McKinsey&Company

How CEOs can tackle the challenge of cybersecurity in the age of the Internet of Things

Advanced Industries June 2017

How CEOs can tackle the challenge of cybersecurity in the age of the Internet of Things

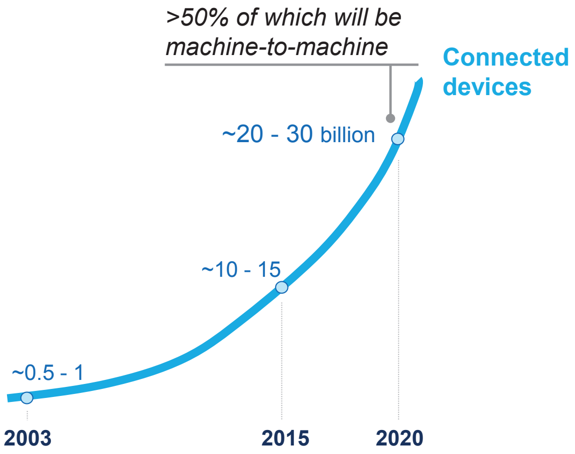
In the age of the "Internet of Everything", we are headed for a collision: billions of – often legacy – devices are being brought online, creating new vulnerabilities and headaches for executives. Here are six ways CEOs can take back control and avoid the collision.

In the last two decades, we have seen digitization rise to the top of the agenda of executive boards across the globe. As a result, cybersecurity skills and processes in most companies have also advanced – though at a slower pace. The fast growth of the so-called Internet of Things (IoT), however, is changing the game. Cybersecurity is more relevant and challenging than ever, and companies will need to pick up the pace of capability building in this area.

Companies are increasingly connecting their devices, products, or production systems, driving rapid growth of the IoT: conventional estimates put the number of connected devices at 20 - 30 billion devices in 2020, up from 10 - 15 billion devices in 2015 (Exhibit 1). The driver behind this is the enormous potential that the IoT has to make a company's products and services better or improve production efficiency. But this potential also comes with a sharp increase in security risk, taking the challenge of cybersecurity to another level for IoT technology users. To date, risking the confidentiality and integrity of information was a bigger concern than any risk regarding availability. In the IoT world, it is the other way around: lack of availability of key plants or – even worse – tampering with a customer product is the bigger risk. How can CEOs and senior executives hedge against that threat?

Exhibit 1: **The number of connected devices globally will likely double over just 5 years**

Estimated number of connected devices, including computers and smartphones



SOURCE: IHS; IDS; Gartner; ITU; McKinsey

The Internet of Things makes cybersecurity even more crucial and also more difficult to achieve

With the IoT, security challenges move from a company's traditional IT infrastructure into its connected products in the field and remain an issue through the entire product lifecycle – long after products have been sold. What is more, the industrial IoT, or Industry 4.0, means that security becomes a pervasive issue in production as well. Cyber threats in the world of IoT can have consequences beyond compromised customer privacy. Critical equipment, such as pacemakers and entire manufacturing plants, are now vulnerable, meaning that customer health and a company's total production capability are at risk.

As the IoT is connecting these additional "things" – be it products, production systems, or other devices – the sheer number of cybersecurity attack vectors increases dramatically. While in the past, the number of endpoints in a large corporate network would be somewhere between 50,000 and 500,000, with the IoT, we are talking about millions or tens of millions of endpoints. Unfortunately, many of these consist of legacy devices with either no or very insufficient security.

All in all, this added complexity makes the IoT a significantly more challenging security environment for companies to manage. If they are successful though, strong cybersecurity can become a differentiating factor in many industries, moving from a cost factor to an asset.

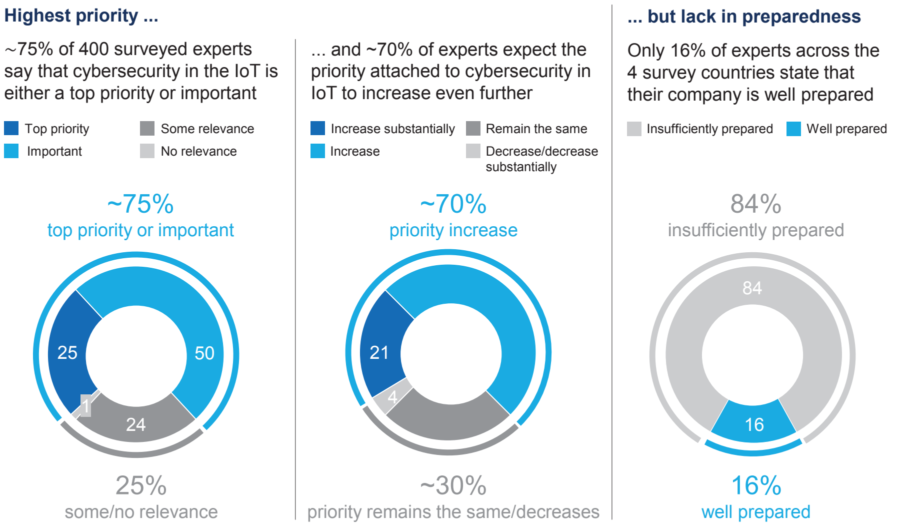
To explore the current perception of the relevance of and preparedness for IoT security, McKinsey conducted a multinational expert survey with 400 managers from Germany, the US, the UK, and Japan. The results indicate that there is a shocking gap between perceived priority and the level of preparedness.

- Of the IoT-involved experts surveyed, 75% say that IoT security is either important or very important – and that its relevance will increase – but only 16% say their company is well prepared for the challenge (Exhibit 2). Typically, low preparedness is also linked to insufficient budget allocated to cybersecurity in the IoT as indicated by the survey.

- Our interviews also revealed that along the IoT security action chain (predict, prevent, detect, react), companies are ill prepared at each step of the way. Especially weak are prediction capabilities (16% feel well prepared compared to 24 to 28% on prevent, detect and react).

- More than one-third of companies do not even have a cybersecurity strategy in place that also covers the IoT. The rest seem to have some sort of strategy but struggle with implementation.

Exhibit 2: **Striking gap between perceived importance of and readiness for IoT security**



Highest priority ...

~75% of 400 surveyed experts say that cybersecurity in the IoT is either a top priority or important

... and ~70% of experts expect the priority attached to cybersecurity in IoT to increase even further

... but lack in preparedness

Only 16% of experts across the 4 survey countries state that their company is well prepared

SOURCE: McKinsey Global Expert Survey on Cybersecurity in IoT 2017

So why are companies' progress levels regarding cybersecurity implementation not commensurate with the size of the threat brought by IoT? As indicated by the survey results, the main reasons seem to be the following:

- **Lack of prioritization.** In general, the "act-now" mentality is in short supply among senior management. In many cases, IoT leaders have yet to make the business case for a specific IoT security strategy – i.e., a budget beyond what has already been allocated for a pre-IoT environment – which would, in turn, prioritize the effort and trigger the allocation of sufficient resources.

- **Unclear responsibility.** There needs to be a holistic cybersecurity concept for the entire IoT stack, but often no single player feels responsible for creating it. Between players, there is the question of whether initial responsibility lies with product makers or with suppliers. Within organizations, it has proven difficult to determine which unit (IT security, production, product development, customer service) should take the lead. Product or plant managers often do not have the cybersecurity expertise, while corporate IT does not have sufficient access to product teams or the industrial control systems (ICS) "behind the fence."

- **Lack of standards and technical skills.** There are some industry working groups, but IoT security standards are still largely nonexistent. Even if there were standards in place, the technical competence to implement them – the required mix of operational technology and IT security knowledge – is in very short supply.

With the advent of the IoT, cybersecurity affects the entire business model. Adequately addressing the threat means bringing together several business perspectives – including the market, the customer, production, and IT. Most often, the CEO is the only leader with the authority to make cybersecurity a priority across all of these areas. We believe that the issue of cybersecurity in many cases will require senior-executive or even CEO initiative.

Six recommendations for CEOs

There is no silver bullet for tackling cybersecurity in the IoT. However, three strategic lenses can help CEOs think about IoT security, and three actions can help CEOs and senior leaders set their organizations up for success:

Three ways to think strategically about cybersecurity in the Internet of Things

1. Understand what IoT security will mean for your specific industry and business model

Across all industries, a certain minimum level of IoT security will be required as a matter of "hygiene." As such, the recent "WannaCry" attack by and large compromised organizations with legacy operating systems, such as Windows XP, which had not appropriately been patched. Simple patch management – a matter of adequate IT management, not sophisticated cyber defense – is something that is expected as "hygiene" from companies, without customers needing to pay a price premium for it."

However, we think that there is potential for treating security as more than just "hygiene." In the last decade, many companies have witnessed how IT evolved from a cost center to a source of real differentiation, driving customer satisfaction and willingness to pay. A similar change could lie ahead for IoT security, and in an increasing number of industries, we are already witnessing it today. One example is the physical security industry. Door lock companies can already today demand a price premium for products with especially strong cybersecurity features, as cybersecurity can make or break the main function of the product.

Effective IoT security solutions consider an organization's business model, where it lies in the value chain, and the industry structures in which it operates. For examples of how industry impacts IoT security, please refer to the Text Box.

Text Box: More trust, less downtime – examples for the role and relevance of IoT security by industry

The goal of the IoT security strategy varies by industry and company type. Industries differ in their approach, depending on many factors, such as the role of cybersecurity in differentiating the product, the supply chain structure and incentives, and the level of maturity reached to date.

- *For an energy utility,* IoT security is mostly a production play, as it will mean dealing with a large installed base of legacy production systems that were never designed to be connected and, in turn, not designed with the defense against cyber attacks in mind. What is more, legacy systems have little additional capacity (e.g., computing performance, memory) that could be used for added security measures, and they are often not accessible in the field. To still reap the huge benefits from connecting these systems, targeted counter-measures need to be taken. Process industry players in particular have leveraged their innate strength in industrial safety for creating new processes and safety measures, creating redundancy, and "sandboxing" key systems to avoid entire system failure. Challenges for industrials lie in the lack of cybersecurity expertise of many component suppliers and the lack of standardization incentives for many integrators.

- *For automotive OEMs,* IoT security is also a product play, and will become the new quality management for the era of connected cars. OEMs are facing a unique level of challenges given the increasing complexity of their product: A modern car is comprised of between 30 and 100 electronic control units (ECUs) and hundreds of millions lines of code – a complexity in which even the best programmers cannot avoid vulnerabilities. What's more, the automotive industry has one of the most fragmented supply chains. The 30 to 100 ECUs could easily be sourced from more than 20 different suppliers, creating additional complexity. Thus, a holistic concept is needed, one that addresses two aspects. On the one hand, cybersecurity needs to be embedded already in the design and development of the product, as well as in the maintenance and response architecture. On the other hand, OEMs must work closely with their ecosystem, e.g., with other industry players and regulatory bodies to set up standards, and with the end users who are directly involved in protecting their cars (e.g., by keeping software updated). However, solutions will have to scale well and be cost effective, as OEMs have to contend with users' limited willingness to pay for added cybersecurity.[1]

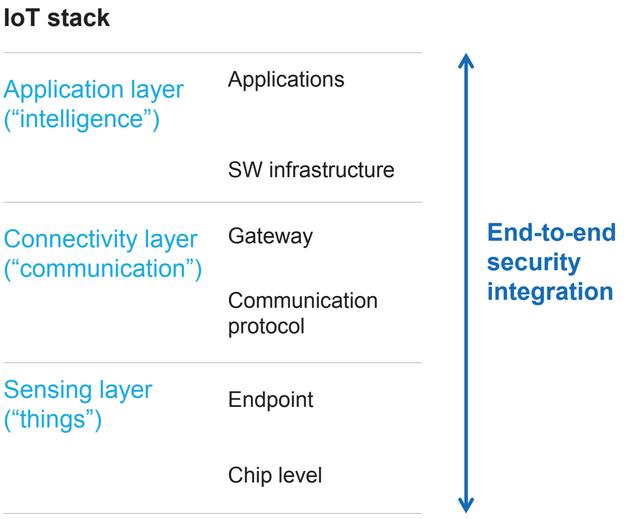
CEOs need to ensure they understand the role and relevance of IoT security in their industry and how they can monetize it in alignment with their specific business model. A thorough understanding of what IoT security means for a company cannot end on the strategic level though. CEOs need to be aware of the main points of vulnerability along the cybersecurity action chain of predict, prevent, detect, react. Typically, an overview of the top attack scenarios for a specific company and an understanding of attackers and their motivation will be a good base for further strategy development and budget allocations. Security investments must be targeted according to the risk most detrimental to the specific business or industry.

2. Set up clear roles and responsibilities for IoT security along your supply chain

IoT requires a holistic cybersecurity concept that extends across the entire IoT stack, i.e., all layers of the application, communication, and sensors. Of course, each individual layer needs to be secured, but companies also need to prepare for cross-layer threats (Exhibit 3).

[1] For further details on cybersecurity in the automotive industry, please refer to the report "Shifting gears in cybersecurity for connected cars" by our McKinsey colleagues Wolf Richter, Simone Ferraresi and Corrado Bordonali

Exhibit 3: **IoT security requires layer-specific as well as cross-layer solutions**



IoT stack

Application layer (“intelligence”)	Applications SW infrastructure
Connectivity layer (“communication”)	Gateway Communication protocol
Sensing layer (“things”)	Endpoint Chip level

End-to-end security integration

SOURCE: McKinsey

This will require a strategic dialogue with upstream and downstream business partners – whether suppliers or customers – to sort out responsibilities for security along the entire supply chain. A starting point for this discussion should be identifying the weakest links in the holistic model; from an attacker’s point of view, these will be targeted first to harm the entire chain. Who then takes on which role should depend on who has the competence and who has the incentives, which might include a monetization model. Industry players active in each part of the IoT stack bring certain advantages they can build on to provide an integrated solution:

- Device and semiconductor manufacturers active at the lower level of the stack can build on their design capabilities of low-level (hardware) security as an advantage for designing higher (software) security.

- Network equipment manufacturers profit from the fact that many key competencies in transport-layer security design are applicable to the application layer. Beyond that, they can build on their hardware design capabilities for offering an integrated solution.

- Application designers can leverage their control of application interfaces and/or customer access as an advantage in defining low-level architectures.

3. Engage in a strategic conversation with your regulator and collaborate with other industry players

A company’s cybersecurity creates externalities that go far beyond the effects on the company’s performance itself and thus needs to be tackled across the classic government-business divide. Most current cybersecurity standards fall short because they are neither industry specific nor detailed enough, and they neglect most layers of the IoT stack, including production and product development. Regulators will eventually be stepping in to address this gap, and companies need to get involved in the discussion, or even better, set the tone.

Industry leaders can shape these structures by proactively getting key players in the industry together to establish IoT security standards for their specific industry. Partnerships with other players, including competitors, can also lead to a mutually beneficial pooling of resources above and beyond official industry standards. For example, in the banking sector, one company got several competitors together to set up “shared assessments” to evaluate the security technology vendors, resulting in enormous efficiency gains for both the banks and the suppliers. Another example from the banking sector is FS-ISAC, an information community through which competing banks share information on security weaknesses, attacks, and successful countermeasures.

Three ways to set your organization up for success in IoT security

4. Conceive of cybersecurity as a priority for the entire product lifecycle, and develop relevant skills to achieve it

Security needs to be part of the entire product lifecycle, starting with product design, moving through the development process, and continuing each day of the product’s use. Fundamental to the security of products while in the field is “security by design” in the product development stage. Security also needs to be ensured during the production/manufacturing process, given the role of Industry 4.0 in driving the proliferation of IoT on shop floors and in other production settings. Lastly, a concept is required for securing the products after they have been sold. To this end, companies need a strategy to deliver security patches to products in the field via, for example, over-the-air update capabilities.

Achieving cybersecurity along the entire product lifecycle requires organizational and technological changes. The organizational component involves clear responsibility for cybersecurity in the product and production environment. A few companies have acted by giving the CISO responsibility for both IT and OT cybersecurity. Whatever the structural setup: an alignment of goals is crucial, since strong collaboration between the CISO function and the respective other departments, be it product development, production, or even customer service, will be required. Additionally, new roles should be created that systematically integrate security into all relevant products and processes. A European telco and media company, for example, is leveraging large-scale training programs conducted by its core CISO organization to create a community of “security champions” throughout the organization. These security champions get additional decision making authority within their teams, e.g., product teams, as a result of achieving “cybersecurity capable” status. The CISO organization is able to leverage these trainings to grow its reach by a factor of 4.

5. Be rigorous in transforming mindsets and skills

Institutionalizing the notion that security is “everyone’s business” starts at the top, with executives role-modeling security behavior and also cultivating a culture where security is constantly evolving and the identification of weak spots is rewarded rather than punished. To that end, some companies have implemented programs that reward employees for identifying security vulnerabilities.

Additionally, CEOs need to ensure that security-specific knowledge and qualifications become a standard requirement for employees in IT, product development, and production. On the one hand, additional training programs for current employees may help; on the other hand, specific IoT security talent needs to be developed. In the age of IoT, cybersecurity specialists must understand product development and production as well as IT security. To develop these new crossover skills at scale, companies should consider working with other players in the industry to, for example, create university programs and vocational training curricula.

6. Create a point-of-contact system for external security researchers and implement a post-breach response plan

Companies need to implement a single, visible point of contact for IoT-security-related notifications or complaints. In the last two years, and especially in the IoT context, there have been numerous examples of security researchers trying to notify a company several times after discovering a breach and the company either not following up at all or the researcher being handed from one department to the next without finding someone who could take responsibility for the matter.

In addition, companies need a response plan in place for different attack scenarios. Recent examples have shown that the fallout from an unprofessional response to an incident has been more damaging than the incident itself. In an IoT world, incidents can affect the heart of a company's operations, so cybersecurity, especially with regard to IoT incidents, needs to be part of business continuity management and disaster recovery planning. Maybe most importantly, a strong communication strategy needs to be designed, one that is scenario specific and delivers current, transparent, and appropriate messaging to customers, regulators, investors, and potentially the general public.

□ □ □

Cybersecurity remains much talked about, yet underleveraged as a differentiating factor on the business side. With the advent of the IoT, there is real opportunity to move ahead and designate the security of products, production process, and platforms as a strategic priority. The breadth of the challenge spans the entire supply chain and the whole product lifecycle and includes both the regulatory and the communication strategy. For CEOs in leading IoT organizations, we believe cybersecurity should be at the top of the agenda until rigorous processes are in place, resilience is established, and mindsets are transformed.

Authors

Dr. Harald Bauer
Senior Partner, Frankfurt
harald_bauer@mckinsey.com

Dr. Gundbert Scherf
Partner, Berlin
gundbert_scherf@mckinsey.com

Valerie von der Tann
Engagement Manager, Berlin
valerie_tann@mckinsey.com

Laura Klinkhammer
Associate, Cologne
laura_klinkhammer@mckinsey.com

The authors wish to thank Venky Anant, Tucker Bailey, James Kaplan, Mark Patel, Chris Rezek, Wolf Richter, Rolf Riemenschnitter, and Dominik Wee for their valuable contributions and for sharing their perspectives.

Advanced Industries
June 2017

Design contact: Visual Media Europe
www.mckinsey.com