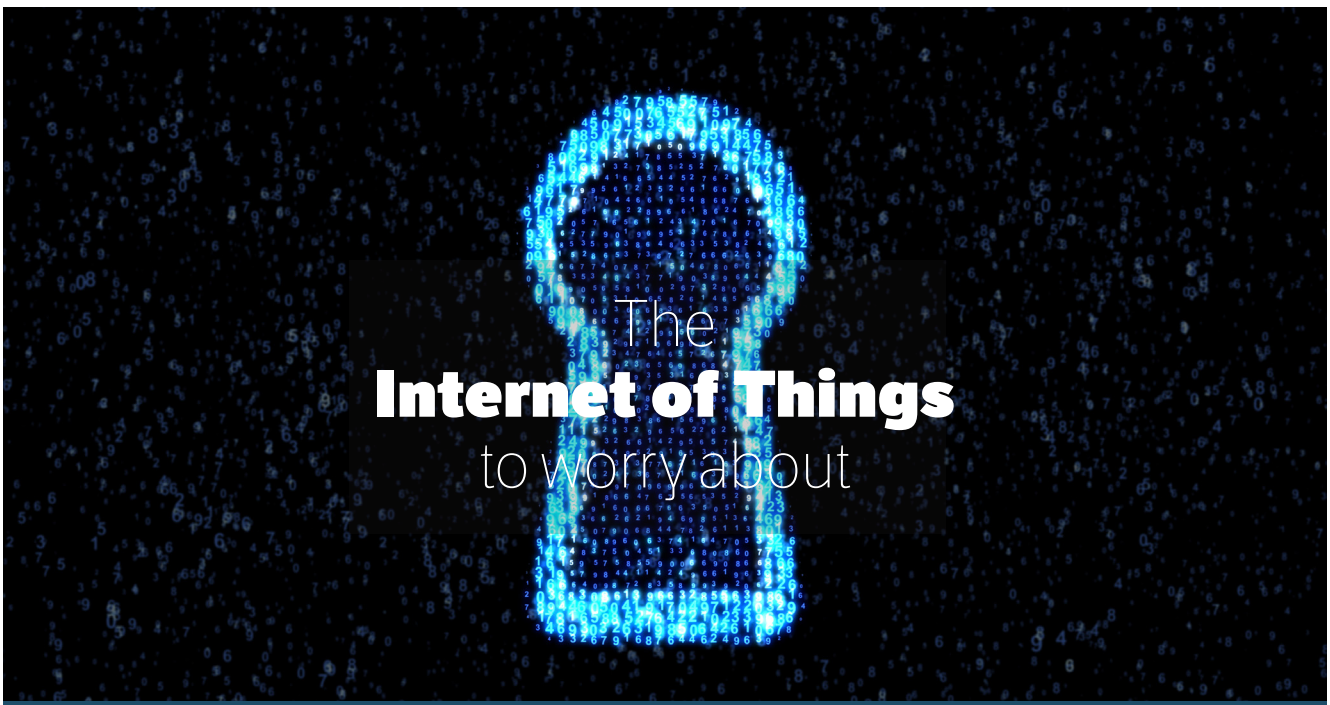
After hours

Book review



Title: **Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry**

Author: **Maciej Kranz**
Publisher: **Wiley**

Kellyanne Conway, the high-profile Counsellor to President Donald Trump of the United States, caused much mirth in March when she stated her fear of being spied on by her kitchen appliances. The ability of microwave ovens to "turn into cameras," she told *MSNBC*, was "a fact of modern life."

Yet in 2012, former Central Intelligence Agency director David Petraeus said so-called "smart homes" would open new doors to spies, and the CIA did find a way to turn Samsung "smart" televisions into covert listening devices. In February, German authorities warned purchasers of a doll named My Friend Cayla to switch it off because hackers could use it to track kids.

Welcome to the dark side of the "Internet of Things," a new technological revolution for manufacturers but a potential source of headaches for consumers. But Maciej Kranz, Vice President, Corporate Strategic Innovation Group, at Cisco Systems focuses on the upside in his new book, *Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry.*

Kranz rates IoT, as it is known, as one of the biggest information technology transformations, exceeding the influence of business process reengineering, Six Sigma, lean manufacturing or agile computing. "By converging… sensors, machines, cells, and zones, IoT-driven factory automation helps enterprises integrate production and business systems and then bring everything online over a single network," he writes.

Coinage of the term "Internet of Things" is attributed to Kevin Ashton, a British manager at Procter & Gamble, who developed an interest in the radio-frequency identification technology used to tag items in stores for pricing and inventory control. It was the title of his 1999 presentation to management on tracking the company's global supply chain.

Ashton went on to co-found the AutoID Lab at the Massachusetts Institute of Technology, which researches advanced sensing technology. In an interview some years ago, Ashton conceded that security had not been his major priority. "Do the security and privacy risks outweigh the benefits? Absolutely not! The benefits are many millions of times greater."

Times have changed. "The ability to deal effectively with security threats is the number 1 make-or-break factor for IoT adoption," Kranz acknowledges in his book. "Many companies continue to be in

denial, still relying on a discredited physical separation approach to securing their plants and infrastructure."

Without adequate security, Kranz argues, "companies will be reluctant to implement IoT and thus not benefit from the growing number of powerful use cases emerging across all industries." And Kranz cites an impressive number of case studies.

In the U.S., Goodyear Tire & Rubber Company wanted to make it easier to gather and analyse data, while Metrolinx, a government-owned transport agency in Canada, sought to digitally integrate services from ticketing to freight to public address systems. FANUC, a Japanese robot manufacturer, collects real-time data on usage and downtime from its customers.

Kranz focuses on the operational side of IoT – noting technical, organizational and regulatory challenges to its adoption – as well as growth projections, new business models and the likely impact on careers, workplace roles and organizational change.

Eventually he tries to answer the sort of hard questions demanded by finance professionals. "When it comes to IoT implementation, every manager wants to know the return on investment," he writes. "Unfortunately, in most cases the answer is specific to each organization, the issues it's trying to address, and its starting point."

Overall, says Kranz, IoT adoption can reduce costs and increase efficiency by, say, optimizing energy consumption. "Predictive maintenance, for example, lowers cost through reductions in unplanned downtime," he observes.

Some of his recommendations will seem obvious to accountants. "Converge around standards," he advises. "Vendors and enterprises alike need to leverage IT industry standards and best practices… and to fill in the gaps between industry-specific and horizontal standards organizations."

Kranz's book is an admirable overview of a technology that many in Hong Kong are only just beginning to encounter. Executives should not be dissuaded by "alternative facts," such as disputed claims of meddling microwaves.

Author interview: Maciej Kranz

Maciej Kranz first encountered the Internet of Things in the early 2000s, as a Cisco Systems manager on a business trip to Rockwell Automation in the industrial city of Cleveland, Ohio, to develop switches that would, through Ethernet, link industrial control and information technology systems.

"We were just beginning to recognize the necessity of building industrial networks on open standards," he recalls. "Ultimately, we began a journey that continues today of connecting more and more things with jointly developed architectures."

Along the way, Kranz felt there was a void developing between the hype about IoT and its practical reality. "Over the past few years, we as an industry have been flooding customers with technology-focused messaging, big numbers and even bigger predictions of numbers of connected devices and revenue impact," he says.

Business managers, such as people who operate plants, retail stores or logistics systems, found the message "over their heads," according to Kranz. "They care about business outcomes such as productivity, uptime, top and bottom line. So the goal of the book was to bridge the gap between hype and reality and show business managers how they can implement IoT today."

Kranz's book focuses on the myriad industrial and commercial applications for IoT, and he acknowledges that for many ordinary people, IoT means scary headlines about appliances running amok.

"Consumer applications tend to get the buzz, but industrial and commercial applications tend to be more robust, and create the most value," he points out.

For example, an October 2016 distributed-denial-of-service attack shut down many popular websites in North America and Europe, including Etsy, Github, Spotify and Twitter. "It got a lot of attention because so many people were affected," says Kranz. He sees government at various levels having a number of key roles to play in regulating IoT. "Agencies must work closely with industry to make sure policies, laws and actions related to IoT are effective," he maintains. "There will be competition for bandwidth and other resources; there will be ideas that may conflict with public policy; and there will be dubious IoT-based ideas that may present a public safety threat or privacy concern. Think drones."

The interconnectedness of IoT, he believes, offers a window into the overall health of operations. "Remote asset management saves you money every time you can identify and fix a problem from the control centre instead of sending a technician out," says Kranz.

"Even more important," he adds, "are the opportunities for new revenue streams, new business models, new business structures, and new value propositions. Once you start connecting things, you can conceive and execute new processes and innovative strategies that wouldn't have been possible before."