



Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

Enterprise customers would buy more IoT devices if vendors could ensure better security.

By Syed Ali, Ann Bosche and Frank Ford

Syed Ali is an expert vice president with Bain & Company in the Houston office. Ann Bosche is a partner with Bain in San Francisco, and Frank Ford is a Bain partner in London. Syed and Frank are experts in cybersecurity and partners in the Global Information Technology practice, and Ann works with Bain's Global Technology practice.

The authors would like to thank Lauren Brom for her contributions to this work.

Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

Executive Summary

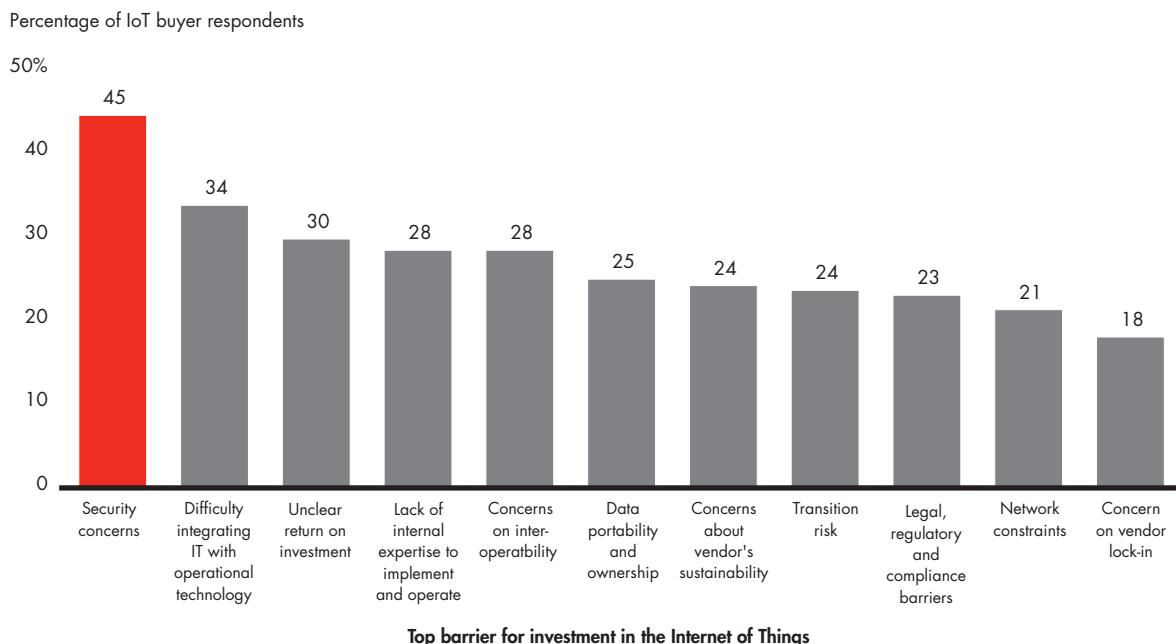
- ▶ Enterprise customers are limiting their investment in IoT devices because they have concerns about security risks.
- ▶ Executives say they would buy more devices and pay more for them if manufacturers could provide better security.
- ▶ Investing to improve security could grow the IoT cybersecurity market by \$9 billion to \$11 billion.

The Internet of Things continues to grow rapidly, but concerns about security remain a significant barrier and are hindering the adoption of IoT devices (see Figure 1).

In fact, research by Bain & Company finds that enterprise customers would be willing to buy more IoT devices if their concerns about cybersecurity risks were addressed—on average, at least 70% more than what they might buy if their concerns remain unresolved (see Figure 2). In addition, 93% of the executives we surveyed said they would pay an average of 22% more for devices with better security. Taken together, Bain estimates that improving security solutions for these devices could grow the IoT cybersecurity market by \$9 billion to \$11 billion. One reason for this willingness may be increased pressure from new regulations such as the EU General Data Protection Regulation, which imposes strict data protection requirements and penalties on companies for security failures, including data breaches.

Figure 1

Security remains the leading barrier for IoT adoption



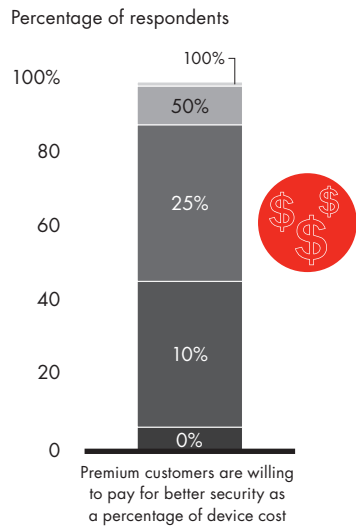
Source: Bain 2018 IoT customer survey (n=521)

Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

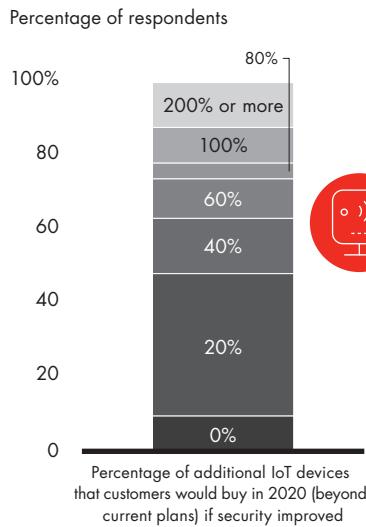
Figure 2

Customers would pay more and buy more devices if security was better

Customers would pay an average of 22% more for secure IoT devices ...



... and would buy an average of 70% more IoT devices if they were secure



Premiums and greater sales would boost the IoT cybersecurity market by \$9 billion to \$11 billion in 2020

Source: Bain 2017 IoT enterprise cybersecurity survey (n=280)

These are among the findings of our research and survey work over three years, including discussions with CEOs, COOs, CIOs, CISOs and other business and technical leaders on cybersecurity and IoT technology.¹ Significantly, executives from companies with the most advanced cybersecurity capabilities are also the most concerned about security risks.

For IoT device vendors—companies that make IoT devices as well as those that provide related solutions—the message is clear: Improve security to gain a competitive edge and grow your market.

How customers think about cybersecurity

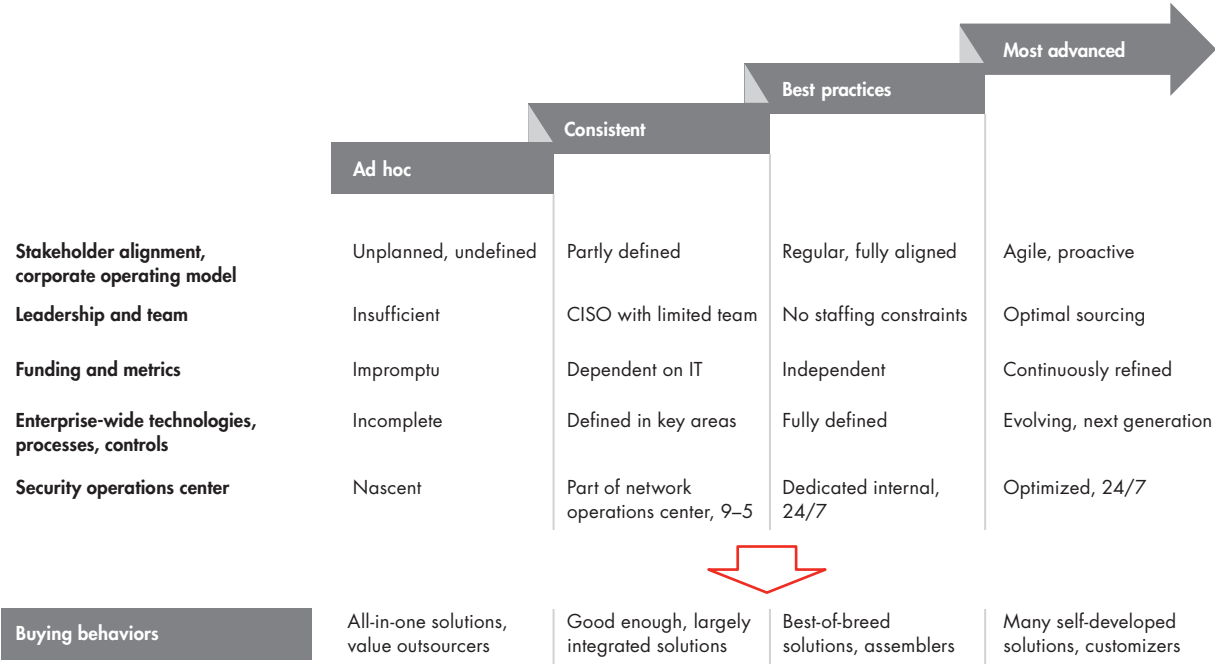
Most executives we surveyed (60%) said they were very concerned about the risks IoT devices pose to their companies—not surprising, given the damages that an IoT security breach can cause to operations, revenue and safety. When poorly protected, IoT devices can allow access to enterprise systems, resulting in large data breaches.

Infected devices can also be commandeered to launch debilitating attacks against enterprises. In October 2016, the Mirai malware attack compromised thousands of sensors, cameras and other devices to create a massive botnet that launched distributed denial-of-service attacks that disrupted popular sites, including GitHub, Netflix, Twitter and Airbnb. In January 2018, a Mirai variant called Okiru targeted popular versions of ARC processors embedded in billions of IoT products. Hijacked IoT devices can also carry out click fraud, which costs advertisers billions of dollars annually. Compromised devices can also be used to mine cryptocurrency such as bitcoin and monero.

Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

Figure 3

Customer segments by cybersecurity maturity



Source: Bain analysis

In determining solutions to guard against these types of attacks, IoT device vendors can segment their target customers by levels of cybersecurity capability maturity. Such a segmentation is helpful in determining distinct approaches based on typical needs, and reflects the reality that enterprise customers’ capabilities are not static but rather are progressing toward more advanced levels (see Figure 3). Our research finds that customers at the least advanced end of the spectrum are more likely to seek out simplified and integrated security solutions, whereas those with more advanced capabilities prefer to invest in best-of-breed or customized point solutions.

Across segments, nearly all executives said that IoT devices pose a moderate or significant risk to their organizations, and executives at companies with greater cybersecurity sophistication see more risk than those at companies with less sophisticated cybersecurity capabilities (see Figure 4).

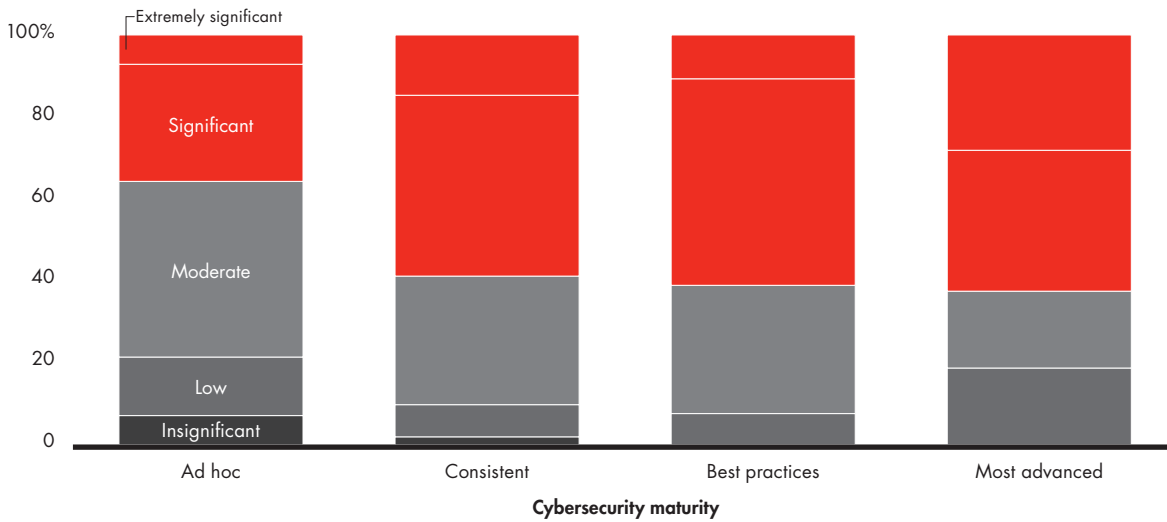
Our research also indicates that executives within some industries see themselves at greater risk than others (see Figure 5). Executives in durable goods, building and construction, energy and utilities, financial services, and technology were most likely to express a significant level of concern. These concerns reflect industry realities, not merely the perceptions of individual executives. In energy, for example, oil and gas producers rely on tens of thousands of IoT sensors and complex production control devices at their wells and drilling platforms. Energy companies use the data from these IoT devices, which can exceed a terabyte on an average day, in near real time to fine-tune their operations while maintaining strict safety thresholds. Compromising the integrity or disrupting the flow of this data could lead to catastrophic damage.

Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

Figure 4

Companies with high levels of cybersecurity maturity are more attentive to IoT risks

Percentage of respondents' level of concern with IoT cybersecurity risk

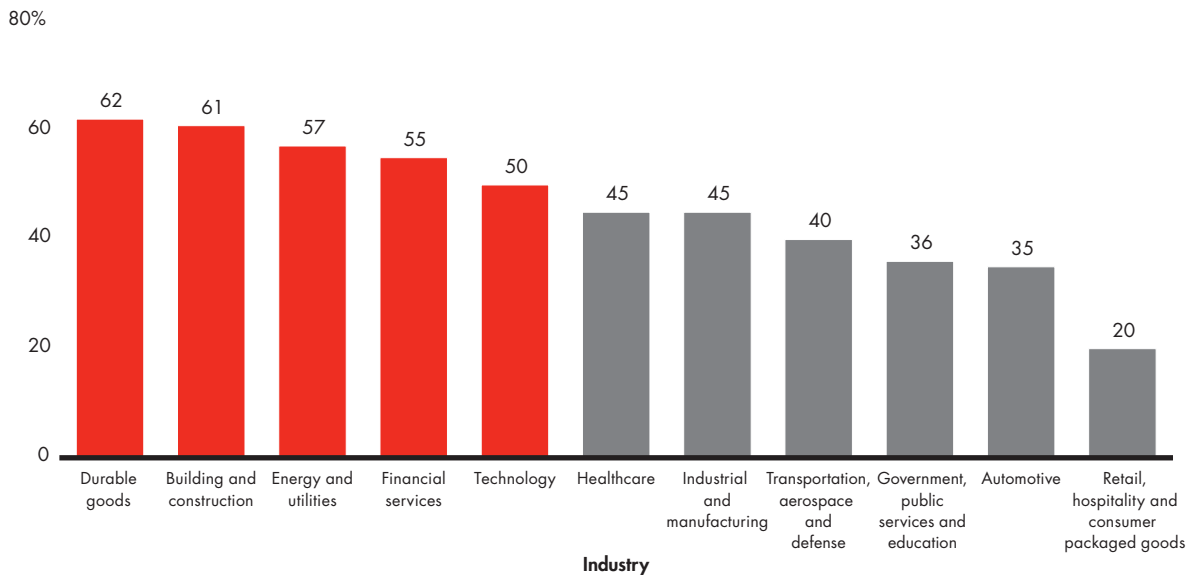


Note: Cybersecurity capability maturity measures an organization's progress toward ever more sophisticated and advanced cybersecurity skills and practices
 Source: Bain 2017 IoT enterprise cybersecurity survey (n=280)

Figure 5

Assessment of security risks in IoT devices differs by industry

Percentage of respondents who expressed significant or extremely significant concern with IoT cybersecurity risk



Source: Bain 2017 IoT enterprise cybersecurity survey (n=280)

Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

Nearly half of healthcare executives see a significant risk. Hospitals and clinics increasingly rely on connected diagnostic monitoring and care delivery equipment from a range of vendors that source components from third parties. MRIs, robotics-assisted surgery devices and drug delivery pumps all present tempting opportunities for unauthorized access—a clear threat to patient safety. In September 2017, the US Industrial Control Systems Cyber Emergency Response Team identified vulnerabilities in wireless syringe infusion pumps, warning that, if unmitigated, these could pose a significant threat to patients.

Manufacturers’ use of IoT also introduces new risks in industrial environments. Large manufacturers might deploy thousands of IoT devices, ranging from sensors to sophisticated, semiautonomous robots. Compromised sensors could lead to data inaccuracies that hinder management’s ability to make critical operational decisions or create inventory problems that wreak havoc across the value chain. Still greater risks may be found on the plant floor, where a compromised robotic device could introduce subtle but dangerous activity or create greater havoc and harm to workers and other equipment.

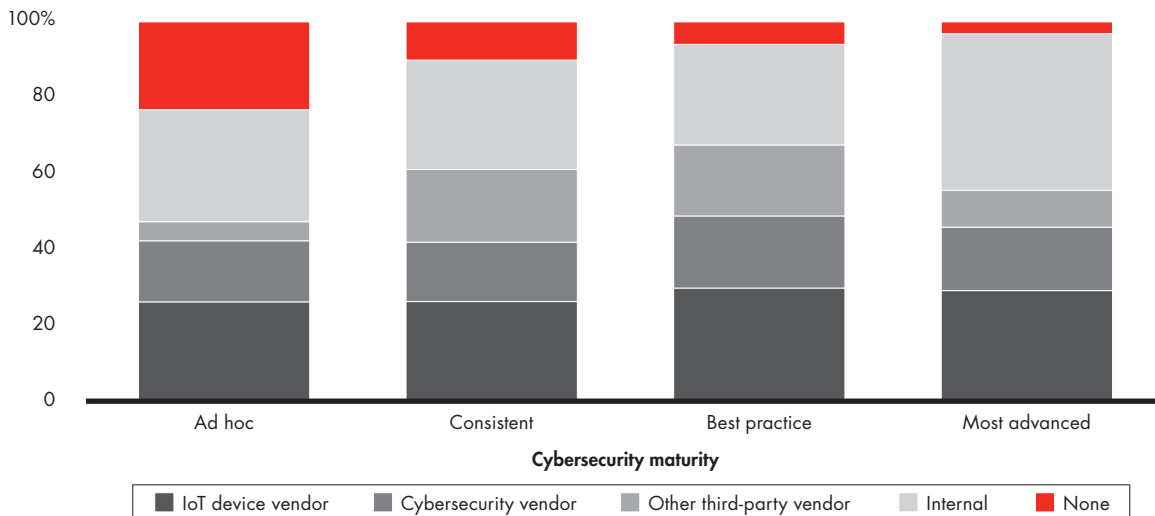
How customers manage IoT cybersecurity

Our conversations with executives who manage security indicate that customers want solutions that are highly effective, easy to integrate and flexible to deploy. Companies take a range of approaches to meet their security needs based on their capabilities and the availability of marketplace solutions from vendors (see Figure 6). Only about a third of IoT cybersecurity solutions used today are from IoT device vendors, indicating that vendors are either not offering holistic, high-quality solutions that meet consumer needs or they are not promoting them well enough. Our research found that companies with the most advanced cybersecurity capabilities rely more

Figure 6

Companies with ad hoc cybersecurity are more likely to have gaps in coverage, presenting opportunities for IoT device makers

Percentage of respondents using various approaches to secure IoT devices



Note: Cybersecurity capability maturity measures an organization's progress toward ever more sophisticated and advanced cybersecurity skills and practices
 Source: Bain 2017 IoT enterprise cybersecurity survey (n=280)

Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

on internally developed security solutions not only because they may have more complex needs but also because they are more likely to have the talent and capabilities to develop their own solutions. Companies with ad hoc security capabilities have the most gaps across all IoT layers that we tested.

A disconnect on customer needs

We also looked at how companies deploy solutions by layer of security, and found ample opportunity for IoT device vendors at every layer of the stack.

Our survey found that the access interface layer has the greatest level of protection, whether internally developed or provided by a manufacturer or third party (see Figure 7). Other layers of the stack were protected by more internal solutions—or, in some cases, none at all. Customers’ preference for internal solutions may be partially explained by considering the specific conditions of each layer.

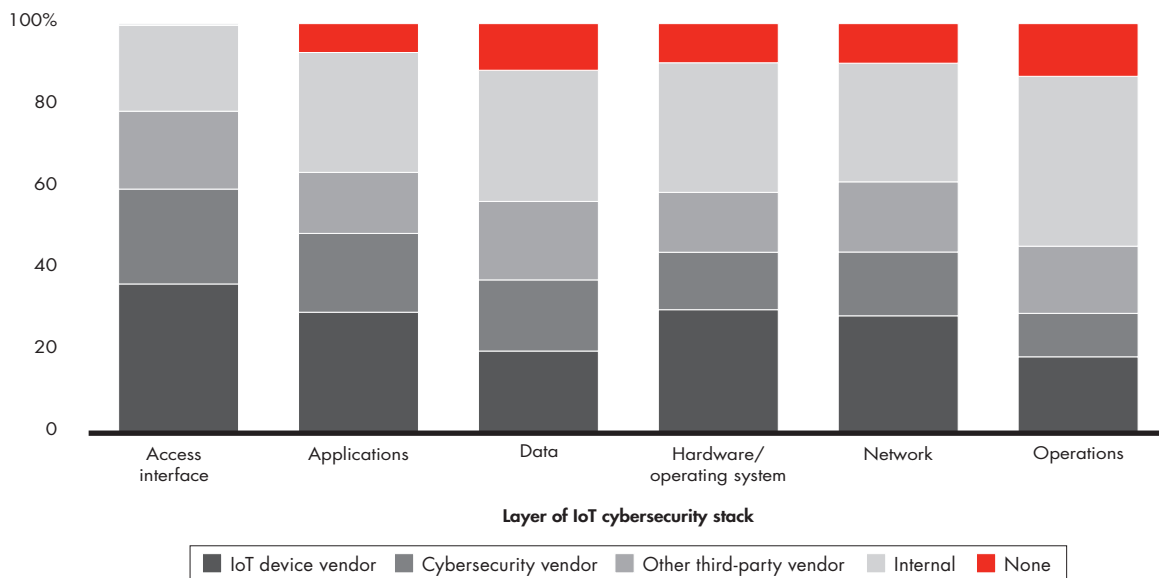
For example, data security solutions typically require more computing and power resources than are currently available on basic IoT devices. MIT researchers have created a new chip that enables encryption on IoT devices using 1/400 of the power and 1/10 of the memory at 500 times the speed of current chips. But until this new technology is widely adopted, manufacturers need to continue to make design and capability trade-offs when balancing these requirements against the size, cost and power of the IoT device.

Hardware security solutions must address vulnerabilities at the physical interface (such as USB or Ethernet ports), the device operating system and firmware. But few manufacturers adequately test hardware against known vulnerabilities before shipping, and far more devices fall short during ongoing tests for new vulnerabilities.

Figure 7

Device vendors currently delivering less than 40% of solutions at all layers

Percentage of respondents using various approaches to secure IoT devices



Source: Bain 2017 IoT enterprise cybersecurity survey (n=280)

Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

Finally, IT security operations must manage and monitor their IoT devices, partly with log data from the other five layers. While most enterprises would like a cohesive set of tools and a unified overview of the security posture of their devices, few IoT device makers understand their customers' operations well enough to provide that kind of solution. Still, they can work with customers to identify trusted third parties to act as partners in developing comprehensive security solutions.

Taken in aggregate, these types of manufacturer shortcomings can leave customers on their own when it comes to securing their IoT devices across these layers. Lacking well-designed IoT cybersecurity products and services, customers are devising their own solutions, forgoing them altogether or failing to implement IoT solutions until vendors can fill the gap.

What IoT device vendors can do to gain market share

IoT device vendors and ecosystem players that move quickly to improve the security around IoT devices are likely to reap rewards not only from their ability to earn a premium but also from an expanded market. Some leaders in the IoT ecosystem are stepping up to meet the security challenge and grab the related opportunities. Amazon has created an ecosystem of IoT solutions integrated with its cloud offering. It recently licensed an open source operating system called FreeRTOS that makes it easier to develop, deploy, manage and secure low-power IoT devices, and enhanced it with libraries and tools that help with IoT device management as well as data and network security. Similarly, Microsoft's Azure IoT Hub provides device management and security capabilities in the form of device provisioning, authentication and secure connection. Another example is GE, an industrial IoT device manufacturer that views cybersecurity as a competitive advantage and strategically strives to embed capabilities across all layers of its IoT technology stack. GE acquired Wurldtech in 2014 and eventually integrated the Achilles security products with its Predix IoT management platform. From a governance perspective, GE assigns risk management and product security responsibilities to dedicated leaders across its organization who ensure that cybersecurity is prioritized and implemented into its products, including IoT devices.

IoT device vendors will need to pay more attention to security in the design, development and deployment of devices.

These efforts represent important progress, but on their own are not enough to address the broader security issues facing IoT adoption. All IoT device vendors will need to pay more attention to security in the design, development and deployment of devices. Four steps can help executives frame their task.


First, manufacturers need to understand how customers are using their devices. Staying current by refreshing their understanding of customer use cases every 12 to 18 months will allow them to stay on top of evolving security requirements and help identify unmet needs. Ascertaining the average cybersecurity maturity level of their customers will help manufacturers invest in the appropriate out-of-the-box and add-on solutions. For example, ad hoc maturity customers tend to seek value instead of the latest and greatest solutions.

Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

Second, manufacturers should provide cybersecurity capabilities on the device and, when possible, partner with trusted cybersecurity vendors to provide additional solutions. Engineering teams should embed secure development practices into the software and hardware components of the device, and provide inherent solutions for the access interface, apps, data and device layers. Most customers will use these out-of-the-box capabilities regardless of their cybersecurity maturity. Taking these measures can mitigate common vulnerabilities in IoT devices such as default or embedded passwords, lack of data security for credentials and network communications, and weak safeguards for ensuring system integrity. Manufacturers can also invest in partnerships with cybersecurity vendors to provide aftermarket solutions at the data, network and operations layers, selectively integrating these for some customer segments. For example, customers with consistent security tend to prefer integrated solutions, while best practice buyers look for best-of-breed solutions rather than integration among solutions.

Third, manufacturers also need to meet quality assurance thresholds and be able to certify that their IoT devices are free from known vulnerabilities. This would mitigate a major pain point for customers who sometimes install new devices without realizing they contain vulnerabilities. Deploying a more methodical process to identify and remove vulnerabilities across layers or engaging third-party vulnerability scanning and penetration test firms can help manufacturers meet this bar. Defining a cybersecurity warranty period with clear obligations tells customers what the vendor is responsible for, and for how long. In combination, these measures deliver a hardened device aligned with many cybersecurity best practices.

Finally, manufacturers can fulfill their obligations during the warranty period by continuously testing for new vulnerabilities, providing software and firmware updates, as well as feature and functionality upgrades for out-of-the-box and aftermarket solutions. Delivering updates to firmware, operating systems and applications in response to newly discovered security vulnerabilities should remain a top priority throughout the warranty period.

These four steps are a start, though by no means the whole of what it will take to begin to address the security concerns that hold back the Internet of Things. While growth in IoT markets seems destined to continue its inexorable march, many enterprise customers will continue to move cautiously until they can gain some reasonable assurance of the security not only of their data but also of the operations that increasingly rely on devices, sensors and the Internet of Things. 

For more on Bain's viewpoint on IoT, see the Bain Brief *"Defining the Battlegrounds of the Internet of Things."*

¹ Bain's 2017 IoT enterprise cybersecurity research drew more than 280 responses from companies with a wide variance in cybersecurity maturity in Canada, Europe and the US, ranging in revenue size from \$100 million to \$10 billion and headcount from 200 to more than 10,000 employees. Our 2018 IoT enterprise customer research drew more than 520 responses from companies in Canada, Europe, China and the US, ranging from \$10 million to more than \$10 billion in revenue size and headcount from 100 to more than 10,000 employees. Two Bain surveys in 2016 measured customer opinions (n=533) and vendors' views (n=158).

Shared Ambition, True Results

Bain & Company is the management consulting firm that the world's business leaders come to when they want results.

Bain advises clients on strategy, operations, technology, organization, private equity and mergers and acquisitions. We develop practical, customized insights that clients act on and transfer skills that make change stick. Founded in 1973, Bain has 56 offices in 36 countries, and our deep expertise and client roster cross every industry and economic sector. Our clients have outperformed the stock market 4 to 1.

What sets us apart

We believe a consulting firm should be more than an adviser. So we put ourselves in our clients' shoes, selling outcomes, not projects. We align our incentives with our clients' by linking our fees to their results and collaborate to unlock the full potential of their business. Our Results Delivery® process builds our clients' capabilities, and our True North values mean we do the right thing for our clients, people and communities—always.



Key contacts in Bain's Information Technology practice

Americas	Syed Ali in Houston (<i>syed.ali@bain.com</i>) Steve Berez in Boston (<i>steve.berez@bain.com</i>) Rudy Puryear in Chicago (<i>rudy.puryear@bain.com</i>)
Asia-Pacific	Arpan Sheth in Bengaluru (<i>arpan.sheth@bain.com</i>)
Europe, Middle East and Africa	Frank Ford in London (<i>frank.ford@bain.com</i>) Stephen Phillips in London (<i>stephen.phillips@bain.com</i>)

Key contacts in Bain's Technology, Media and Telecommunications practice

Americas	Ann Bosche in San Francisco (<i>ann.bosche@bain.com</i>) David Crawford in Silicon Valley (<i>david.crawford@bain.com</i>) Darren Jackson in Los Angeles (<i>darren.jackson@bain.com</i>) Michael Schallehn in Silicon Valley (<i>michael.schallehn@bain.com</i>) Paul Smith in Silicon Valley (<i>paul.smith@bain.com</i>)
Asia-Pacific	Bumshik Hong in Seoul (<i>bumshik.hong@bain.com</i>) Florian Hoppe in Singapore (<i>florian.hoppe@bain.com</i>) Bhanu Singh in New Delhi (<i>bhanu.singh@bain.com</i>)
Europe, Middle East and Africa	Laurent-Pierre Baculard in Paris (<i>laurent-pierre.baculard@bain.com</i>) Michael Schertler in Munich (<i>michael.schertler@bain.com</i>) Christopher Schorling in Frankfurt (<i>christopher.schorling@bain.com</i>)

For more information, visit www.bain.com