IoT adoption and growth; chief among them is cybersecurity risk. Only by seriously addressing this issue with a new, holistic approach can the market maximize the value enabled by this and many other advanced IoT use cases.

IoT market adoption and key drivers

IoT adoption has accelerated in recent years, shifting from *millions of siloed IoT clusters* made up of a collection of interacting, smart devices to a *fully interconnected IoT environment*. This shift is happening within industry verticals and across industry boundaries. By 2025, the IoT suppliers' market is expected to reach $300 billion, with 8 percent CAGR from 2020 to 2025 and 11 percent CAGR from 2025 to 2030.

The future IoT environment will consist of billions of connected devices communicating through heterogenous operating systems, networks, and platforms, increasingly through cloud-based data storage and cloud-native programming. This environment should empower constant information exchange with a high level of autonomy and, in turn, enable designers and engineers of IoT solutions to create a seamless experience, which IoT technology providers, integrators, and customers have recently started to advocate for.

The ability to develop seamless experiences will likely spur further adoption of the IoT, as it helps address critical factors such as confidentiality, connectivity performance, cybersecurity, installation, interoperability, privacy, and technology performance (see sidebar "Key factors for a seamless IoT experience"). In the McKinsey B2B IoT Survey, more than 90 percent of surveyed IoT solution suppliers and buyers cite at least one of those issues as a key reason for decelerating

Key factors for a seamless IoT experience

A seamless Internet of Things (IoT) experience will consist of six components that span enterprise and consumer use cases:

- *Hyperconnected.* Connectivity through multiple standards will be pervasive, connecting a vast number of devices and sensors that seamlessly share data.
- *Integrated.* Integration within and across tech stacks of devices will be effortless (including minimized sign-in effort, self-managed devices, and over-the-air patch updates), with simultaneous use of multiple connectivity standards, platforms, and back-end systems.
- *Secure and trusted.* Dynamic cybersecurity will enable a high degree of trust in handling the multilayered complexity of legacy systems and new solutions, with security enabled through AI-based threat protection at all layers.
- *Intelligent.* Devices and systems will have the intelligence (enabled by AI and machine learning) to draw insights from data and make real-time decisions, allowing the leap from monitored to automated implementation.
- *Mobile.* Devices and networks will require minimal maintenance, be battery efficient, and have a persona (corporate or personal identity) to allow for futuristic experiences.
- *Hyperpersonalized.* There will be personalized experiences across different platforms and scenarios (from home to office and everywhere in between), enabled by the other factors.

IoT adoption. Interoperability and cybersecurity occupied the top two spots. Interoperability is an essential ingredient, given the need for multiple interconnected systems; common standards across the IoT value chain would bolster it. Cybersecurity is just as critical but an even bigger challenge.

The pivotal role of cybersecurity

Survey respondents across all industries cite cybersecurity deficiencies as a major impediment to IoT adoption (Exhibit 1). Roughly 30 percent of participants name cybersecurity risk as their top concern. Of these respondents, 40 percent indicate that they would increase the IoT budget and deployment by 25 percent or more if cybersecurity concerns were resolved.

Cybersecurity risk multiplies due to the interconnectedness of IT and operational technology within the IoT, especially in use cases that involve the transmission of critical data or the operation of critical business processes. Per McKinsey research in 2021, more than 10 percent annual growth in the number of interconnected IoT devices leads to higher vulnerability from cyberattacks, data breaches, and mistrust.[3] According to the McKinsey B2B IoT Survey, IoT application software and human–machine interfaces are the most vulnerable layers of the IoT stack.

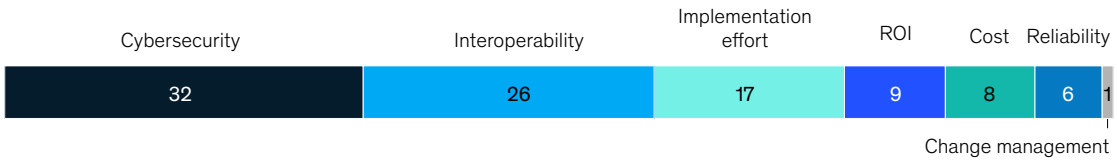
Both the frequency and severity of IoT-related cyberattacks are expected to increase.[4] Without

[3] Michael Chui, Mark Collins, and Mark Patel, "IoT value set to accelerate through 2030: Where and how to capture it," McKinsey, November 9, 2021.
[4] For more, see Bharath Aiyer, Jeffrey Caso, Peter Russell, and Marc Sorel, "New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers," McKinsey, October 27, 2022.

Exhibit 1

Enterprise buyers rate cybersecurity as the biggest obstacle to B2B Internet of Things adoption and spending.

Top impediment to Internet of Things adoption, % of respondents



Note: Figures do not sum to 100%, because of rounding.
Source: McKinsey B2B Internet of Things Survey, 117 buyers, Q3 2022

McKinsey & Company

effective IoT cybersecurity, this heightened risk may prevent organizations from taking their IoT deployments from pilot, in which risk is localized, to production, in which risk is amplified because of the expanded scale.

Up to now, achieving a trusted level of IoT cybersecurity has been difficult. Most participants in the space have tended to treat cybersecurity as a separate software category, providing bolt-on solutions rather than making it a core, integral part of the IoT design process. The interconnected nature of the IoT means that the approach has to change to a comprehensive one that includes all five functionalities defined by the National Institute of Standards and Technology: identification of risks, protection against attacks, detection of breaches, response to attacks, and recovery from attacks.

The current IoT infrastructure could have security gaps along the entire value chain. For example, cybersecurity testing might be limited in scope during the design stage or occur too late in the design process. As a result, security might not be sufficiently embedded, leading to potential gaps in the production stage. An IoT device's upgradability would then be reliant on patches, and the device may struggle to stay up to date with the most recent security regulations and certifications.

Ideally, IoT-specific certification and standards will one day ensure that security is embedded, leading people to trust IoT devices and authorize machines to operate more autonomously. Given the differences in requirements of various use cases and industrial verticals, the future of cybersecurity in the IoT will likely feature a combination of traditional and bespoke tooling, as well as security-centric product design.

Traditionally, cybersecurity for enterprise IT has focused on confidentiality and integrity, while cybersecurity for operational technology has focused on availability. Our research suggests that the IoT requires a more holistic approach. Since cybersecurity risk for the IoT spans digital security to physical security, it's essential to address the entire confidentiality, integrity, and availability (CIA) framework. Six key outcomes enable a secure IoT environment: data privacy and access under confidentiality, reliability and compliance under integrity, and uptime and resilience under availability (see sidebar "Expanding the cyber-risk framework for the IoT").

Expanding the cyber-risk framework for the IoT

Confidentiality, integrity, and availability make up a well-known enterprise framework for assessing cyber-risk impact:

- *Confidentiality.* Only authorized endpoints or users have access.
- *Integrity.* Data are transferred as expected—complete and unaltered.
- *Availability.* Data and system functionality meet user demand and expectations.

The framework can be expanded to six dimensions in Internet of Things (IoT) environments, capturing the unique risks and concerns to ensure IoT security—especially those around safety in operational environments (exhibit):

- *Confidentiality: privacy and access.* As the IoT is adopted in highly regulated industries (such as healthcare), the data flowing through the IoT tech stack should be handled with the highest degree of protection, with uninterrupted access for authorized users.
- *Integrity: reliability and compliance.* As the IoT optimizes processes—and eventually, autonomously controls them—users should trust that the data flowing throughout the IoT tech stack are accurate, relevant, and unadulterated. As cybersecurity regulation for the IoT evolves, users should trust that IoT systems are compliant with and have automatically adapted to the latest regulations.
- *Availability: uptime and resilience.* For the IoT to make the transition from being used for open-loop systems to being used for closed-loop systems, users shouldn't need to worry about any operational disruptions. Also, in IoT use cases for which humans are in the loop, cybersecurity should be capable of guaranteeing fail-safe mechanisms.

Exhibit

Expanding an enterprise cyber-risk framework to six dimensions can offer a more holistic security approach in Internet of Things environments.

Confidentiality, integrity, and availability framework

McKinsey & Company

Massive value at stake: Variations by industry

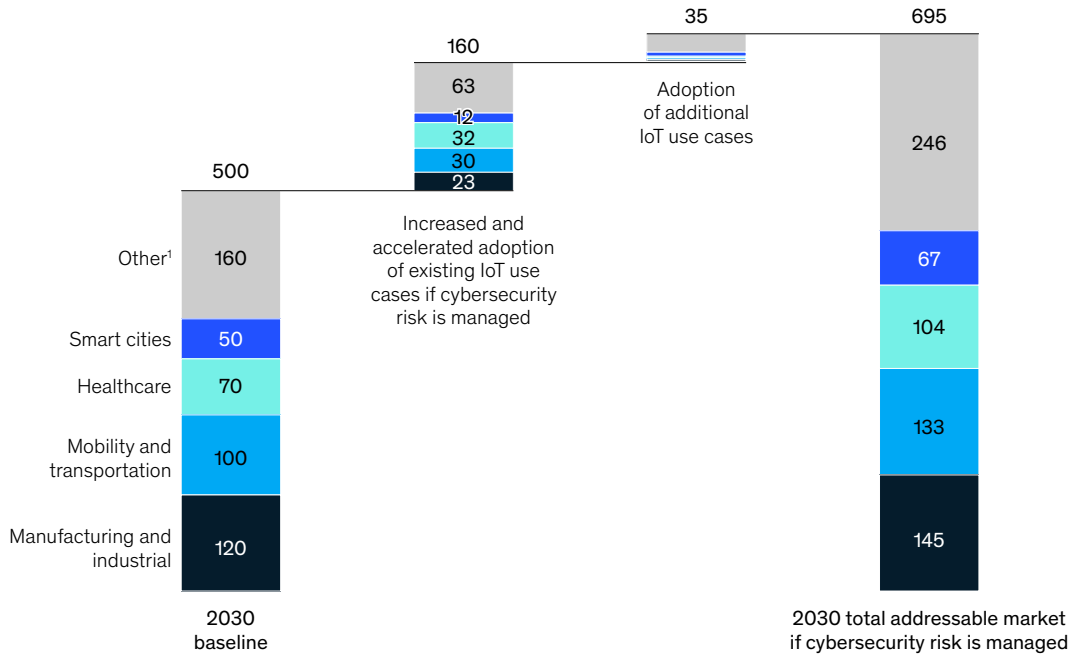
Although a baseline cybersecurity functionality is inherent to all IoT industrial verticals and use cases (such as avoidance of unauthorized access), the specific cybersecurity risks that each industry is addressing may vary by use case. For example, cybersecurity in remote patient monitoring in healthcare needs to prioritize confidentiality and availability, while the most important cybersecurity outcome in autonomous vehicles is availability, as operational disruptions could lead to safety hazards. Contactless payments for financial services depend heavily on data integrity.

In a 2030 baseline scenario, the TAM value for IoT suppliers across industries is $500 billion (Exhibit 2). The largest four industry verticals—manufacturing and industrial, mobility and transportation, healthcare, and smart cities—make up more than 65 percent of this total market. If cybersecurity risk were adequately managed, executives would spend an average of 20 to 40 percent more, amounting to $100 billion to

Exhibit 2

While B2B Internet of Things value capture is expected to grow across sectors, more effective cyber practices can increase use-case adoption.

Estimated 2030 Internet of Things (IoT) suppliers' value capture with improved cybersecurity, $ billion



Note: Figures may not sum to 100%, because of rounding.
[1]Logistics, oil and gas, retail, smart homes, smart offices (enterprise and IT), and utilities.
Source: McKinsey B2B Internet of Things Survey, 208 participants (117 buyers and 91 providers), Q3 2022; McKinsey analysis

McKinsey & Company

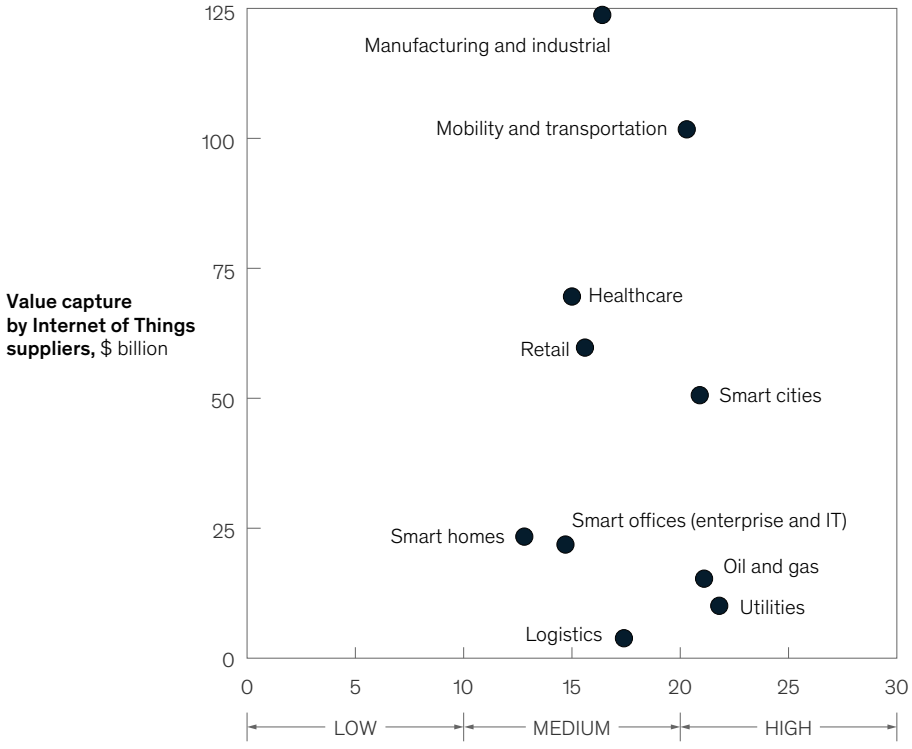
$200 billion, in aggregate, on the IoT. Heightened levels of cybersecurity not only result in increased TAM for existing use cases but also create an environment for new and emerging use cases to thrive. As a result, there would be an estimated five to ten percentage points of additional value for IoT suppliers, equating to $25 billion to $50 billion. This implies a combined TAM value of $625 billion to $750 billion across industries for IoT suppliers.

Cybersecurity efforts can benefit all industries, but some are poised to tap the most IoT value (Exhibits 3 and 4). The industries with the highest cyber risk also have the highest value to be unlocked through improved cybersecurity practices. In a scenario in which cybersecurity risk is effectively addressed, manufacturing and industrial, healthcare, mobility and transportation, and smart-city sectors would have the highest additional spending on IoT applications. This article focuses on the latter three verticals, as industrial IoT has been discussed in

Exhibit 3

Improved Internet of Things security practices offer the greatest potential value to many of the sectors with the highest cyber risk.

Baseline 2030 Internet of Things value capture and cybersecurity risk score, by use case



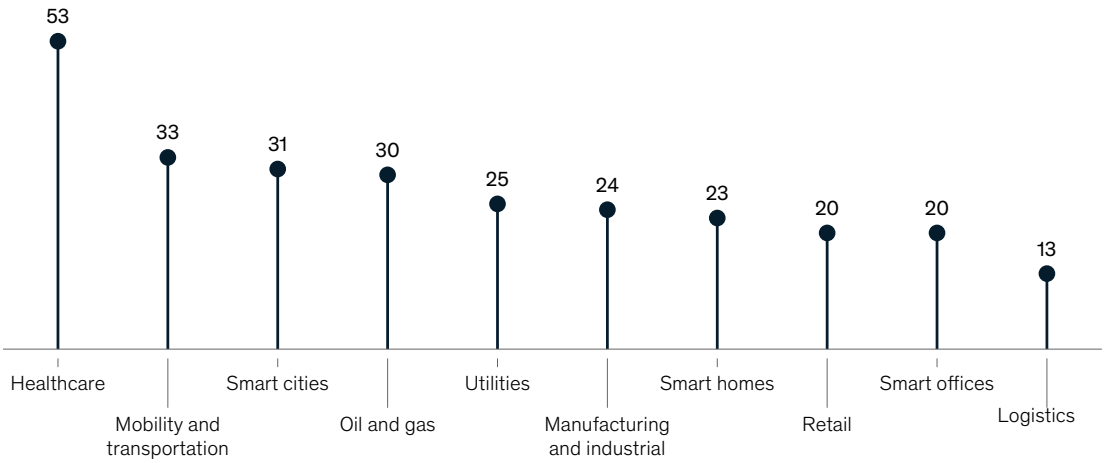
Source: McKinsey B2B Internet of Things Survey, 117 buyers, Q3 2022; McKinsey analysis

McKinsey & Company

Exhibit 4

Increased cybersecurity can help all industries grow, but certain industries are poised to unlock the most Internet of Things value.

Average increase in Internet of Things spending if cybersecurity risk is managed, by use case, %



Source: McKinsey B2B Internet of Things Survey, 208 participants (117 buyers and 91 providers), Q3 2022; McKinsey analysis

McKinsey & Company

multiple McKinsey articles.[5] Based on the CIA cybersecurity criteria, each of these three sectors requires a different cybersecurity focus.

The limits of today's IoT ecosystem

In the current, fragmented IoT ecosystem, providers sell customized IoT systems to industrial buyers. These systems feature IoT devices with embedded cybersecurity but don't contain holistic cybersecurity functionality to protect the entire IoT value chain. Each IoT provider only has control over the protection of its systems and doesn't play a role in the integration of its system with those from other providers.

As a result, IoT buyers take on the enormous responsibility of protecting the IoT value chain. They typically do so by partnering with cybersecurity vendors to provide add-on solutions. These tend to be enterprise-wide cybersecurity solutions rather than IoT-specific products, with additional security features bolted on later as needed.

Mind the gap: Disconnects exist between buyers and providers

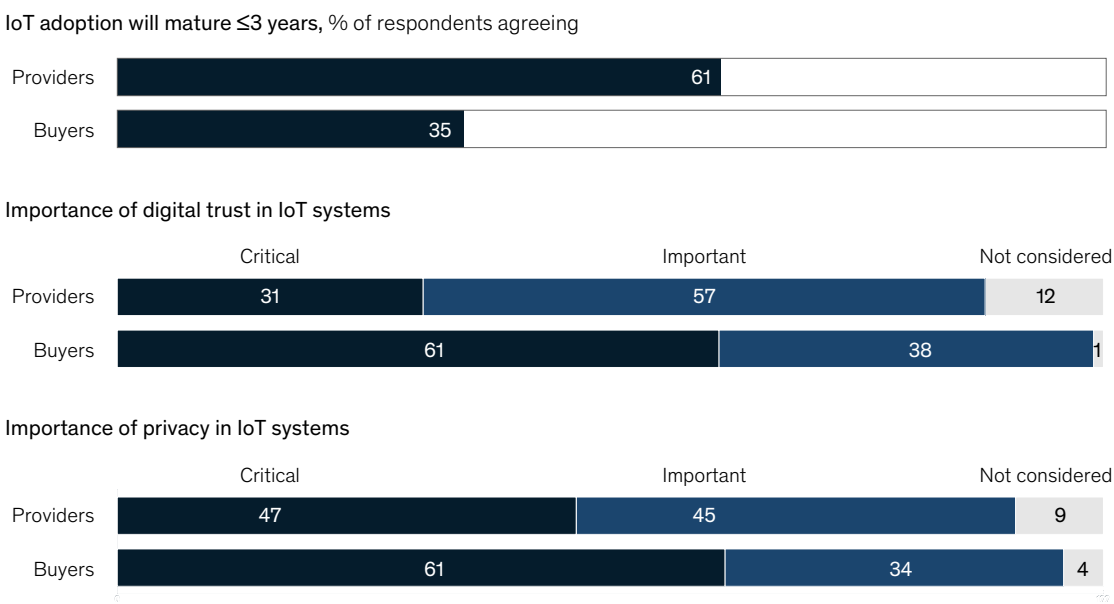
IoT buyers and providers hold differing views on a variety of critical issues, including the expected pace of IoT adoption, concern about digital trust and privacy for IoT solutions, and the degree to which siloed decision making leads to IoT delays (Exhibit 5):

[5] For more, see "A manufacturer's guide to scaling Industrial IoT," McKinsey, February 5, 2021, and Francisco Betti, Enno de Boer, and Yves Giraud, "Industry's fast-mover advantage: Enterprise value from digital factories," McKinsey, January 10, 2020.

Exhibit 5

Internet of Things buyers' and providers' views on issues like adoption pace, digital trust, and decision making diverge, likely hampering market growth.

Internet of Things (IoT) sentiment, % of respondents



Note: Figures may not sum to 100%, because of rounding.
Source: McKinsey B2B Internet of Things Survey, 208 participants (117 buyers and 91 providers), Q3 2022

McKinsey & Company

— *IoT buyers are more conservative than providers on the speed of IoT adoption.* According to the B2B IoT Survey, this could be explained by the interoperability, integration, and cybersecurity challenges that buyers have wrestled with as they scale their IoT efforts.

— *Digital trust and privacy factor more in purchase decisions than providers realize.* Of IoT buyers in the survey, 61 percent rank digital trust as a critical element of their purchase decision, while only 31 percent of IoT providers rank it as a critical element in their system design. Likewise for privacy: 61 percent of IoT buyers deem it critical, compared with 47 percent of providers.

— *IoT providers consider siloed decision making in industrial verticals to be a larger obstacle than buyers do.* More than 80 percent of surveyed IoT providers express the view that siloed decision making between IoT and

cybersecurity leaders on the buyer end is to blame for delayed IoT adoption. Conversely, only 42 percent of buyers share that view. Providers cite complex approval processes for cross-functional decisions and a lack of understanding of the risks and opportunities at the ground level as other bottlenecks hindering IoT adoption.

These disconnects contribute to the problems that IoT providers have in designing the systems that buyers need; likewise, they account for skepticism on adoption speed. Providers' lower rankings of digital trust and privacy than buyers' could stem from providers not sufficiently engaging with cybersecurity decision makers (such as chief information officers and chief information security officers). Thus, they have limited visibility on the need for additional trust, privacy, and security; moreover, they are uncertain how those elements will be paid for.

Silos perpetuate the status quo

At most IoT buyers, there are different decision makers for IoT and cybersecurity procurement (such as chief technology officer, chief information officer, and chief information security officer). Across these organizations, more executives and managers are involved in IoT procurement than in cybersecurity procurement. Additionally, 14 percent of respondents note that while business-unit heads are directly involved in IoT procurement, they have minimum involvement in cybersecurity decision making. This suggests that cybersecurity solutions have yet to be customized at the product level, let alone in an end-to-end manner that factors security into the full scope of the data architecture of the IoT use cases. With better visibility, chief information and information security officers can make better cybersecurity control decisions.

A more comprehensive approach, with IoT buyers and providers along the product value chain implementing cybersecurity by regulatory compliance, is optimal, as governments have been pushing for more holistic regulations to manage risks (such as International Organization for Standardization [ISO] rule ISO 21434 and the guidelines from the UN Economic Commission for Europe World Forum for Harmonization of Vehicle Regulations in the automotive industry). In today's new use cases, buyers and providers rely on "handshake agreements" in which no clear delineation of cyberattack responsibilities exists. These agreements often result in players extending their IT cybersecurity to IoT applications through functionality add-ons. Increased IoT adoption and emerging cyberthreats will require rigorous regulatory compliance models to prevent any breaches.

Integration and beyond: Reaching true convergence

Most IoT systems today are designed for one-way data flow—from monitoring of sensors to data analysis—controlled by humans. As IoT cybersecurity transitions to a holistic, system-level approach that addresses the CIA framework, it can enable a change from systems that require operator input for data collection and data monitoring to IoT systems that need no human interface. This would mean a shift in how IoT solutions are designed and implemented. In the future, the industry could move to models in which IoT solutions are designed to operate on the basis of holistic self-trust. It would mark the convergence of cybersecurity and the IoT.

Convergence can happen at an architectural, parallel-design, or software-add-on level. At an architectural level, IoT solution providers build secured code into the backbone software across all tech stack layers (including firmware and hardware). At a parallel-design level, IoT solution providers and cybersecurity solution providers partner strategically throughout the IoT-system-design process (for example, from platform to cloud). With software add-ons, IoT solution providers install additional cybersecurity solutions to secure applications.

Integration can provide immediate benefits on the way to convergence

Despite current ecosystem bottlenecks—and those likely to appear on the path to full convergence—

both IoT buyers and providers would benefit from more integrated IoT and cybersecurity solutions. These would reduce complexity in the IoT buyer–cybersecurity portfolio while making IoT buyers less prone to vulnerabilities across the IoT stack. IoT providers, in turn, would benefit from buyers having less concern around cybersecurity risk.

Cross-functional or cross-technological IoT and cybersecurity integration is emerging, partially driven by buyers' demand for a holistic and seamless IoT experience. Close to *90 percent* of buyers are reducing the number of cybersecurity solutions deployed in their organizations, driven by the desire to reduce procurement complexity. Another major reason for the emergence is that cloud migration presents a unique opportunity for enterprises to design more robust cybersecurity tooling.

Convergence will eventually unleash high-stakes IoT use cases

Practically, IoT–cybersecurity convergence and better solution designs can make identity and authentication a more seamless experience while adding the capability to block instead of only detect cyberattacks and cyber intrusions. A trust-based model would establish networks and devices in which interoperability standards would be defined to support much greater functionality. Imagine the ability to drop a new device into a network and have it immediately scanned, welcomed, and assigned a trust score. At the highest level, it could immediately start to operate, using data collected by other devices in that network. Examples are drones that leverage data from vehicles in a city and a building security system that's informed by nearby emergency services to move into lockdown.

This new approach to cybersecurity would also provide the trust required to enable particular IoT use cases that involve personal, financial, and otherwise sensitive data, such as those that depend on credible transactions. Examples of the use cases benefiting from the approach are machine-to-machine car payments, touchless security enabled by camera recognition within the office, and real-time traffic management.

A cleansheet cybersecurity design would help enable the convergence, serving as an early-stage integration of cybersecurity into IoT systems, starting at the design of the IoT system and remaining operational from the pilot phase onward. This would greatly enhance the security of IoT systems. Today many OEMs fail to secure their systems and network completely in mass-production stages if the embedded security software isn't deployed early during development. As IoT functions shift beyond the monitoring of use cases to autonomous control with less and less human interface, cybersecurity would also need to pivot from detect only to detect and block.

Many pain points need to be solved to achieve such a goal. First, substantial customization will be needed to integrate cybersecurity into legacy IoT infrastructure by industry or use case. This challenge is compounded by the lack of industry talent and support to take on this work. Additional integration challenges come from the high volume of suppliers and the complexity of the ecosystem (in which most systems aren't compatible). Currently, there are multiple network connectivity standards, which also makes seamless experience harder to achieve. At the product level, there is the constant dilemma between achieving high performance and meeting strong cybersecurity requirements on smart devices that have limited computing capacity. This is all happening in conjunction with the growing urgency to solidify user confidence in digital trust and privacy.

Convergence is emerging

There is a strong realization that the IoT market needs to move from bolt-on to integrated cybersecurity solutions, resulting in multiple forms of convergence. In the current ecosystem, multiple players across the tech stack are already crossing territory between the IoT and cybersecurity (see sidebar "The IoT tech stack and cybersecurity solutions"). For instance, device and IoT solution providers are providing cybersecurity solutions for

The IoT tech stack and cybersecurity solutions

Internet of Things (IoT) and cybersecurity convergence can be driven by three types of providers: IoT providers, cybersecurity providers, and platform providers. Convergence, in this case, is the combination of any technical, functional, or commercial element of the IoT with cybersecurity to form a new, integrated whole.

IoT providers (such as Bosch.IO, Koninklijke Philips, and Medtronic) can integrate more cybersecurity into their IoT products. With their knowledge of the data architecture, they could safeguard the end-to-end security of the IoT stack. Cybersecurity providers (such as Dragos and Palo Alto Networks) are best positioned to provide insights on holistic cybersecurity protection across the IoT value chain. Platform providers, which include cloud service providers and communications companies (such as Amazon Web Services, C3.ai, Telefonaktiebolaget LM Ericsson, and Verizon), can position themselves as neutral integrators of IoT systems. A few companies (such as BlackBerry and Siemens) sit at the intersection of cybersecurity and the IoT and are positioned to marry enterprise cybersecurity solutions with IoT platforms.

The IoT market is trending toward convergence, but it isn't likely that this will result in a one-size-fits-all solution. These products may still need to be tailored to vertical- and use-case-specific needs.

their IoT platforms through routine patch updates to remove vulnerabilities, and enterprise cybersecurity providers have developed IoT management and analytic platforms to complement their offerings.

Approximately 80 percent of surveyed IoT providers are embedding security in some form into their IoT products, and roughly 70 percent of cybersecurity providers are making IoT-specific products, indicating early signs of convergence. Notably, however, only 50 percent of providers are building more holistic solutions for *both* cybersecurity *and* the IoT, as it's hard to create a one-size-fits-all solution for cybersecurity needs across different verticals and use cases. Specialized companies will continue to play a role in IoT and cybersecurity operations because of their differing functionality, their heterogenous operating systems, and the lack of standard interfaces and criteria across regions, industries, and requirements. Approximately 60 percent of providers are partnering with other companies to offer comprehensive IoT and cybersecurity solutions rather than building those capabilities in house.

Industry snapshots: Convergence prospects

To examine some examples of convergence of the IoT and cybersecurity, we can consider applications in the automotive, healthcare, and smart city contexts. Automotive IoT adoption is growing, with an estimated $100 billion 2030 market for IoT providers, and supported by future trends in the autonomous, connected, electric, and shared mobility space. Use cases range from in-car services such as autonomous driving to shared mobility. Likewise, in healthcare, IoT adoption is growing, with widescale deployment anticipated in three to five years and a projected 2030 provider market of $70 billion. Use cases include clinical applications such as robot-assisted surgery and consumer applications such as improving wellness. Smart cities, still at an early

stage of IoT adoption, are headed to an estimated $30 billion IoT provider market by 2030 as adoption ramps up in public services, safety, and transportation.

Cybersecurity risk is at the forefront across industry verticals, so further expansion of solutions and innovation is needed to secure various outcomes in the key CIA framework. Vehicles are becoming "moving computers on wheels" that pose an exponentially higher challenge in cybersecurity availability, particularly in security resilience and system uptime to prevent collisions. In use cases such as autonomous driving, extremely high safety and security requirements are crucial. The healthcare space presents critical risk, both in patient privacy and data-driven care decisions; in fact, survey respondents rank it highest for cybersecurity impact among all verticals. As such, confidentiality and availability are the focus. For smart cities, the primary concern is data integrity, as the security solutions involve multiple stakeholders and cross-cutting natures. Implementing a comprehensive cybersecurity strategy is complicated by the lack of standardization in protocols and a gap in cybersecurity talent at city governments.

IoT–cybersecurity convergence has the potential to ease such pain points. In the automotive sector, there is currently a lack of consensus among internal stakeholders on balancing performance with security. This is compounded by complicated integration and interoperability, beckoning a move to a software-defined, domain-based architecture. Healthcare is experiencing limited visibility and control of IoT devices, which also tend to have low computing capacity for security software. These challenges are all complicated by varying cybersecurity standards in network protocols. Smart cities have strong interdependence upon a range of verticals, necessitating significant coordination, which runs up against market segmentation across city networks and use cases.

While the specifics of IoT and cybersecurity convergence differ for each industry, there are common elements. For the automotive space, it means cybersecurity built in at the component level and rigorously tested from initial boot to system interaction. Architectural-level cybersecurity will also be critical in the healthcare sector, with an increasing tendency toward embedded endpoint security.

Additionally, partnerships are also an important element of convergence across verticals. For example, automotive OEMs will partner with security providers and tier-one and -two suppliers to develop standards and establish clear lines of security responsibility. Convergence in smart cities will involve partnerships across verticals and government agencies to meet governments' data reliability standards. Most city use cases are dependent upon other verticals (such as utilities), so convergence in any one of them could lead to convergence for cities.

The IoT is at a crossroads: provide incremental value in siloed clusters or unlock sizable value as an interconnected environment. When the IoT can make the transition to an integrated network within and across industrial verticals, it can provide a fully seamless industrial and consumer experience.

Cybersecurity is a key enabler, providing the trust to integrate IoT networks. As the IoT has exacerbated cybersecurity risk, ranging from digital to physical security, the convergence of IoT and cybersecurity solutions could accelerate adoption of the IoT. However, there are many challenges, including buyers' high expectations for privacy and digital trust, siloed decision making for the IoT and cybersecurity, and the lack of industry-specific architectural security solutions at the design stage. If security risks are comprehensively managed, an additional $125 billion to $250 billion in IoT value captured by IoT suppliers could be unlocked, implying a $625 billion to $750 billion TAM value in 2030.

IoT and cybersecurity convergence should address IoT buyers' concerns around digital trust and privacy, enable new use cases, and amplify adoption of existing ones. It will likely allow the IoT industry to adopt higher security standards, driven by government mandates. Convergence will be tailored for vertical needs rather than offer a one-size-fits-all solution, and it will span the entire tech stack rather than be a simple fix that applies only to a portion of the ecosystem.

A shared cybersecurity responsibility model will require strategic partnerships among IoT buyers, providers, and platform players. This presents an opportunity for providers of integrated solutions to consolidate today's fragmented IoT and cybersecurity provider ecosystem. Still, this won't be a winner-takes-all market environment. To maximize the opportunity for the IoT to play an increased role in many aspects of people's lives, numerous players will have to work together to reduce risk, and numerous players will be in a position to reap the rewards.

Jeffrey Caso is an associate partner in McKinsey's Washington, DC, office; **Zina Cole** is a partner in the New York office; **Mark Patel** is a senior partner in the Bay Area office; and **Wendy Zhu** is a consultant in the Denver office.

The authors wish to thank Ayman Al Issa, Rich Armour, Michael Chui, Sara Cinnamon, Mark Collins, Jeremy Eaton, Yvonne Ferrier, Bodo Koerber, Aamer Rao, Dan Tucker, Daniel Wallance, and Jonathan Woetzel for their contributions to this article.

Designed by McKinsey Global Publishing