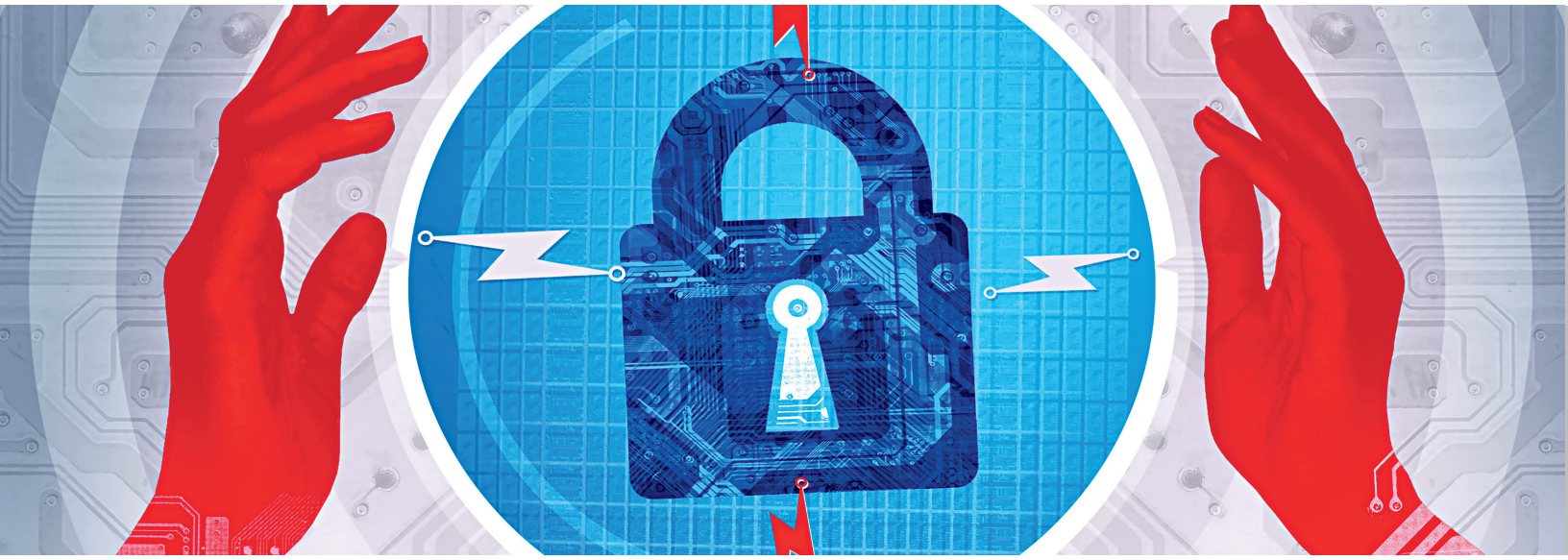
MAY 2017



SEMICONDUCTORS

Security in the Internet of Things

Security issues may represent the greatest obstacle to growth of the Internet of Things. How can semiconductor companies help resolve them?

Harald Bauer, Ondrej Burkacky, and Christian Knochenhauer

Over the past few years, the Internet of Things (IoT) has captured headlines across the world, with newspaper and magazine articles describing its potential to transform our daily lives. With its network of "smart," sensor-enabled devices that can communicate and coordinate with one another via the Internet, the IoT could facilitate computer-mediated strategies for conducting business, providing healthcare, and managing city resources, among numerous other tasks. For the public, the IoT could transform many of our most mundane activities by enabling innovations as diverse as self-driving cars and connected refrigerators capable of sending pictures of their contents to shoppers in grocery stores.

Although the IoT is still a nascent phenomenon, with many aspects of its infrastructure under development, the McKinsey Global Institute predicts it could have an annual economic impact of $3.9 trillion to $11.1 trillion worldwide by 2025.[1] For the semiconductor sector, one of the many industries poised to benefit from the IoT's growth, the economic gains could be particularly significant.

The IoT's way forward may be complicated, however. As with any market in its early stages, growth projections could prove overly optimistic if innovators and business leaders are unable to overcome various technological, regulatory, and market challenges. In the case of the IoT, weak security may

be the most important issue—a point underscored by a survey that McKinsey conducted in 2015 in collaboration with the Global Semiconductor Alliance (GSA).[2] When we asked respondents about their greatest concerns about the IoT, security topped the list.

Given the importance of IoT security to semiconductor companies, McKinsey and the GSA conducted an additional survey and interviews on this topic in 2016 (see sidebar, "Our research methodology"). The new research, which forms the focus of this article, revealed that respondents still view security as a major challenge to the IoT's growth. But they also believe that semiconductor companies can help overcome these problems and capture significant value by providing security solutions across industry verticals.

Our research methodology

The 2015 collaboration between McKinsey and the Global Semiconductor Alliance (GSA) involved the following research:

- interviews with 30 GSA members who were senior executives at semiconductor companies or at companies in adjacent industries that are part of the Internet of Things (IoT) ecosystem, such as network equipment and industrial automation
- a survey of 229 semiconductor executives at GSA member companies
- development of a fact base on the IoT, focusing on issues relevant to semiconductor companies

Our 2016 research, which focused on IoT security, involved interviews with 30 GSA executives, including some from our original study, and monthly meetings with a C-level executive steering committee. We also surveyed 100 executives within the semiconductor sector and adjacent industries, and interviewed McKinsey experts.

IoT security: A role for semiconductor companies

Hackers have already wreaked havoc by infiltrating connected IoT devices. Paradoxically, they usually aren't targeting device owners, who often remain unaware of security breaches. Instead, the hackers simply use IoT devices as starting points for attacks directed against another target. For instance, the 2016 Mirai attack used IoT devices to attack the Internet infrastructure, causing shutdowns across Europe and North America that resulted in an estimated $110 million in economic damage.

With the IoT installed base expected to increase by about 15 to 20 percent annually through 2020, security is simultaneously a major opportunity and a challenge. Semiconductor companies are therefore obliged to develop solutions that strengthen IoT security and also contribute to their bottom line. However, our recent research suggests that four major challenges may prevent them from capturing opportunities (Exhibit 1).

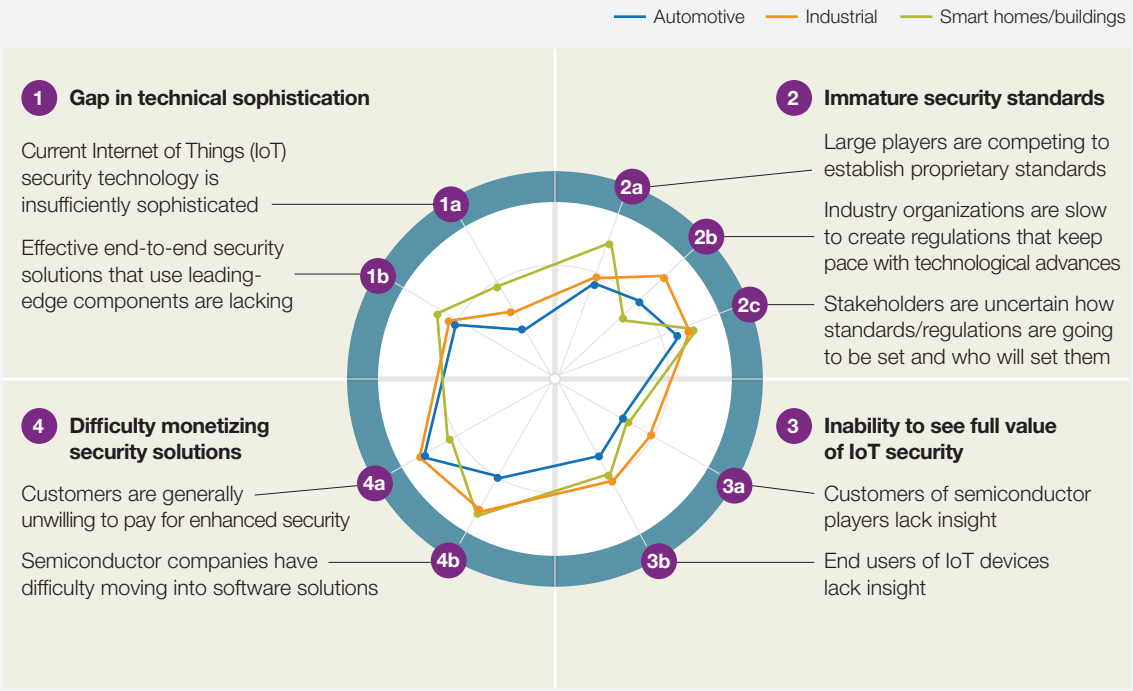
Challenge 1: Gaps in technical sophistication

By nature, a complex system of connected devices opens many new attack vectors, even if each device is secure when used independently. Since a system's most vulnerable point determines its overall security level, a comprehensive, end-to-end approach is required to secure it. Such approaches are difficult to develop, however, because most hackers concentrate on breaching a specific element within the technology stack by using one methodology. By contrast, system operators or integrators must provide end-to-end protection against all possible attack vectors, dividing their attention and resources across the system.

It is not yet clear who will take the lead in developing end-to-end security solutions for the IoT. Component suppliers and OEMs are not well positioned to accomplish this task, since the IoT includes such a broad network of devices of different provenance.

Exhibit 1 **Semiconductor companies see four main challenges in providing Internet of Things solutions.**

Average rating of challenge and relevance on 0–3 scale[1]



[1]4-point scale where 0 = not challenging/irrelevant, 3 = most challenging/relevant. Center scaled to 1 in graphic.

Source: McKinsey/GSA Semiconductor Industry Executive Survey

Integrators are better positioned to provide solutions, but they often lack the necessary capabilities.

Challenge 2: Standards are absent or immature

The IoT lacks well-established overarching standards that describe how the different parts of the technology stack should interact. Instead, large players and industry organizations use their own solutions. Some segments, such as industrials, still rely on a small set of proprietary, incompatible technology standards issued by the major players, as they have done for many years. In other segments, such as automotive or smart buildings, standards are rudimentary. This lack of standards may slow IoT adoption or discourage device manufacturers and others from developing new technological solutions, since they do not know whether their innovations will meet the guidelines that eventually become dominant. In addition, IoT players will have difficulty developing end-to-end security solutions without common standards.

Challenge 3: Customers and end users view IoT security as a commodity

Our research confirmed that customers and producers consider security essential, but they also view it as a commodity—a basic feature that does not merit higher prices. This creates a fundamental disconnect between the desire for security and the willingness to pay for it. In our survey, 31 percent of semiconductor leaders claimed that their manufacturing customers want to try to avoid all security breaches at any cost; an additional 38 percent believed that their customers want security solutions that eliminate at least 98 percent of potential risks (Exhibit 2). Only 15 percent of

respondents believed that their customers would be willing to pay a premium higher than 20 percent for the next tier of enhanced chip security. More than 40 percent indicated that their customers either are unwilling to pay any premium or expect security costs to decline.

This disconnect could hinder technology progress and inhibit the growth of many IoT applications. Unlike challenges related to technology or standards, this issue can be resolved only by changing customer mind-sets—in other words, by convincing them that security is worth additional cost.

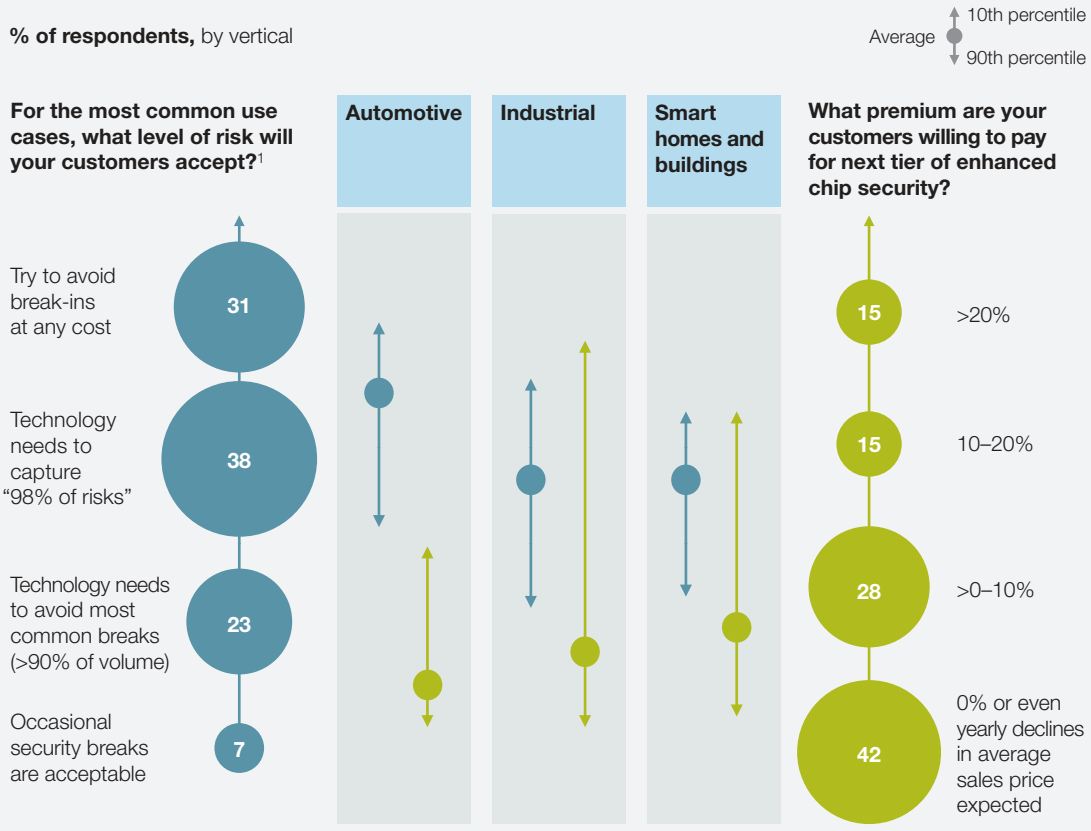
The implications of these findings for semiconductor companies are clear: they need to understand their customers thoroughly before developing security solutions, targeting those with a real willingness to pay, and then developing products that meet their specific needs.

Challenge 4: Semiconductor companies struggle to profit from security

With end customers and device manufacturers unwilling to pay for significant security measures, semiconductor companies are in a bind. In our survey, 38 percent of semiconductor executives

Exhibit 2

Customers of semiconductor companies want security but are unwilling to pay a premium for it.



[1]Figures may not sum to 100%, because of rounding.

Source: McKinsey/GSA Semiconductor Industry Executive Survey; McKinsey analysis

said that it is highly difficult to make money by offering security solutions, and 40 percent said it is difficult. Their troubles may largely stem from the long-standing, widespread perception that software providers have greater security expertise. For those semiconductor companies that choose to create security software, or that are forced in that direction, the potential profits may not be commensurate with the effort required. After all, many semiconductor players have stepped up their software ventures in recent years, but most have been disappointed with their returns.

Challenges and trends in specific industry verticals

Since IoT industry verticals differ in many respects, their security challenges also will vary, as we discovered when we undertook a detailed examination of three important areas: automotive, industrial, and smart homes and buildings.

Automotive

According to our research on the automotive sector, semiconductor leaders are primarily concerned about how standards will evolve and who will set them, since there is still much uncertainty. Many respondents felt that major OEMs and industry consortia will move first in designing their own standards and technical solutions. However, some respondents also thought that other scenarios were plausible. For instance, a small group of OEMs might band together to take the lead, or reported new entrants to the automotive space, such as Apple, might gain enough scale and influence to establish de facto standards.

Semiconductor companies that want to pursue automotive opportunities may find it difficult to monetize solutions. While OEMs are concerned about security, they also need to keep material costs of the car's base model constant, even when introducing a new one, so they are often reluctant to pay more for security features. With this in mind, semiconductor companies should position their security offerings as part of optional features that are not part of a car's base price. For example, advanced driver-assistance systems (ADAS) currently generate an additional €3,000 to €5,000 in lifetime revenue for OEMs per car. But OEMs will not be able to develop these features any further unless they can ensure their safety—an imperative that gives them an incentive to pay for security. To obtain the additional €3,000 to €5,000 per car that ADAS features generate, our experts estimate that OEMs could spend an extra €50 to €150 per car on security solutions.

Industrials

Innovative industrial IoT applications ("Industry 4.0") are slowly gaining traction within factories and plants, helping companies pursue operational improvement. Despite those benefits, many companies have been slow to implement IoT use cases, often because of security challenges.

Insufficient security technology in industrials often relates to the large variety of legacy systems in the field, as well as a lack of standards. In many businesses, operations largely depend on older computer systems and dated machinery. When companies connect those legacy systems to the Internet, they often struggle to maintain end-to-end security or find it impossible.

To resolve the issues with legacy systems, our research suggests that IoT players should consider designing and implementing new solutions, such as completely ring-fenced networks or redundant sensor networks. Semiconductor companies could contribute to the development of such systems, allowing them to capture value from IoT security. The opportunities exist in two areas with different industry dynamics: common applications for mainstream-market equipment and niche applications for specialty equipment.

Within mainstream equipment, a few players have developed their own ecosystems of proprietary

technologies and are significantly investing in end-to-end IoT applications and platforms. Since security is an essential part of the value proposition for mainstream-equipment ecosystems, semiconductor players should try to determine which company's ecosystem is likely to offer the most opportunities, and then develop security features that complement it.

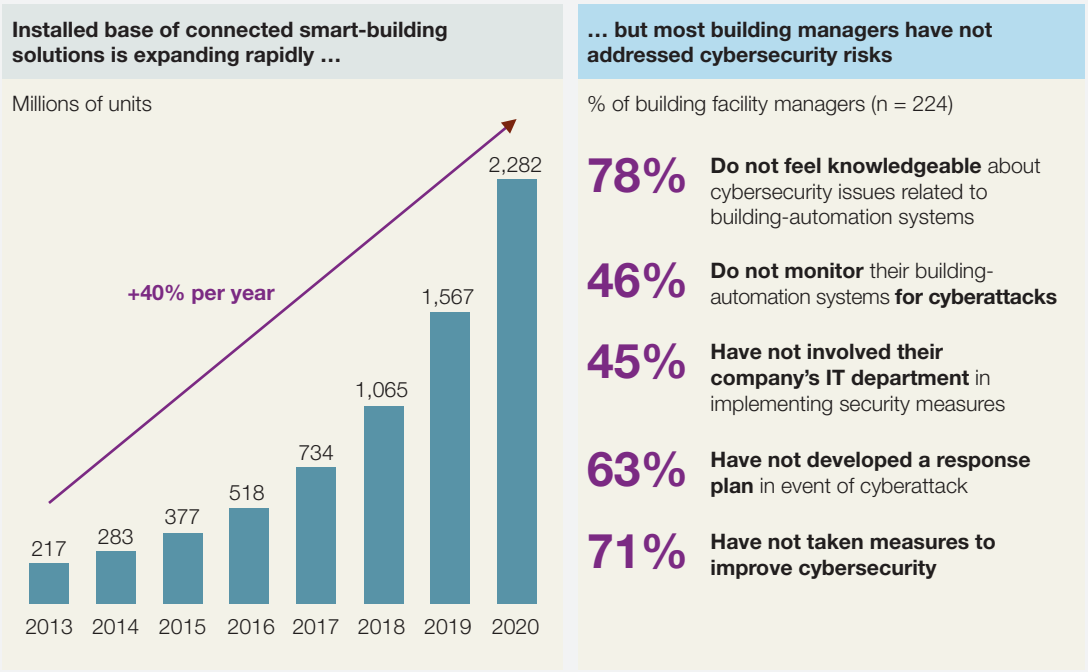
Within niche applications for specialty equipment, OEMs typically create tailored solutions for their customers. In many cases, however, they have little incentive to provide security features that will drive up the cost of their solutions. In addition, specialty integrators and machinery OEMs often do not consider the total cost of ownership for IoT applications. The situation will not change until end customers specifically demand such applications and the security that goes with them—a trend that will take time to gain momentum.

Smart homes and buildings

We have recently seen major growth in IoT applications for smart homes (private residences) and smart buildings (commercial use)—and this has also increased security issues.

Smart buildings. We expect the IoT installed base in the smart-building segment to grow by 40 percent until 2020, introducing a multitude of new attack vectors per building (Exhibit 3). Our research suggests that the smart-buildings segment is still in its infancy, with many players still developing applications and associated security solutions.

Exhibit 3 **Many professional building managers are not addressing Internet of Things security threats.**



Source: Gartner; IBM; smart-building facility-manager survey in *Building Operating Management*, Jan 2015

While this presents opportunities for semiconductor companies, it will take time until end customers deploy applications at scale. That means it could be the right moment for bold moves and investments in technology, but only for those willing to assume significant risks related to the lack of standards and uncertainty of demand. The payoff could be great, however, since our research suggests that professional building owners and managers feel unprepared for the threat ahead.

Smart homes. IoT security breaches are rising in residential applications. The fact that few end customers take extra steps to ensure security, such as updating firmware, suggests that many do not prioritize privacy issues. These factors may explain why end customers are extremely reluctant to pay for enhanced security.

Many companies have attempted to establish security standards for smart-home IoT applications, including OEMs, Internet players, and tech companies. The companies that become dominant within the nascent sector should prevail in setting standards, but it is not yet clear which these will be.

As with the automotive vertical, we believe that smart-home security could gain traction if developers link it with another feature that customers value, such as usability. For example, technologies or solutions that considerably simplify setup efforts and increase security could be in high demand. Since many smart-home devices have short replacement cycles, and since they require a limited investment per household, the market could experience healthy growth if stimulated by a major event, as described above. To benefit from this trend, semiconductor companies should place their bets now on the smart-home ecosystems that will become dominant.

Value-creation opportunities for semiconductor companies

When pursuing IoT opportunities—including those related to turning security solutions into an important new revenue source—semiconductor companies should choose among three core strategies, adapting them to suit their customers and industry (Exhibit 4):

- developing tailored security technologies for a broad range of customers
- formulating a sharper value proposition that draws attention to the benefits that security offerings bring to end customers
- creating security solutions that allow semiconductor companies to expand into adjacent business areas and develop new business models

Promoting tailored innovation

Semiconductor companies should develop a tool kit of security offerings that allows them to customize their products by vertical and customer segment. Some offerings will provide state-of-the-art security for applications requiring the most stringent degree of protection. But for standard applications, where customers consider security less important and are thus less willing to pay a premium, semiconductor companies must provide offerings with "good enough" security features that protect against only the most common threats. Ideally, such solutions will enable other features, unrelated to security, such as those that increase convenience or usability for end users.

Developing a sharper value proposition for security

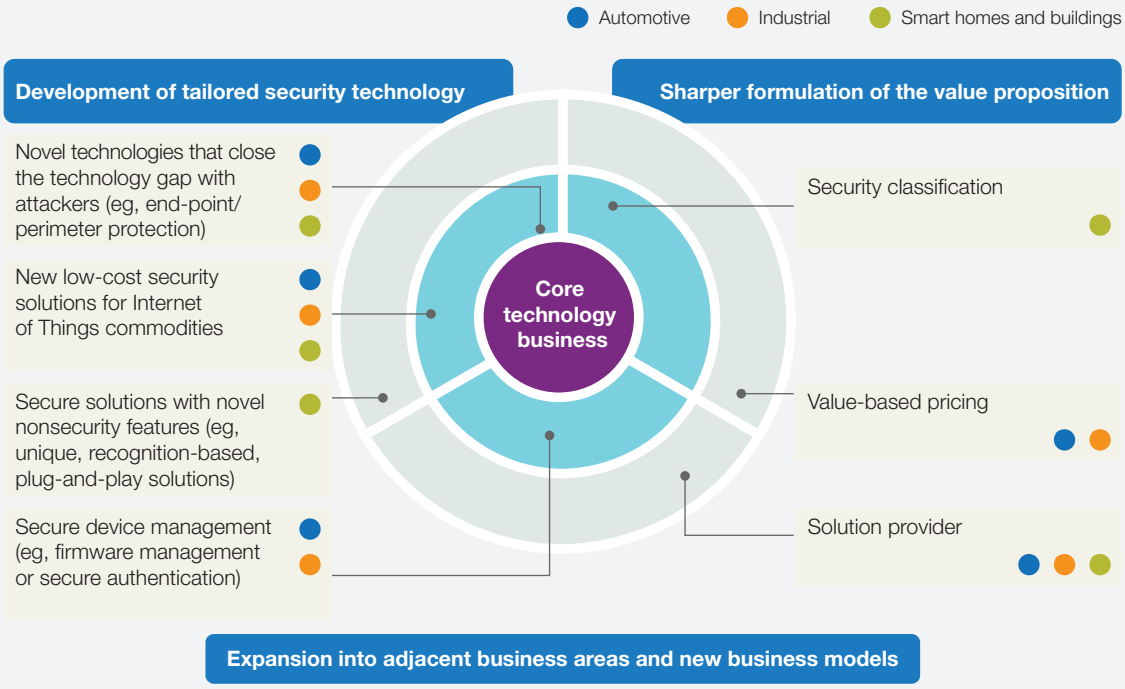
As we have noted, most companies do not view semiconductor players as potential partners in developing security solutions. To change that perception and increase the likelihood of generating profits, they will need to create a strong value proposition for their security offerings.

In consumer markets, companies often link value propositions that are difficult to understand for the end customer to ratings or other guidelines

Exhibit 4

Semiconductor companies need to create an Internet of Things strategy that involves three elements.

Strategy elements, positioned to show departure from semiconductor company's core technology business[1]



[1]Examples shown are not exhaustive. Items' position on target indicates how far they depart from semiconductor company's core technology business.

Source: Expert interviews; McKinsey/GSA Semiconductor Industry Executive Survey; McKinsey analysis

issued by a neutral third party. For instance, automakers have voluntarily developed vehicle-safety ratings and are actively publicizing their results to make consumers aware of features that might otherwise go unnoticed. With the IoT, the introduction of a "security seal" could increase awareness about the degree of protection that each device offers. Ratings from external sources might also help consumers appreciate the importance of IoT security.

In business-to-business markets, semiconductor companies need to go beyond ratings from external agencies to illustrate the value of their security offerings. Instead, they must create individual business cases for each customer—or their customer's customer—that quantify the benefits of their security features.

Expanding into new areas of the technology stack

The IoT security challenge may help semiconductor companies expand into new markets along the value chain. They may especially find opportunities within the middle layers of the technology stack, between application and hardware, such as software infrastructure, gateway communication, and communication protocols. However, this is new ground for most semiconductor companies and competition will be tough, since many other players,

including start-ups and strong incumbents from adjacent markets, are trying to develop security solutions for these layers.

When pursuing opportunities in the middle segment, semiconductor players must have a clear strategy that considers their capabilities. Overall, success in obtaining value will require strong software and infrastructure-management expertise—areas where semiconductor companies may still be developing. Thus, partnerships and collaborations will probably be the preferred choice.

Semiconductor players should also continue to look for new business models along the value chain. For instance, they could help create end-to-end security offerings, which are essential to the IoT's success. Ideally, they should play a leading role when developing such offerings, to ensure that they obtain their fair share of value.

Despite the challenges ahead, we still believe that many IoT verticals present major opportunities for semiconductor companies to become part of the security solution and capture additional value. Our survey and interviews revealed that semiconductor leaders see the possibilities ahead. Those companies that act now may become leaders—and preferred partners—in securing the IoT.

[1] For the full McKinsey Global Institute report, see *Unlocking the potential of the Internet of Things*, June 2015, on McKinsey.com.

[2] Harald Bauer, Mark Patel, and Jan Veira, "Internet of Things: Opportunities and challenges for semiconductor companies," October 2015, McKinsey.com.

Harald Bauer is a senior partner in McKinsey's Frankfurt office, **Ondrej Burkacky** is a partner in the Munich office, and **Christian Knochenhauer** is an associate partner in the Berlin office.

The authors wish to thank all executives from GSA member companies who participated in the interviews and survey that helped serve as a basis for this article.